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

CRISTIANE BARBOSA PRADO

AVALIAÇÃO DA ROBUSTEZ DE REDES SEM FIO INDUSTRIAIS POR MEIO DE MODELO DIGITAL E TÉCNICAS DE CENTRALIDADES

Porto Alegre
2026

CRISTIANE BARBOSA PRADO

AVALIAÇÃO DA ROBUSTEZ DE REDES SEM FIO INDUSTRIAIS POR MEIO DE MODELO DIGITAL E TÉCNICAS DE CENTRALIDADES

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: Eletrônica

ORIENTADOR: Prof. Dr. Ivan Müller

Porto Alegre
2026

CRISTIANE BARBOSA PRADO

AVALIAÇÃO DA ROBUSTEZ DE REDES SEM FIO INDUSTRIAIS POR MEIO DE MODELO DIGITAL E TÉCNICAS DE CENTRALIDADES

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. Carlos Eduardo Pereira, PPGEE - UFRGS
Doutor pela Technische Universitat Stuttgart – Alemanha

Prof. Dr. João Cesar Netto, PPGC - UFRGS
Doutor pela Université Catholique de Louvain – Bélgica

Prof. Dr. Ivanovitch Medeiros Dantas da Silva, DECA - UFRN
Doutor pela Universidade Federal do Rio Grande do Norte – Natal, Brasil – com período sanduíche em Faculdade de Engenharia da Universidade do Porto

Coordenador do PPGEE: _____
Prof. Dr. Ing-. Luís Alberto Pereira

Porto Alegre, janeiro de 2026.

DEDICATÓRIA

Dedico este trabalho à minha mãe, em especial pela dedicação e apoio em todos os momentos.

AGRADECIMENTOS

Ao Programa de Pós-Graduação em Engenharia Elétrica, PPGEE, pela oportunidade de realização de trabalhos em minha área de pesquisa.

Ao meu orientador por me acolher em sua equipe de pesquisa.

Aos colegas do PPGEE pelo seu auxílio nas tarefas desenvolvidas durante o curso e apoio na revisão deste trabalho.

À CAPES pela provisão da bolsa de mestrado.

RESUMO

As redes sem fio são amplamente utilizadas em ambientes industriais devido à praticidade e mobilidade, mas enfrentam desafios como interferências, limitações de banda e problemas de segurança, que impactam sua confiabilidade e consumo de energia. Este trabalho utiliza o conceito “Gêmeo Digital de Rede" (DTN, do inglês *Digital Twin Network*) com o intuito de virtualizar uma rede sem fio industrial, para efetuar alterações prévias na rede física, a fim de analisar seu desempenho, diagnosticar problemas, prever resultados futuros e implementar melhorias de forma segura e eficiente. O projeto utiliza uma aplicação desenvolvida para coletar os dados da rede real, como níveis de sinal, taxas de perda de pacotes e desempenho geral. Esses dados são usados para construir um modelo virtual (DTN), que é utilizado para simular diferentes técnicas de roteamento e analisar melhorias propostas antes de aplicá-las à rede física. A análise utiliza conceitos de teoria de grafos, como centralidades de intermediação, grau e proximidade, para identificar gargalos e nós críticos. A partir disso, intervenções são simuladas, como a adição de repetidores, para verificar suas implicações à escalabilidade da rede.

Palavras-chave: Gêmeo Digital de Rede, *Fieldbus*, Redes Sem Fio Industriais, Roteamento.

ABSTRACT

Wireless networks are widely used in industrial environments due to their practicality and mobility, but they face challenges such as interference, bandwidth limitations, and security issues, which affect their reliability and energy consumption. This work employs the concept of a “Digital Twin Network” (DTN) to virtualize an industrial wireless network, in order to perform preliminary modifications to the physical network, aiming to analyze its performance, diagnose problems, predict future outcomes, and implement improvements safely and efficiently. The project uses an application developed to collect data from the real network, such as signal levels, packet loss rates, and overall performance. These data are used to build a virtual model (DTN), which is then employed to simulate different routing techniques and analyze proposed improvements before applying them to the physical network. The analysis uses concepts from graph theory, such as betweenness, degree, and closeness centralities, to identify bottlenecks and critical nodes. Based on this information, interventions are simulated, such as the addition of repeaters, to verify their implications for network scalability.

Keywords: Digital Twin of Network, Fieldbus, Wireless Industrial Network, routing.

LISTA DE ILUSTRAÇÕES

Figura 1 – Roteamento *Convergecast*. 16
Figura 2 – Diferença entre os roteamentos *unicast*, *broadcast* e *convercast*. . . . 22
Figura 3 – Primeiro caminho encontrado no cálculo do caminho mais curto de A até D. A seta indica o atual nó ativo. 24
Figura 4 – Roteamento de Grafo. 25
Figura 5 – Exemplo de roteamento RPL. 27
Figura 6 – Densidade probabilística em função da média μ e do desvio padrão σ. 29
Figura 7 – Exemplificação de centralidades em uma grafo de nodos. 32
Figura 8 – CPF do DCCMO e configurações do sensor sem fio para pontos em destaque. 41
Figura 9 – Rede *Wireless*HART e seu DT. 47
Figura 10 – Diagrama de sequência do sistema de virtualização da RSFI. 67
Figura 11 – *Setup* utilizado. 68
Figura 12 – Ler entradas de dispositivos (*Bytes* de dados de requisição). 68
Figura 13 – Ler entradas de dispositivos (*Bytes* de dados de resposta). 68
Figura 14 – Relatório de lista de saúde dos vizinhos (*Bytes* de dados de requisição). 68
Figura 15 – Relatório de lista de saúde dos vizinhos (*Bytes* de dados de resposta). 69
Figura 16 – Ler apelido do dispositivo (*Bytes* de dados de resposta). 69
Figura 17 – Relatório de níveis de sinal dos vizinhos (*Bytes* de dados de requisição). 69
Figura 18 – Relatório de níveis de sinal dos vizinhos (*Bytes* de dados de resposta). 69
Figura 19 – Ilustração de um *superframe* de 100 *slots* com salto de canais. 69
Figura 20 – Perdas por *buffer* cheio e obsolência. 70
Figura 21 – Posicionamento dos dispositivos de campo em relação ao *gateway*. . . 71
Figura 22 – Grafo gerado pelo Gerenciador da rede. 72
Figura 23 – RSFI evidenciando os enlaces não estabelecidos pelo gerenciador de rede. 75
Figura 24 – Resultado das centralidades para a rede simulada. 76
Figura 25 – Porcentagem de pacotes perdidos por TTL para cada método de intervenção na rede. 78
Figura 26 – Porcentagem de pacotes perdidos por *buffer* cheio para cada método de intervenção na rede. 79
Figura 27 – Porcentagem de pacotes em trânsito ao final do teste para cada método de intervenção na rede. 80
Figura 28 – Confiabilidade da rede após cada método de intervenção. 81
Figura 29 – rede ampliada. 86
Figura 30 – Porcentagem de pacotes perdidos por TTL para cada método de intervenção na rede. 87

Figura 31 – Porcentagem de pacotes perdidos por *buffer* cheio para cada método de intervenção na rede. 87
Figura 32 – Porcentagem de pacotes em trânsito ao final do teste para cada método de intervenção na rede. 88
Figura 33 – Confiabilidade da rede após cada método de intervenção. 88
Figura 34 – Confiabilidade da rede em relação ao total de dispositivos acrescentados. 89

LISTA DE TABELAS

Tabela 1 – Densidade probabilística em função da quantidade de desvios padrões 30
Tabela 2 – Comparação entre os estudos 46

LISTA DE ABREVIATURAS

ACK	*Acknowledgement*
ASN	*Absolute slot Number*
CG	Centralidade de Grau
CI	Centralidade de Intermediação
CP	Centralidade de Proximidade
DT	*Digital Twin*
DTN	*Digital Twin of Network*
EIoT	*Edge Internet of Things*
ETX	*Expected Transmission Count*
FIFO	*First In First Out*
IIoT	*Industrial Internet of Things*
IIR	*Infinite Impulse Response*
IoT	*Internet of Things*
ISO	*International Organization for Standardization*
HART	*Highway Addressable Remote Transducer*
HART-IP	*Highway Addressable Remote Transducer over Internet Protocol*
LQI	*Link Quality Indicator*
MAC	*Medium Access Control*
PDP	*Packet Delivery Probability*
PDR	*Packet Delivery Ratio*
RPL	*IPv6 Routing Protocol for Low power and Lossy Networks*
RSFI	Redes Sem Fio Industriais
RSL	*Received Signal Level*
RSSI	*Received Signal Strength Indicator*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TTL	*Time to Live*

TDMA *Time Division Multiple Access*

TSCH *Time Slotted Channel Hopping*

UAV *Unmanned Aerial Vehicle*

WH *Wireless*HART

LISTA DE SÍMBOLOS

$Carga_{PA}$	Proporção de dispositivos de uma cadeia em relação ao total de dispositivos da rede
p_{per}	Total de pacotes perdidos
p_{suc}	Total de pacotes bem sucedidos
λ	Constante de ponderação do algoritmo RPL
σ	Desvio padrão
μ	Média
θ	Confiabilidade

SUMÁRIO

1 INTRODUÇÃO 15
1.1 Motivação 16
1.2 Objetivos 17
1.2.1 Objetivo Geral 17
1.2.2 Objetivos Específicos 17

2 FUNDAMENTAÇÃO TEÓRICA 18
2.1 Elementos que compõem uma RSFI 19
2.1.1 Gerenciador de Rede 19
2.1.2 Gateway 20
2.1.3 Ponto de Acesso 21
2.1.4 Dispositivos de Campo 21
2.2 Tipos de Roteamento 21
2.2.1 *Unicast* 22
2.2.2 *Broadcast* 23
2.2.3 *Convergecast* 23
2.2.4 Roteamento em RSFI: exemplo WH 24
2.2.5 Confiabilidade de RSFI 28
2.3 Centralidades 30
2.3.1 Centralidade de Grau 33
2.3.2 Centralidade de Proximidade 33
2.3.3 Centralidade de Intermediação 34
2.4 Gêmeo Digital 35

3 ESTADO DA ARTE 38
3.1 Análise de posicionamento de dispositivo 38
3.2 DTN 41
3.2.1 DTN em aplicações não industriais 42
3.2.2 DTN na Indústria 43
3.3 Resumo 45

4 MATERIAIS E MÉTODOS 47
4.1 Setup RSFI 48
4.2 Comandos WH Implementados no Sistema 49
4.3 Leitura da Rede 50
4.4 Classes do Gêmeo Digital de Rede de uma RSFI 52
4.5 Roteamento na DTN 54

4.6 Simulação de desempenho da RSFI 56
4.7 Métricas de desempenho da RSFI 59
4.7.1 Perda de pacotes por *buffer* cheio 60
4.7.2 Perda de pacotes por obsolência de TTL 62
4.8 Identificação de nodos críticos e intervenções 63
4.8.1 Simulação de adição de *links* 63
4.8.2 Simulação de novo roteamento 64
4.8.3 Simulação de adição de nodos redundantes 64
4.9 *Setup* das RSFI utilizadas 65

5 RESULTADOS 73
5.1 Experimentos realizados na rede virtual 73
5.1.1 Nodos críticos 74
5.1.2 Pacotes perdidos por TTL 77
5.1.3 Pacotes perdidos por *buffer* cheio 78
5.1.4 Pacotes em trânsito 80
5.1.5 Confiabilidade da rede 81
5.2 Ampliação da rede virtual 82
5.2.1 Pacotes perdidos por TTL 83
5.2.2 Pacotes perdidos por *buffer* cheio 83
5.2.3 Pacotes em trânsito 83
5.2.4 Confiabilidade da rede 84
5.3 Acréscimo de dispositivos 84

6 CONCLUSÕES 90
6.1 RSFI Implementada 91
6.2 RSFI Ampliada 92
6.3 Avaliação dos resultados 92
6.4 Trabalhos Futuros 93

REFERÊNCIAS 95

1 INTRODUÇÃO

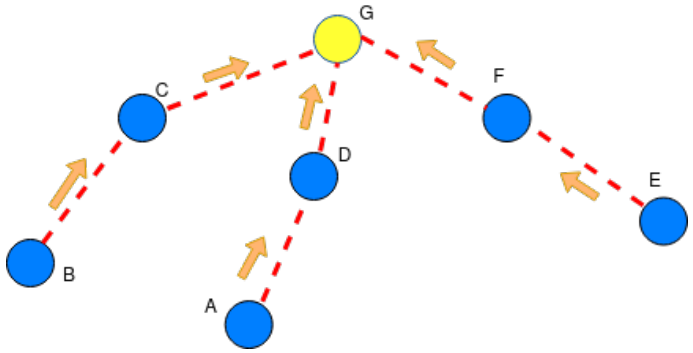
Redes Sem Fio Industriais (RSFI) estão cada vez mais presentes em ambientes fabris devido à praticidade de implantação e mobilidade dos seus componentes. Isto implica aumento do custo-benefício total para determinadas aplicações, já que não é necessário realizar a instalação e manutenção de uma extensa rede cabeada. Aplicações típicas de RSFI com gerenciamento centralizado envolvem a troca de dados cíclicos entre um controlador central e um conjunto de sensores e atuadores distribuídos. Estas redes geralmente são compostas por: gerenciador de rede, *gateway*, ponto de acesso e dispositivos de campo. O gerenciador é responsável por tarefas como provisionamento de novos dispositivos, roteamento, escalonamento e otimização da rede, além de adaptações a questões dinâmicas da rede (KüNZEL; INDRUSIAK; PEREIRA, 2020).

Para que sejam de fato robustas, as RSFI devem lidar com problemas tais como o processo de roteamento, que consome muitos dos recursos já limitados nos dispositivos, bem como o fato de que as comunicações sem fio disputam o uso do meio com interferências eletromagnéticas, ruídos e coexistência com outras redes, que implicam perda de pacotes (diminui a confiabilidade da rede) e aumento do consumo de energia (devido aos reenvios de pacotes pós-falha).

A característica da rede que descreve a sua capacidade de permitir variabilidade de quantidade e diversidade de nodos, roteamentos, topologias e aplicações, e ao mesmo tempo permanece com níveis aceitáveis de critérios de desempenho, é a escalabilidade. O aumento do número de nodos na rede impacta o desempenho, ao aumentar a ocupação da banda limitada e as interferências. Este fenômeno pode ser notado mais especificamente em roteamentos *convergecast*, onde vários nodos da rede destinam pacotes a um nodo em comum. No caso de uma RSFI é fácil associar com o processo de envio de pacotes destinados ao *Gateway* da rede, onde os nodos encaminham as mensagens ao ponto de acesso mais próximo através de rotas *uplink*, conforme a Figura 1 apresenta.

Este trabalho visa analisar a robustez e a confiabilidade de RSFI por meio da virtualização de uma rede que seja conhecida e que esteja em operação. A partir dos dados coletados da RSFI analisada, é construída a simulação, onde o roteamento é reconstruído para testar a robustez e a confiabilidade da rede. Além disso, o trabalho identifica os

Figura 1 – Roteamento *Convergecast*.



Fonte: autor.

nodos gargalos através de critérios de centralidade, simula possíveis intervenções, como a adição de novos enlaces, substituição do algoritmo de roteamento por outro, e adição de repetidores próximos ao nodo mais crítico. Após as alterações na rede, a simulação é submetida a novos testes para comparar a confiabilidade do sistema antes e após as intervenções.

A abordagem adotada para a realização deste trabalho estabelece uma base conceitual e técnica que pode ser expandida para a implementação de um Gêmeo Digital de Rede (DTN, do inglês *Digital Twin of Network*), o que permite, além do monitoramento e análise preditiva, a execução de ajustes e otimizações na RSFI existente de forma integrada. Entretanto, neste estudo, o escopo foi restrito à etapa de virtualização da rede, não abrangendo o envio dos resultados da simulação ao gerenciador da RSFI. Para completar o ciclo de um DTN a este trabalho, é necessário incorporar o processo de intervenção do ambiente virtual sobre o físico, o que possibilitará a retroalimentação contínua e a tomada de decisões automatizada ou assistida em tempo real, onde se compartilha inteligência e cooperação entre sistemas físicos e sistemas virtuais da rede (WU; ZHANG; ZHANG, 2021).

1.1 Motivação

O intuito de utilizar um DTN é aumentar a robustez de uma RSFI e proporcionar ferramentas aos gerenciadores da rede para que tomadas de decisões aconteçam de forma mais rápida e com menor custo. Como o DTN co-evolui com a rede, ele permite que pequenas alterações na rede sejam mapeadas, analisadas e comparadas com cenários antigos, atuais e futuros, e permite que seus resultados sejam implementados na rede já em operação, de modo a diminuir a necessidade de intervenção externa para tomadas de decisão.

As intervenções que são sugeridas para a aplicação desenvolvida foram definidas com a intenção de garantir que a rede continue dentro de parâmetros de interesse, utilizando intervenções que impliquem mínima alteração física e que sejam possíveis de ser implementadas em um curto período de tempo, de modo a manter uma das principais caracte-

rísticas de RSFI, que é flexibilidade e facilidade de instalação. Para tanto, algumas intervenções que atendem a estes critérios são otimizar as rotas e roteamentos, e acrescentar dispositivos sem fio.

Assim, torna-se pertinente levantar hipóteses que investiguem se é possível aprimorar o desempenho da rede sem a necessidade de intervenções físicas diretas durante a operação normal do sistema. Diante desse cenário, uma hipótese central consiste em assumir que o uso de um DTN permite avaliar e validar estratégias de fortalecimento da rede de forma segura e controlada, sem a interrupção do processo produtivo. Parte-se do pressuposto de que, ao virtualizar a topologia da rede e reproduzir seu comportamento por meio de dados reais coletados continuamente, é possível simular diferentes técnicas de intervenção, como reconfiguração de enlaces, alteração de rotas ou adição de redundâncias, antecipando seus impactos sobre métricas de confiabilidade e desempenho. Dessa forma, a hipótese sustenta que decisões baseadas em simulações preditivas reduzem a necessidade de testes empíricos no ambiente físico.

Adicionalmente, assume-se como hipótese que a aplicação iterativa desse processo de digitalização, simulação e realimentação de dados contribui para o aumento progressivo da robustez da rede ao longo do tempo. Ao comparar cenários históricos, atuais e preditivos, o administrador da rede pode identificar padrões de degradação, gargalos recorrentes e nós críticos, adotando intervenções planejadas e fundamentadas. Assim, a hipótese geral é que a integração entre análise virtual e implementação controlada no domínio físico constitui uma abordagem eficaz para fortalecer as RSFI, garantindo sua robustez operacional sem comprometer a continuidade da produção.

1.2 Objetivos

Nesta seção são abordadas as metas que o estudo se propõe a alcançar.

1.2.1 Objetivo Geral

Coletar dados de uma RSFI conhecida e em operação, de modo a virtualizá-la. Implementar diferentes intervenções de otimização na versão virtualizada da rede e comparar os resultados obtidos após as intervenções, com o intuito de analisar os impactos de cada método na confiabilidade da rede.

1.2.2 Objetivos Específicos

- Implementar algoritmos de roteamentos na RSFI virtual;
- Diagnosticar os nodos críticos da RSFI virtual e simular acréscimos de nodos próximos, para aumentar a confiabilidade da RSFI virtual;
- Analisar o desempenho da RSFI virtual antes e após as intervenções.

2 FUNDAMENTAÇÃO TEÓRICA

A ideia-chave de um DT é criar uma réplica digital (ou virtual) de um sistema físico conectado a ele e capaz de tornar o conteúdo informativo associado acessível e acionável. Precisa existir um fluxo de dados entre o mundo real e a sua contraparte virtual (e vice-versa) (GRIEVES, 2014). Inicialmente, o Gêmeo Digital (DT, do inglês *Digital Twin*), foi criado para abranger todo o ciclo de vida de um produto, desde seu *design* até a fabricação e, eventualmente, seu estágio de descarte (GRIEVES, 2014). O uso de DTs pode fornecer dados para um ambiente de simulação confiável, o que é especialmente importante antes de aplicar decisões em larga escala em redes físicas reais. Quando um DTN é criado, ele não deve apenas refletir os recursos da rede, mas também evoluir com a rede real em termos de atualizações de software e hardware, até o descarte da rede. O DTN pode servir como um espaço centralizado que coleta, armazena e processa informações globais do sistema físico (VAEZI *et al.*, 2022). Durante esse processo, o DTN ajuda a otimizar as operações e o gerenciamento da rede.

Como um caso de uso direto de construção de DTs, o modelo virtual de uma rede real pode ser duplicado e colocado dentro de roteadores. Isso fornece aos roteadores os estados atuais dos nós circundantes e os ajuda a tomar melhores decisões de roteamento e encaminhamento (WEI *et al.*, 2021). Ao analisar as condições de trabalho passadas e atuais, diagnosticar problemas potenciais, prever o desempenho futuro e ajudar a tomar decisões sobre mudanças na implantação da rede, operações e outros aspectos, o DTN não apenas influencia as operações da rede em tempo real, mas também evolui com a rede real ao longo de sua vida útil (VAEZI *et al.*, 2022). Na seção 2.1 são apresentadas as características dos elementos que compõem a RSFI utilizada nesta pesquisa. Na seção 2.2 são apresentados os conceitos utilizados para desenvolver os roteamentos da rede virtual, e na seção 2.3 são apresentados os conceitos que possibilitam identificar os nodos críticos da RSFI.

2.1 Elementos que compõem uma RSFI

A arquitetura de uma RSFI é composta por diferentes camadas e componentes, que juntos viabilizam a coleta, o processamento e a transmissão de dados em ambientes industriais. A compreensão da estrutura física e lógica dessas redes é fundamental para o desenvolvimento de soluções eficientes em automação e controle de processos. Cada elemento da RSFI desempenha um papel específico na manutenção da integridade e confiabilidade da comunicação, sendo essencial conhecer suas funções e interações para uma análise aprofundada do desempenho da rede. Os elementos principais de uma RSFI incluem dispositivos de campo, pontos de acesso, *gateways*, e um sistema de controle central. Essa estrutura permite a comunicação robusta e segura, essencial para ambientes industriais exigentes. Nas subseções a seguir, são descritos os dispositivos que compõem a estrutura da rede, bem como suas principais funções.

2.1.1 Gerenciador de Rede

O gerenciador de rede é responsável pela criação e manutenção da RSFI, bem como pela gestão dos dispositivos que a integram. O gerenciador de rede estabelece conexão direta com o *gateway*, o qual atua como intermediário, por meio do ponto de acesso, na comunicação entre os dispositivos de campo e as aplicações superiores. Entre as principais atribuições do gerenciador de rede destacam-se o provisionamento dos dispositivos, o monitoramento contínuo do estado da rede e a execução de funções críticas para o funcionamento eficiente do sistema (CHEN; NIXON; MOK, 2010). As atividades centrais associadas ao gerenciador são descritas a seguir:

Associação: denominado *Join Process*, constitui uma sequência de operações coordenadas pelo gerenciador de rede. A função do gerenciador é garantir que a inserção do novo dispositivo ocorra de forma compatível com os requisitos de escalonamento, roteamento e segurança. Embora a gestão do processo seja centralizada, sua inicialização parte do próprio dispositivo, mediante o envio de uma solicitação de ingresso. A agregação pode ser concluída com sucesso, resultar em falha, ou ser interrompida prematuramente. Inicialmente, o dispositivo realiza a sincronização com a rede, recebe pacotes de anúncio, formaliza a solicitação de ingresso e obtém as chaves de segurança. Em seguida, inicia-se a etapa de provisionamento, na qual o dispositivo recebe instruções de configuração provenientes do gerenciador, incluindo a escrita de *superframes*, *links* e grafos, além da definição de parâmetros temporais e outras variáveis operacionais. Após essa etapa, o dispositivo entra em um período de quarentena, no qual aguarda o estabelecimento de uma sessão com o *gateway* para se tornar plenamente funcional. Caso deseje publicar dados periodicamente, o dispositivo deverá solicitar esse serviço ao gerenciador, que, por sua vez, alocará os recursos necessários de largura de banda para a transmissão de dados.

Escalonamento: refere-se ao processo de alocação de *superframes* e *links* específicos

para cada dispositivo da rede, de forma a organizar sua participação nas comunicações. Embora normalmente executado durante o provisionamento inicial, esse processo pode ser reavaliado em função de mudanças na topologia da rede, como a adição de novos dispositivos ou a ocorrência de falhas. O escalonamento permite que cada dispositivo disponha de *slots* de tempo nos quais deverá atuar, seja transmitindo ou recebendo dados. Trata-se de uma tarefa complexa, pois requer a consideração de múltiplos fatores, incluindo a frequência de envio de dados por cada dispositivo, a prioridade das transmissões, a necessidade de redundância nos enlaces e demais características operacionais da rede.

Roteamento: Essa função diz respeito à construção e manutenção das rotas de comunicação entre os dispositivos da rede. O gerenciador de rede possui conhecimento completo da topologia da rede e, com base nisso, calcula e distribui rotas específicas para cada nó. O gerenciador mantém a tabela de roteamento global, enquanto os dispositivos individuais armazenam apenas subconjuntos dessa tabela, contendo as rotas que lhes são pertinentes. A construção dessas rotas baseia-se nas informações das listas de vizinhos, periodicamente reportadas pelos dispositivos, além de outras estatísticas sobre o estado da rede.

Diagnóstico da rede: O diagnóstico consiste na coleta e atualização contínua das informações sobre o estado da rede. Os dispositivos enviam periodicamente relatórios ao gerenciador contendo dados sobre vizinhos conectados (com *link*), vizinhos detectados (sem *link*), pacotes transmitidos e recebidos, status de alimentação e registros de falhas na recepção de pacotes.

Além das funções supracitadas, o gerenciador de rede é também responsável por diversas outras atividades associadas à segurança, manutenção e integridade da rede.

2.1.2 Gateway

O *gateway* desempenha a função central de interconectar os diversos dispositivos que compõem a rede, portanto, atua como elemento intermediário entre o gerenciador de rede, os pontos de acesso e o sistema de automação da planta. Sua principal responsabilidade é viabilizar a troca de dados entre esses elementos, de modo a permitir a integração entre os sistemas de controle e os dispositivos de campo. A comunicação entre o *gateway* e a automação da planta pode ser estabelecida por meio de diferentes protocolos e interfaces, conforme a arquitetura do sistema industrial (TANENBAUM, 2003). Essa comunicação pode atender a múltiplas finalidades, tais como: (i) a transmissão periódica de dados de processo e eventos, conforme ciclos de publicação previamente definidos; (ii) a notificação esporádica de falhas ou condições anômalas, geralmente associada a mensagens com elevada criticidade e baixa latência; e (iii) o envio de comandos de configuração e manutenção da rede, tipicamente executados de forma não frequente. Por meio dessa interface, as aplicações de supervisão e controle têm acesso transparente aos dispositivos da rede. Esta característica do *gateway* possibilita que sejam coletadas informações repetidamente,

e em momentos diferentes, com variados objetivos. Neste caso, algumas das informações obtidas da rede através do *gateway* são as informações pertinentes para a construção do DTN.

O *gateway* também exerce a função de conversor de protocolos, de modo a possibilitar a comunicação entre redes heterogêneas com diferentes padrões de comunicação. Adicionalmente, admite-se a conexão de múltiplos pontos de acesso ao mesmo *gateway*, o que proporciona maior confiabilidade operacional e aumento da largura de banda disponível para o tráfego de dados.

Outra função crítica atribuída ao *gateway* é a distribuição de tempo de rede. Ele atua como fonte primária de sincronização, propagando o relógio de referência por meio dos pontos de acesso. O ponto de acesso conectado diretamente ao *gateway* dissemina o sinal de tempo para os demais dispositivos da rede. Em arquiteturas com múltiplos pontos de acesso, cabe ao *gateway* garantir a sincronização entre os respectivos relógios, assegurando a coerência temporal necessária ao funcionamento determinístico da rede.

2.1.3 Ponto de Acesso

Os pontos de acesso são dispositivos responsáveis por estabelecer a conexão entre os nós sem fio presentes na planta industrial e o *gateway* da rede. Durante a fase de inicialização da rede, e antes da associação de quaisquer dispositivos de campo, o ponto de acesso desempenha o papel exclusivo de disseminador de pacotes de anúncio (*advertisement packets*), fundamentais para permitir que novos dispositivos identifiquem a rede e iniciem o processo de associação (*join process*). Assim, o ponto de acesso físico constitui a principal interface entre os dados trafegados na rede sem fio e o *gateway*, de modo a possibilitar a integração entre a camada de comunicação sem fio e as aplicações de supervisão e controle da rede industrial.

2.1.4 Dispositivos de Campo

Os dispositivos de campo são os elementos da rede responsáveis pela interface direta com a planta industrial, por meio da conexão a sensores e atuadores. Esses dispositivos podem ser alimentados por diferentes fontes de energia, tais como baterias, sistemas de colheita de energia (*energy harvesting*) ou conexão direta à rede elétrica, dependendo das características e restrições da aplicação.

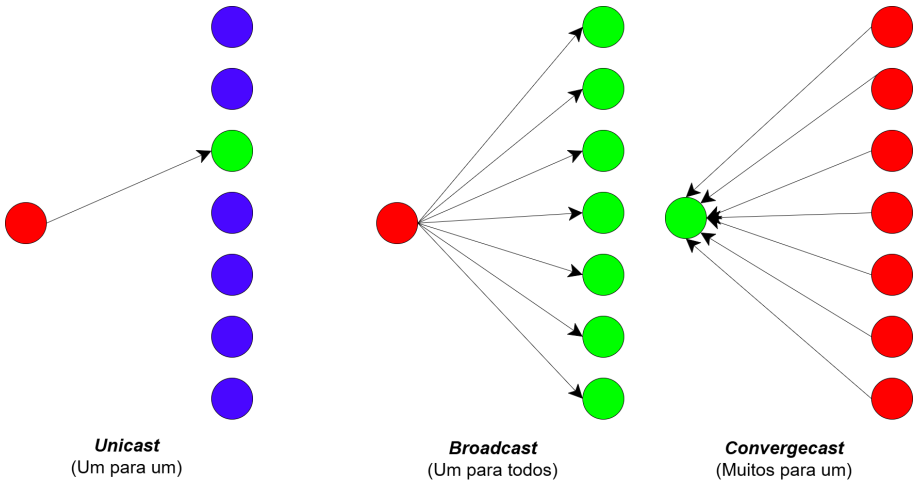
2.2 Tipos de Roteamento

O roteamento de dados em redes de comunicação desempenha um papel fundamental na eficiência e confiabilidade dos sistemas distribuídos, especialmente em contextos como redes de sensores sem fio, redes industriais e sistemas embarcados. A forma como os dados são transmitidos entre os dispositivos influencia diretamente o desempenho da rede, o

consumo energético e a latência das comunicações. Dentre os diversos métodos de roteamento existentes, destacam-se aqueles que organizam o fluxo de informações com base no padrão de comunicação exigido pela aplicação. Essa organização permite otimizar os recursos disponíveis e atender aos requisitos específicos de cada cenário.

Algumas das principais categorias de roteamento associadas ao fluxo de dados em redes incluem os modos *unicast* e *broadcast* para transmissão em uso disseminado dos dados (TANENBAUM, 2003). Neste trabalho, o foco da análise recai sobre o roteamento do tipo *convergecast*, que é semelhante ao roteamento *unicast*, porém, é um roteamento onde múltiplos dispositivos (não um só) enviam dados de forma agregada para um ponto central, pois ao considerar todos os pacotes transmitidos em RSFI, observa-se que a maior parte das comunicações de aplicação em controle de processos é de monitoramento, ou seja, *convergecast*. A Figura 2 destaca as diferenças entre os roteamentos, que serão explanadas a seguir.

Figura 2 – Diferença entre os roteamentos *unicast*, *broadcast* e *convercast*.



Fonte: autor.

2.2.1 *Unicast*

O roteamento *unicast* caracteriza-se, comumente, pela transmissão de mensagens originadas em um único nó com destino final a outro nó específico. Um exemplo típico é a comunicação entre o gerenciador de rede e sensores ou atuadores individuais, quando comandos específicos são direcionados. O roteamento *unicast* pode assumir diferentes formas, como (i) rotas *source*, no qual o nó emissor especifica detalhadamente, no cabeçalho da mensagem, o caminho ponto a ponto a ser seguido por todos os nós intermediários, (ii) rotas de grafo, no qual o nó de origem apenas define o destino final, e os nós intermediários tomam decisões de encaminhamento com base em grafos pré-configurados pelo gerenciador de rede e na qualidade atual dos enlaces, (iii) e rotas *proxy*, empregado no processo de associação (*join*) de novos dispositivos à rede, de modo a permitir que um

dispositivo já integrado atue como intermediário na comunicação com o novo nó.

2.2.2 *Broadcast*

No roteamento *broadcast*, mensagens originadas por um único nó são destinadas a múltiplos dispositivos da rede. Essa modalidade é comumente utilizada pelo gerenciador de rede e pelo *gateway*, especialmente em situações que exigem atualizações de configuração em larga escala, como a inclusão ou remoção de nós da rede. Nestes casos, torna-se necessário que os dispositivos atualizem suas tabelas de vizinhança e estruturas de roteamento de acordo com as novas topologias.

2.2.3 *Convergecast*

O roteamento *convergecast* é típico de arquiteturas de comunicação centralizadas, nas quais múltiplos nós da rede encaminham seus dados a um único destino. No contexto das RSFI, isso é comum porque, no controle de processos industriais, o que mais circula pela rede é monitoramento, ou seja, *convergecast*. Os dados são transmitidos por meio de enlaces *uplink* até um ou mais pontos de acesso conectados ao *gateway*. Esse mesmo padrão de tráfego é observado em aplicações de monitoramento, nas quais dados coletados por sensores são enviados ao *gateway* da rede. Em redes de grande escala, a presença limitada ou a distribuição ineficiente de pontos de acesso pode provocar gargalos e aumento da taxa de perda de pacotes, uma vez que a capacidade de recepção do ponto de acesso pode se tornar um fator limitante (ZATS *et al.*, 2011).

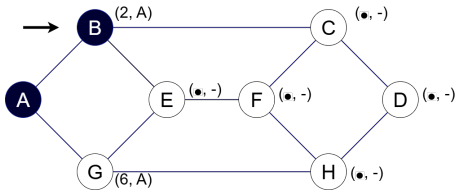
O algoritmo de Dijkstra é uma técnica clássica de roteamento utilizada para determinar o caminho mais curto entre dois nós em um grafo. A métrica utilizada para o cálculo de distância pode variar conforme o objetivo da aplicação. Em RSFI, diversos parâmetros podem ser utilizados para mensurar a qualidade de um enlace de comunicação, entre os quais se destacam o *Received Signal Strength Indicator* (RSSI), o *Link Quality Indicator* (LQI), o *Packet Delivery Ratio* (PDR) e o *Received Signal Level* (RSL). O RSSI mede a potência do sinal recebido, refletindo diretamente a intensidade com que o sinal chega ao receptor, enquanto o LQI fornece uma estimativa da qualidade do enlace considerando fatores como ruído e interferência. Já o PDR representa a taxa de sucesso na entrega de pacotes, sendo um indicador de confiabilidade global do enlace. O presente trabalho adota o parâmetro RSL por este ser amplamente empregado em aplicações industriais compatíveis com redes de campo, permitindo uma análise mais direta do nível de sinal efetivamente percebido pelos dispositivos de campo. Além disso, o RSL oferece uma métrica quantitativa e padronizada para correlacionar o desempenho físico do enlace com o comportamento lógico da rede, servindo como base para o processo de virtualização e posterior implementação do DTN.

Para o algoritmo de Dijkstra, inicialmente nenhum caminho é conhecido. Todos os nós recebem rótulos com valor infinito, exceto o nó de origem, que é marcado como per-

manente com custo zero. À medida que o algoritmo avança, os rótulos provisórios dos nós são atualizados com base nos menores custos encontrados, até que se tornem permanentes, refletindo os caminhos mais curtos. Um rótulo, uma vez tornado permanente, não é mais modificado (TANENBAUM, 2003). O processo começa com o nó de origem, marcado como ativo. Em seguida, cada vizinho adjacente é analisado, e seus rótulos são atualizados de acordo com o custo de transição a partir do nó ativo. Após essa etapa, o algoritmo busca, entre todos os nós ainda com rótulos provisórios, aquele com o menor custo acumulado, que então se torna o novo nó ativo e é marcado como permanente. Este processo é repetido iterativamente até que todos os caminhos tenham sido estabelecidos.

A Figura 3 ilustra uma aplicação do algoritmo na busca do caminho mais curto entre os nós A e D. Na primeira iteração, foram avaliados todos os vizinhos do nó A (inicialmente ativo), e o nó B foi identificado como o próximo com menor custo, passando então à condição de ativo. Os caminhos ainda não explorados permanecem com custo infinito até que sejam descobertos e processados nas iterações seguintes.

Figura 3 – Primeiro caminho encontrado no cálculo do caminho mais curto de A até D. A seta indica o atual nó ativo.



Fonte: Adaptado de (TANENBAUM, 2003).

2.2.4 Roteamento em RSFI: exemplo WH

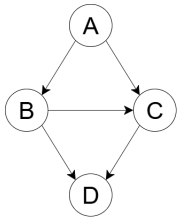
Existem diversas estratégias de roteamento, cada uma projetada para atender a diferentes requisitos de desempenho, como confiabilidade, latência e eficiência. Em redes em malhas, o roteamento pode ser tanto *unicast* (de um para um), *multicast* (de um para muitos) ou *broadcast* (de um para todos) a depender da aplicação e do protocolo de roteamento utilizado. Tipicamente, numa RSFI, múltiplos métodos de roteamento são suportados, entre eles o roteamento de origem (*source routing*), o roteamento baseado em grafos (*graph routing*) e o roteamento por *superframe*. Além disso, o roteamento por *proxy* é utilizado no processo de associação de novos dispositivos à rede. Como exemplo de RSFI, o protocolo *Wireless*HART (WH) suporta os seguintes roteamentos:

- O **Roteamento de origem** é direto; a rota completa entre o remetente e o destinatário é inserida diretamente no cabeçalho da mensagem. Cada dispositivo intermediário simplesmente encaminha o pacote ao próximo nó especificado na rota. Essa abordagem é comumente empregada pelo gerenciador de rede, que possui conhecimento completo da topologia da rede e, portanto, é capaz de construir rotas

otimizadas. Para que um dispositivo utilize o roteamento de origem, ele deve ser previamente configurado pelo gerenciador de rede. Como exemplo, um protocolo pode incluir comandos de escrita de rota por meio do qual a rota completa é armazenada no dispositivo, associando-se ao endereço de destino por meio do comando de escrita de rota. Durante o encaminhamento, o dispositivo consulta as rotas configuradas e, se encontrar uma rota do tipo origem, procede com o roteamento correspondente;

- No **Roteamento de Grafos**, as mensagens são encaminhadas com base em um identificador de grafo (ID), codificado em dois *bytes* no cabeçalho do pacote. Cada ID representa um grafo direcionado, em que os vértices correspondem aos dispositivos da rede e as arestas representam enlaces de transmissão válidos entre pares de nós. O grafo é definido e mantido pelo gerenciador de rede, que distribui aos dispositivos participantes informações relativas ao ID do grafo, bem como os endereços dos vizinhos que constituem seus destinos válidos (arestas de saída). Ao encaminhar uma mensagem, o dispositivo seleciona o primeiro *link* disponível que esteja associado a uma aresta do grafo, independentemente de qual vizinho se trate. Caso o dispositivo também transmita dados próprios através do grafo, ele deve conhecer previamente o endereço de destino associado àquela estrutura. Para garantir o funcionamento correto do roteamento baseado em grafos, todos os caminhos devem convergir para um único destino, sendo responsabilidade do gerenciador de rede assegurar a consistência da estrutura. Embora o padrão não proíba explicitamente a presença de *loops* em um grafo, estes devem ser evitados, uma vez que podem comprometer a entrega pontual das mensagens e gerar tráfego indefinido na rede. Como exemplificado na Figura 4, um grafo formado pelos dispositivos A, B, C e D, com cinco arestas direcionais, permite que o nó B encaminhe mensagens para C ou D. Uma mensagem originada em A, contendo o ID do grafo, pode ser encaminhada sequencialmente por B e C até atingir o destino D;

Figura 4 – Roteamento de Grafo.



Fonte: Adaptado de (FOUNDATION, 2008).

- O **Roteamento Misto**, é uma abordagem em que as informações referentes tanto ao roteamento por origem quanto ao roteamento baseado em grafos são codificadas em campos distintos no cabeçalho da mensagem da camada de rede, e podem

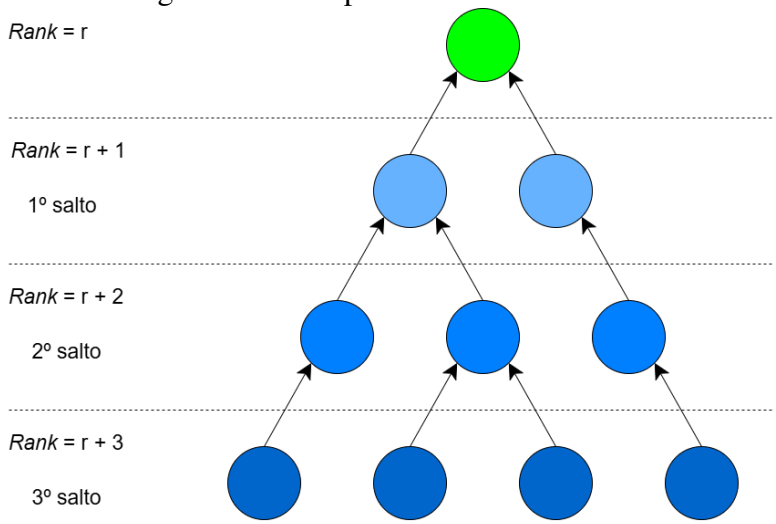
coexistir em uma única transmissão. Essa flexibilidade proporciona maior resiliência ao encaminhar dados, de modo a aumentar as chances de sucesso na entrega das mensagens. Caso uma rota se torne inviável, o dispositivo intermediário pode optar por um método de roteamento alternativo. O protocolo também prevê regras específicas para simplificar determinadas situações. Por exemplo, quando o destino da mensagem é um vizinho direto, o dispositivo pode desconsiderar a estratégia de roteamento definida no cabeçalho e encaminhar a mensagem diretamente ao nó de destino.

- Uma forma especializada de roteamento de grafos é chamada **Roteamento de *Superframe***. Essa técnica é uma especialização do roteamento baseado em grafos, na qual as mensagens são encaminhadas com base no identificador do *superframe* embutido no cabeçalho da mensagem. O *superframe* é previamente configurado pelo gerenciador de rede, que distribui aos dispositivos participantes as informações sobre os enlaces e a estrutura do *superframe*. Cada dispositivo envolvido em algum enlace deve ser informado sobre os parâmetros do *superframe* a que pertence. Durante o encaminhamento, o dispositivo seleciona o primeiro enlace de transmissão normal disponível no *superframe*, independentemente de qual vizinho será alcançado. Caso um dispositivo transmita dados próprios através do roteamento por *superframe*, ele também deve conhecer o endereço do destino final associado àquela estrutura. Por exemplo, para aplicar roteamento por *superframe* ao cenário ilustrado na Figura 4, um *superframe* pode ser configurado contendo cinco enlaces principais: A para B, A para C, B para C, B para D e C para D;

Para que qualquer forma de roteamento seja viável, é necessário que exista uma sessão ativa entre os dispositivos de origem e destino. Com o intuito de manter elevada a segurança, a criação de sessões entre dispositivos é evitada, uma vez que isto permitiria a geração e consumo de mensagens de aplicação sem passar pelo *gateway*. E toda comunicação entre o gerenciador de rede e os dispositivos passa, obrigatoriamente, pelo *gateway*. Convencionalmente, utiliza-se o termo *uplink* para se referir ao caminho da comunicação em direção ao *gateway*, enquanto o termo *downlink* é empregado para designar a direção oposta, ou seja, do *gateway* para os dispositivos de campo.

Neste trabalho, dois roteamentos foram estudados e implementados. Ambos consideram pesos para cada *link* da rede, que pode se referir a algum dado equivalente, como o RSL recebido por cada vizinho. São eles o algoritmo Dijkstra, que já foi brevemente descrito em 2.2.3, e o algoritmo *Routing Protocol for Low power and Lossy Networks* (RPL) que é voltado para sistemas alimentados à bateria (eletrônica de baixo consumo), enquanto mantém alto o PDR. O algoritmo RPL constrói rotas em topologia de árvore, e busca o balanceamento estrutural das cadeias de comunicação. O custo associado a cada *link* é calculado conforme definido na Equação (1), proposta em (ZATS *et al.*, 2011), e

Figura 5 – Exemplo de roteamento RPL.



Fonte: autor.

cada nodo é classificado em *ranks* de acordo com a quantidade de saltos necessários para enviar um pacote ao destino, conforme apresentado na Figura 5.

Uma das principais métricas utilizadas é a Contagem Esperada de Transmissões (ETX, do inglês *Expected Transmission Count*), que representa a média de tentativas necessárias para que uma transmissão entre dois nós seja bem-sucedida. O valor de ETX é obtido a partir dos dados empíricos coletados da rede, e é definido como o inverso do PDR. Por exemplo, se a taxa de entrega entre dois dispositivos for de 80%, o ETX será igual a 1,25. Este valor indica que, em média, são necessárias 1,25 tentativas para que uma transmissão seja concluída com êxito. Durante a execução do algoritmo, o termo $Custo_{vizinho}$ é atualizado iterativamente. Cada dispositivo avalia os possíveis *links* com seus vizinhos e calcula o custo de cada enlace como a soma entre a classificação do vizinho e o ETX correspondente (termos $Custo_{vizinho}$ e $ETX_{vizinho}$ na Equação 1). Em seguida, o dispositivo seleciona o *link* com menor custo acumulado e atualiza sua própria classificação com base nesse valor. Adicionalmente, o modelo incorpora um fator de balanceamento de carga baseado na distribuição de dispositivos entre os pontos de acesso. Esse fator é representado pelo termo $Carga_{PA}$, definido como a proporção de dispositivos conectados a um determinado ponto de acesso em relação ao total de dispositivos da rede. Para ponderar sua influência no cálculo do custo total, esse termo é multiplicado por uma constante λ, que tem por finalidade ajustar a relevância do balanceamento no processo de otimização. O valor de λ é arbitrado como sendo a média dos custos dos nós em uma execução prévia do algoritmo sem balanceamento de carga, de modo a evitar a superestimação ou subestimação desse fator na definição das rotas.

$$Custo_{link} = Custo_{vizinho} + ETX_{vizinho} + \lambda * Carga_{PA} \quad (1)$$

Como é possível analisar, ambos os algoritmos são semelhantes e pertencem ao mesmo

grupo, porém o RPL considera mais características intrínsecas à rede sem fio, e por isso define os *links* baseados em mais informações inerentes à rede.

2.2.5 Confiabilidade de RSFI

A confiabilidade em RSFI é usualmente definida como a razão entre o número de pacotes entregues com sucesso aos seus respectivos destinos finais e o total de pacotes gerados na rede, conforme proposto em (ZATS *et al.*, 2011) e representado pela Equação (2). Nessa equação, o parâmetro θ representa a confiabilidade da rede, enquanto p_{suc} e p_{per} correspondem, respectivamente, ao número total de pacotes entregues com sucesso e ao número total de pacotes perdidos durante a transmissão fim-a-fim.

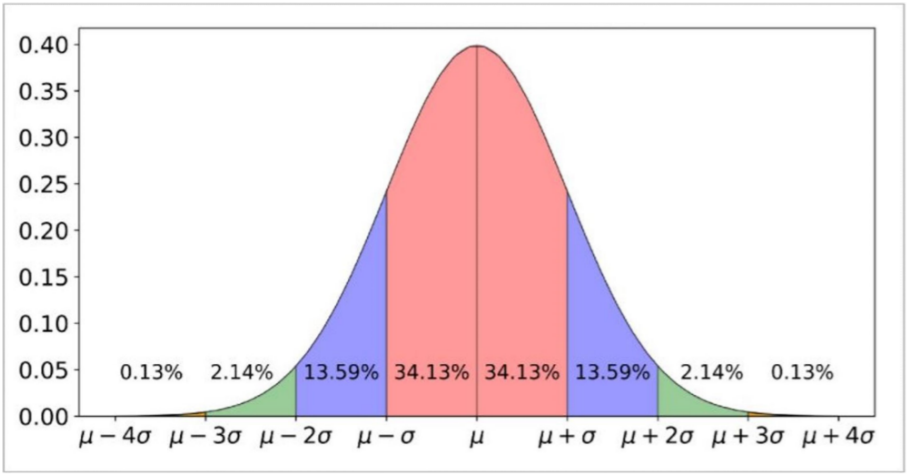
$$\theta = \frac{p_{suc}}{p_{per} + p_{suc}} \tag{2}$$

Como critério para o descarte definitivo de pacotes na simulação e, consequentemente, para a caracterização de perda de confiabilidade na rede, foram adotadas duas abordagens amplamente reconhecidas que serão detalhadas com a devida contextualização e exemplificação: a obsolescência de pacotes baseada no TTL (*Time to Live*) e o esgotamento da capacidade de armazenamento do *buffer* nos dispositivos de campo.

Numa rede TDMA, geralmente, cada pacote gerado pela rede é associado a um carimbo temporal denominado *Absolute Slot Number* (ASN), que registra o *slot* exato em que o pacote foi criado. Com base no ASN atual e no valor de ASN do pacote, os dispositivos podem calcular a "idade" do pacote em unidades de *slots*. O TTL, por sua vez, é um parâmetro específico de cada pacote que define a idade máxima em que este ainda será considerado válido. Ao comparar a idade atual do pacote com seu TTL, os dispositivos decidem se devem descartá-lo, evitando o consumo de recursos com pacotes obsoletos. Adicionalmente, perdas ocasionadas por *buffer* cheio ocorrem quando o dispositivo não possui mais espaço disponível para armazenar ou processar novos pacotes. Cada dispositivo possui uma capacidade limitada de *buffer*, sendo que a retenção prolongada de pacotes pode levá-los à obsolescência. O modelo adotado para gerenciamento da fila de pacotes é do tipo *First In, First Out* (FIFO). Nesse contexto, falhas sucessivas na transmissão de um pacote resultam no bloqueio do fluxo de saída da fila, e levam ao acúmulo de pacotes provenientes de nós vizinhos ou gerados localmente. Caso novos pacotes sejam recebidos ou gerados enquanto não há espaço livre no *buffer*, estes são automaticamente descartados. Quando o pacote descartado por saturação do *buffer* é proveniente do próprio dispositivo, não há alternativas além de sua eliminação definitiva, o que compromete diretamente a confiabilidade da rede. Esse evento caracteriza uma perda irreversível, refletindo falhas na capacidade do sistema de manter o desempenho esperado.

No contexto de RSFI, a confiabilidade é uma das principais métricas associadas ao determinismo, entendido como a garantia de que o sistema irá operar dentro dos limites de desempenho esperados, desde que as condições de operação permaneçam dentro

Figura 6 – Densidade probabilística em função da média μ e do desvio padrão σ.



Fonte: (TENNANT, 2001).

dos parâmetros definidos (CHEN *et al.*, 2014). Em redes de comunicação, o determinismo refere-se à capacidade da rede de entregar informações dentro do tempo previsto, mantendo uma frequência de atualização constante. Isso implica baixa taxa de perda de pacotes, variação mínima na latência (*jitter*) e regularidade nas atualizações.

Fenômenos associados ao desempenho da rede, como perda de pacotes ou atraso, podem ser modelados estatisticamente por meio de uma distribuição normal. A função densidade de probabilidade de um fenômeno $f(x)$ pode ser expressa conforme a Equação (3), em que μ representa a média e σ o desvio padrão da variável aleatória considerada (PAPOULIS; PILLAI, 2001).

$$f(x) = \frac{1}{\sigma\sqrt{(2\pi)}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2} \tag{3}$$

A curva de uma distribuição normal pode ser demonstrada em função de μ e σ, como mostra o gráfico apresentado na Figura 6. A partir deste gráfico, infere-se que para cada subdivisão da curva normal há uma porcentagem de dados que corresponde à área sobre a curva normal. Os dados com desvio de até 1σ acima ou abaixo da média representam um total de, aproximadamente, 68,26% da área sobre a curva, os dados com desvio de até 2σ acima ou abaixo da média representam um total de, aproximadamente, 95,44% da área sobre a curva, e assim por diante.

A métrica de confiabilidade de redes é comumente descrita em função de σ, que é um indicador de desvio padrão de uma distribuição normal. Segundo o teorema do limite central, sob determinadas condições, a distribuição da média de variáveis aleatórias independentes tende à normalidade, independentemente da distribuição original das variáveis, conforme (4), onde n é o tamanho amostral.

$$\overline{X} \sim N(\mu, \frac{\sigma}{\sqrt{n}}) \tag{4}$$

Tabela 1 – Densidade probabilística em função da quantidade de desvios padrões

Desvios Padrões σ	Densidade Probabilística
$\pm\sigma$	68,26%
$\pm 2\sigma$	95,44%
$\pm 3\sigma$	99,72%
$\pm 4\sigma$	99,98%

Fonte: adaptado de (TENNANT, 2001).

Na avaliação do desempenho de redes industriais, observa-se a presença de diversos fatores interferentes, que incluem ruídos no meio físico e erros de medição. Em razão dessa variabilidade, e do princípio estatístico da agregação de múltiplos fatores aleatórios, admite-se que o comportamento global da rede tende a seguir uma distribuição normal à medida que o número de amostras aumenta.

2.3 Centralidades

As técnicas de centralidade em redes surgiram no contexto da teoria dos grafos e da análise de redes sociais, inicialmente associadas aos trabalhos de Leonhard Euler no século XVIII, com a formalização de grafos, e consolidadas no século XX a partir de estudos em sociologia matemática, estatística e ciência das redes (HARARY, 1972). A partir da década de 1950, pesquisadores passaram a empregar métricas de centralidade para quantificar a importância relativa de vértices em estruturas complexas, especialmente para compreender padrões de influência, fluxo de informação e conectividade em redes sociais, biológicas e de transporte (FREEMAN, 1979).

Com o avanço das redes complexas e da capacidade computacional, o uso de métricas de centralidade foi gradualmente estendido para áreas como telecomunicações e redes de computadores, sobretudo a partir das décadas de 1990 e 2000 (DE ARAÚJO; BASTOS-FILHO; MARTINS-FILHO, 2014) (AUSIELLO; FIRMANI; LAURA, 2013). Nesse período, o crescimento das redes sem fio e *ad hoc* estimulou a adoção dessas métricas como ferramentas analíticas para avaliar robustez, tolerância a falhas e eficiência de roteamento. Em particular, a modelagem de redes como grafos ponderados permitiu associar atributos físicos, como qualidade de enlace e distância, às análises estruturais tradicionalmente abstratas.

No contexto das RSFI, o uso sistemático de técnicas de centralidade passou a ganhar relevância com a consolidação de padrões como o WirelessHART e o ISA100, que operam em topologias malhadas e altamente dinâmicas. A partir da década de 2010, diversos estudos passaram a empregar métricas de centralidade para identificar nós críticos, gargalos de comunicação e pontos vulneráveis da rede, sobretudo em cenários onde confiabilidade, determinismo temporal e eficiência energética são requisitos fundamentais (TIMM,

2022). Nessas aplicações, as métricas de centralidade auxiliam tanto no diagnóstico do desempenho da rede quanto no planejamento de intervenções estruturais.

A centralidade de grau é uma das métricas mais elementares e mede o número de conexões diretas associadas a um nó. Em RSFI, essa métrica está relacionada à densidade local de conectividade e pode indicar dispositivos que atuam como concentradores de tráfego ou repetidores naturais. Embora simples, a centralidade de grau fornece informações relevantes sobre a redundância de enlaces e a capacidade de um nó em oferecer caminhos alternativos, o que impacta diretamente a confiabilidade da comunicação em topologias malhadas.

Por sua vez, a centralidade de intermediação e a centralidade de proximidade oferecem uma visão mais global da rede. A centralidade de intermediação quantifica o quanto um nó participa dos caminhos mínimos entre pares de nós, sendo particularmente útil para identificar dispositivos cuja falha pode provocar degradação significativa no desempenho da rede. Já a centralidade de proximidade avalia a distância média de um nó em relação aos demais, refletindo sua eficiência potencial na disseminação de informações. Em RSFI, ambas as métricas são amplamente utilizadas para apoiar estratégias de roteamento, posicionamento de dispositivos e definição de intervenções, especialmente quando integradas a abordagens mais recentes, como o conceito de DTN, no qual a análise estrutural orienta decisões antes da aplicação no ambiente físico.

As cadeias de comunicação *uplink* com maior propensão à perda de pacotes não são, necessariamente, aquelas compostas por dispositivos fisicamente mais distantes ou com maior número de saltos até os pontos de acesso. Os maiores índices de perda tendem a ocorrer em cadeias mais suscetíveis à formação de gargalos, especialmente aquelas que dependem de um número reduzido de nós localizados nas proximidades dos destinos finais.

Nesse contexto, a análise da centralidade torna-se uma ferramenta relevante. Trata-se de um conceito originado da Teoria dos Grafos e amplamente utilizado na análise de redes complexas, como redes sociais, epidemiológicas, neurais e de comunicação. A centralidade tem por objetivo quantificar o grau de importância de cada vértice (ou nodo) em relação à estrutura global da rede (BONACICH, 1987). Essa abordagem permite identificar e classificar os elementos mais influentes dentro da topologia da rede (BORGATTI, 2005).

As métricas de centralidade utilizadas neste trabalho são: Centralidade de Grau (CG), Centralidade de Proximidade (CP) e Centralidade de Intermediação (CI). A CG quantifica a quantidade de conexões diretas de um nó em relação ao total possível (se estivesse conectado a todos os outros dispositivos da rede). A CP mede a distância média de um nó em relação a todos os demais, de modo a refletir sua acessibilidade na rede. Por sua vez, a CI avalia a frequência com que um determinado nó atua como intermediário nos caminhos mais curtos entre outros pares de nós, o que destaca seu papel como elo de

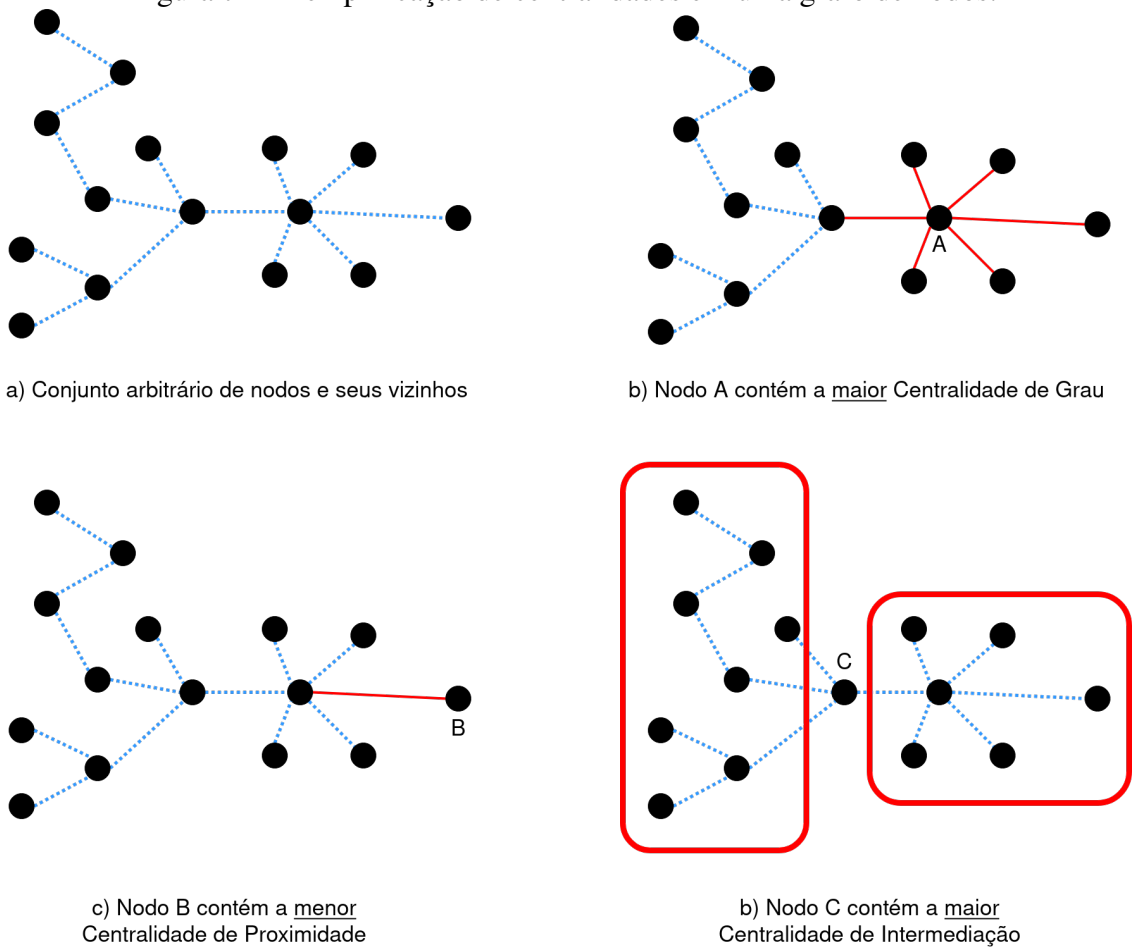
ligação entre diferentes regiões da rede.

Este trabalho propõe a aplicação dessas métricas de centralidade na análise da distribuição espacial dos dispositivos, bem como na estrutura de *links* e no balanceamento da carga de tráfego nos pontos de acesso, com o intuito de aprimorar o desempenho da rede. Ressalta-se que os valores obtidos por meio da análise de centralidade possuem caráter relativo, ou seja, são úteis para comparações dentro do contexto da rede analisada, como, por exemplo, para identificar se um nó apresenta maior relevância topológica em comparação a outro. No entanto, os valores absolutos de centralidade não têm, isoladamente, valor interpretativo significativo (GUTIéRREZ GAITáN *et al.*, 2021).

É importante destacar que as métricas de centralidade aplicadas neste trabalho não dependem diretamente do desempenho observado da rede, uma vez que são baseadas exclusivamente na estrutura de roteamento estabelecida. Portanto, tais métricas podem ser computadas a partir das informações obtidas durante a etapa de definição de rotas, conforme representado na Figura 7.

As três variantes de centralidade adotadas neste estudo seguem as definições propostas em (BONACICH, 1987), (BORGATTI, 2005) e (GUTIéRREZ GAITáN *et al.*, 2021).

Figura 7 – Exemplificação de centralidades em uma grafo de nodos.



Fonte: Adaptado de (TIMM, 2022).

2.3.1 Centralidade de Grau

A CG é considerada uma das métricas de centralidade mais simples e amplamente utilizadas na análise de redes (GUTIéRREZ GAITáN *et al.*, 2021). Essa medida é definida com base no número de conexões diretas (*links*) que um determinado nó mantém com outros nós da rede, em relação ao número máximo possível de conexões que esse nó poderia possuir se estivesse conectado a todos os demais dispositivos da rede. A Equação (5) apresenta o cálculo da CG para um nó i, onde N representa o número total de nós na rede e $grau(i)$ indica a quantidade de *links* diretamente associados ao nó i.

$$CG_i = \frac{grau(i)}{N-1} \tag{5}$$

No contexto dos estudos de caso realizados neste trabalho, a análise da CG visa investigar seu impacto na disponibilidade dos pontos de acesso e na carga de comunicação dos dispositivos adjacentes. A hipótese avaliada é que valores elevados de CG estão associados a nós com maior número de vizinhos diretos, os quais tendem a desempenhar papéis centrais na topologia da rede, de modo a contribuir para a formação de gargalos de comunicação.

A CG, conforme expressa na Equação (5), quantifica de forma relativa o número de conexões diretas que um determinado nó possui nas rotas primárias de *uplink*, em comparação com o número máximo possível de conexões que esse nó poderia estabelecer com os demais dispositivos da rede. Na Figura 7, observa-se que, no conjunto arbitrário de nós representado no detalhe 7.a, o nó com maior CG é o nó A, como destacado no detalhe 7.b, dado que nenhum outro vértice no grafo apresenta a mesma quantidade de conexões diretas.

Apesar de representar uma das formas mais simples de centralidade, a CG fornece informações relevantes para a análise da topologia de comunicação. Como os nós com menor custo de ETX tendem a ser preferidos nas seleções de rota, eles acumulam mais conexões diretas e, portanto, tornam-se pontos críticos na estrutura de *uplink*. A combinação da análise de CG com a CI possibilita uma avaliação mais abrangente dos possíveis gargalos da rede, tanto sob a perspectiva das conexões diretas quanto da recorrência de um nó como elo intermediário nas cadeias de transmissão de dados.

2.3.2 Centralidade de Proximidade

A CP tem como objetivo quantificar o quão central é um determinado nó em relação aos demais nós da rede, com base em sua acessibilidade topológica. Essa métrica é definida como o inverso da soma das distâncias geodésicas entre um nó i e todos os demais nós pertencentes ao grafo V, conforme expresso na Equação (6), em que $a \in V$ representa qualquer nó pertencente ao conjunto de vértices da rede, e $dist(i, a)$ corresponde à distância geodésica entre os nós i e a.

Neste trabalho, a métrica tradicional de distância física entre nós é substituída por uma medida relativa baseada na probabilidade de perda de pacotes. Assim, distâncias relativas mais elevadas são atribuídas a enlaces com maior propensão à perda, de modo a refletir a degradação na qualidade da comunicação. Essa adaptação permite que a CP seja aplicada de forma mais aderente às características específicas das RSFI analisadas. O ETX, definido como o inverso da Probabilidade de Entrega de Pacotes (PDP, do inglês *Packet Delivery Probability*), indica a quantidade média de tentativas de transmissão necessárias para que um pacote seja entregue com sucesso. Por representar diretamente a viabilidade de uma conexão entre dois dispositivos, o ETX é utilizado como base para o cálculo da CP, e assim substitui a métrica de distância geodésica tradicional.

$$CP_i = \frac{1}{\sum_{a \in V} dist(i, a)} \tag{6}$$

Nos estudos de caso desenvolvidos, busca-se examinar em que medida a CP dos pontos de acesso influencia os índices de perda de pacotes ponto a ponto. A hipótese considerada é que valores mais elevados de CP estão associados a nodos com melhor acessibilidade topológica, o que tende a reduzir a ocorrência de ramificações excessivas nas cadeias de comunicação *uplink*, contribuindo assim, para uma maior eficiência na transmissão dos dados.

A CP, conforme proposta e expressa na Equação (6), quantifica o quão próximo um determinado nó está em relação aos demais, sendo definida como o inverso da soma das distâncias geodésicas até os demais nós da rede. Trata-se, portanto, de uma métrica relativa de acessibilidade topológica. No exemplo ilustrado na Figura 7, considerando o conjunto arbitrário de nós representado no detalhe 7.a, o nó B, evidenciado no detalhe 7.c, apresenta a menor CP, por estar relativamente mais afastado da maioria dos demais nós da topologia.

2.3.3 Centralidade de Intermediação

A CI é uma métrica que quantifica a importância de um nó com base em sua função como intermediário nas rotas de comunicação entre pares de nós em uma rede. Em termos práticos, a CI representa a frequência com que um determinado dispositivo aparece nas rotas mais curtas entre outros nós da rede. Ou seja, quanto mais frequentemente um nó é utilizado como passagem obrigatória em rotas primárias estabelecidas pelo algoritmo de roteamento, maior será sua CI. A Equação (7) formaliza esse cálculo, onde $rotas_i(p, q)$ corresponde ao número de rotas entre os nós p e q que passam pelo nó i, e $rotas(p, q)$ representa o total de rotas existentes entre esses dois nós.

$$CI_i = \sum_{p \neq q} \frac{rotas_i(p, q)}{rotas(p, q)} \tag{7}$$

Nos estudos de caso deste trabalho, a CI é adotada como critério principal para a iden-

tificação de nós com potencial para se tornarem gargalos na comunicação da rede. Dispositivos com alta CI tendem a concentrar grande volume de tráfego, sendo, portanto, mais críticos para o desempenho global da rede. A ocorrência de falhas ou perdas significativas nesses dispositivos pode comprometer múltiplas rotas simultaneamente, desencadeando efeitos em cascata, como o acúmulo de mensagens em *buffers* e o aumento da latência na entrega de dados de diversos outros dispositivos.

A CI, conforme expressa na Equação (7), representa uma métrica relativa que quantifica a importância de um determinado nó enquanto elo de ligação entre pares de nós na rede. Em outras palavras, essa métrica indica a frequência com que um nó atua como intermediário nas rotas de comunicação entre outros dois nós distintos, refletindo seu papel na conectividade geral da topologia. No exemplo ilustrado na Figura 7, considerando o conjunto arbitrário de nós apresentado no detalhe 7.a, o nó C, evidenciado no detalhe 7.d, exibe a maior CI, por ser o principal ponto de interligação entre dois subconjuntos distintos de nós, funcionando como uma ponte essencial para o tráfego de dados entre eles.

Para obtenção da CI na simulação, a ferramenta percorre todas as cadeias de roteamento *uplink* da rede, identifica assim a presença de cada nó nas rotas entre diferentes pares de origem e destino. Essa abordagem fornece uma medida objetiva do quanto determinado nó é estratégico para o escoamento de dados na rede. Nós com elevada CI são particularmente relevantes para a manutenção da eficiência das rotas de *uplink*, pois concentram uma parcela significativa do tráfego. Sua falha, congestão ou saturação pode comprometer o desempenho de diversos nós subordinados na topologia, especialmente em relação a perdas de pacotes causadas por *buffer* cheio ou obsolescência decorrente de atrasos sucessivos. Além disso, a análise combinada da CI com a CG permite identificar os nós que, simultaneamente, concentram um elevado número de conexões diretas e exercem papel de elo crítico entre diferentes segmentos da rede. Esses nós são considerados pontos de vulnerabilidade para o desempenho global, sendo, portanto, alvos prioritários para estratégias de balanceamento de carga e resiliência na comunicação.

2.4 Gêmeo Digital

O conceito de DT tem origem no início dos anos 2000, no contexto do gerenciamento do ciclo de vida de produtos. Segundo (GRIEVES; VICKERS, 2016), a ideia fundamental consiste na criação de uma representação digital informacional que espelha um sistema físico real, estabelecendo uma correspondência contínua entre ambos ao longo de todo o seu ciclo de vida. Essa representação virtual não se limita a um modelo estático, mas constitui uma entidade dinâmica, capaz de evoluir em paralelo ao sistema físico, refletindo suas características, estados operacionais e histórico de alterações. A formulação inicial do DT foi apresentada em 2002 como um modelo conceitual que integrava espaço físico e espaço virtual, conectados por fluxos bidirecionais de dados e informações. Esse mo-

delo, inicialmente denominado *Mirrored Spaces Model* ou *Information Mirroring Model*, estabelecia que todo sistema físico deveria possuir um correspondente virtual contendo todas as informações relevantes para sua descrição, operação e análise. A consolidação do termo *Digital Twin* ocorreu posteriormente, à medida que o conceito foi ampliado e aplicado a sistemas complexos, especialmente em ambientes industriais e aeroespaciais.

No âmbito conceitual, o DT é definido como um conjunto de construções virtuais capazes de descrever completamente um produto físico, desde o nível microestrutural até o macrogeométrico (GRIEVES; VICKERS, 2016). Esse conceito é desdobrado em diferentes manifestações, incluindo o protótipo de DT, que representa o artefato ainda na fase de concepção, e a instância de DT, que corresponde a uma instância física específica em operação. Além disso, o DT agregado permite a análise conjunta de múltiplas instâncias, viabilizando estudos estatísticos, prognósticos e análises de confiabilidade em larga escala.

Um dos principais diferenciais do DT reside na sua capacidade de apoiar análises preditivas e interrogativas ao longo do ciclo de vida do sistema. Durante a fase de criação, o ambiente virtual permite simular comportamentos, identificar falhas emergentes e avaliar cenários que seriam inviáveis ou excessivamente custosos no domínio físico. Já na fase operacional, a integração contínua entre sensores do sistema real e o modelo virtual possibilita o monitoramento em tempo real, a previsão de falhas e a tomada de decisões baseada em dados históricos e estados futuros estimados. Por fim, o modelo de DT estende-se até as fases finais do ciclo de vida, incluindo a manutenção, o suporte e o descarte do sistema. A preservação do conhecimento acumulado no ambiente virtual permite não apenas otimizar a operação de sistemas em uso, mas também retroalimentar projetos futuros, reduzindo falhas recorrentes e impactos ambientais associados ao descarte inadequado.

O DTN aplicado às RSFI consiste na virtualização da infraestrutura de comunicação, incluindo topologia, enlaces, métricas de desempenho e mecanismos de roteamento, de forma a espelhar o comportamento da rede física em um ambiente computacional. Diferentemente de um DT tradicional focado em ativos individuais, o DTN tem como objeto de estudo o sistema de comunicação como um todo, permitindo a análise integrada das interações entre dispositivos, fluxos de dados e condições de operação da rede industrial.

Em RSFI, o DTN é construído a partir da coleta contínua de dados provenientes da rede real, tais como RSL, taxas de perda de pacotes, contadores de falhas, estados de *buffer* e informações de vizinhança. Esses dados alimentam o modelo virtual, que passa a representar com maior fidelidade as condições reais de propagação, conectividade e carga da rede. Dessa forma, o DTN deixa de ser uma abstração puramente teórica e passa a atuar como uma réplica operacional, capaz de reproduzir fenômenos como enlaces instáveis, congestionamentos e falhas intermitentes.

DTN em RSFI possibilita simular intervenções antes de sua aplicação na rede física.

Por meio do ambiente virtual, é possível avaliar diferentes estratégias de roteamento, testar a adição ou remoção de dispositivos, criar novos enlaces e analisar o impacto dessas ações sobre métricas críticas, como confiabilidade, latência e consumo energético. Esse processo reduz significativamente os riscos associados a alterações diretas na infraestrutura industrial, além de apoiar a tomada de decisão de forma mais segura e fundamentada. Além do caráter preditivo, o DTN também desempenha um papel analítico e diagnóstico em RSFI. A modelagem da rede como um grafo possibilita a aplicação de métricas de centralidade, identificação de nós críticos e avaliação da dependência estrutural entre dispositivos. Essas análises auxiliam na detecção de gargalos de comunicação, rotas excessivamente sobrecarregadas e pontos únicos de falha, fornecendo subsídios objetivos para intervenções que visem aumentar a robustez e a resiliência da rede. Ao integrar monitoramento contínuo, simulação e análise comparativa entre cenários reais e virtuais, o DTN possibilita uma abordagem proativa na manutenção e otimização da rede. Essa perspectiva é particularmente relevante em ambientes industriais dinâmicos, nos quais mudanças frequentes no processo e no *layout* físico exigem soluções capazes de antecipar problemas e preservar níveis elevados de confiabilidade operacional.

3 ESTADO DA ARTE

Este capítulo apresenta alguns dos principais trabalhos publicados nos últimos cinco anos relacionados à análise de posicionamento de dispositivos em RSFI, e os trabalhos realizados em relação ao DTN.

Analisar o posicionamento de elementos é relevante em diversas aplicações de redes. Em RSFI particularmente, o posicionamento dos elementos impacta tanto na logística de instalação dos elementos como nas perdas de pacotes transmitidos, aumento do consumo de energia pelos dispositivos ao reenviar pacotes e queda da confiabilidade da rede. Por sua vez, o DTN constitui o objeto central deste estudo, uma vez que se configura como uma ferramenta estratégica voltada à otimização de redes complexas e críticas. Diversos trabalhos relacionados a este tema foram encontrados, de tal forma a corroborar com o potencial em explorar e ampliar o desenvolvimento dessa abordagem, bem como reconhecem seu potencial para aprimorar processos de monitoramento, análise e tomada de decisão. Nesse contexto, torna-se pertinente investigar a implementação dessa metodologia em aplicações específicas para RSFI de campo, de modo a avaliar sua viabilidade e benefícios no âmbito da confiabilidade e eficiência operacional. Na seção 3.1 são apresentados trabalhos relacionados à análise de posicionamento de elementos que compõem redes sem fio, e a seção 3.2 apresenta trabalhos realizados em relação ao DTN.

3.1 Análise de posicionamento de dispositivo

O trabalho desenvolvido por (TIMM, 2022) concentra-se na análise da escalabilidade e da confiabilidade de RSFI centralizadas, com foco específico em redes WH operando sob tráfego do tipo *convergecast*. O autor demonstra que, à medida que a escala da rede aumenta, surgem gargalos estruturais principalmente nas proximidades dos pontos de acesso, resultando em perdas de pacotes associadas à saturação de *buffers*, retransmissões excessivas e à obsolescência de pacotes devido à limitação do TTL. Para investigar esse comportamento, são aplicadas técnicas de análise de redes complexas, em especial métricas de CG, CP e CI, correlacionando essas métricas com o desempenho fim a fim das cadeias *uplink*. Os resultados indicam que dispositivos com elevada centralidade, par-

ticularmente de intermediação, tendem a concentrar tráfego crítico e apresentam maior probabilidade de causar degradação da confiabilidade global da rede. Com base nessas observações, o autor propõe uma técnica preventiva de redistribuição espacial de pontos de acesso, capaz de mitigar gargalos antes que ocorram falhas operacionais, alcançando incrementos de até 10% na confiabilidade média da rede. O presente trabalho utiliza e estende as ferramentas originalmente desenvolvidas por (TIMM, 2022), as quais foram concebidas para a análise de confiabilidade e escalabilidade em RSFI modeladas de forma sintética. No trabalho de referência, o autor constrói uma rede modelo, na qual são avaliadas métricas de desempenho e confiabilidade a partir de parâmetros simulados, permitindo identificar gargalos estruturais e dispositivos críticos por meio de critérios de centralidade, como CG, CP e CI. Nesta dissertação, essa mesma base metodológica é reaproveitada, porém aplicada a um contexto distinto, no qual os dados de entrada são provenientes de uma rede real, previamente digitalizados e integrados a um ambiente virtual. A partir desses dados reais, a ferramenta desenvolvida por (TIMM, 2022) é empregada para avaliar o comportamento da rede e identificar nodos críticos, mantendo a coerência conceitual com o modelo original. Entretanto, enquanto o trabalho de (TIMM, 2022) tem como foco principal a otimização do posicionamento do *gateway* como estratégia para mitigar gargalos e melhorar a confiabilidade global da rede, o presente estudo tem como escopo de atuação do DTN ao considerar diferentes tipos de intervenções. Especificamente, são simuladas modificações nos enlaces existentes, alterações nas estratégias de roteamento e a adição de nodos repetidores posicionados próximos aos dispositivos de campo. Dessa forma, o trabalho avança no uso do DT como ferramenta de suporte à tomada de decisão, permitindo avaliar múltiplas alternativas de otimização estrutural e operacional sem a necessidade de intervenções físicas na rede real.

(GUO *et al.*, 2021) investiga o problema de posicionamento ótimo de *gateways* em redes de satélites LEO, tratando-o como um problema de otimização multiobjetivo e multirrestritivo, cujo impacto se reflete diretamente na qualidade de serviço e no balanceamento de carga da rede. O modelo proposto busca simultaneamente minimizar o número de *gateways*, reduzindo custos de implantação, e maximizar o equilíbrio do tráfego, considerando restrições realistas do sistema, como limitações de largura de banda nos enlaces satélite-solo, número finito de antenas e interferência entre *gateways* próximos. Para estimar a matriz de tráfego, os autores empregam o modelo gravitacional, amplamente utilizado em cenários onde dados reais não estão disponíveis, e resolvem o problema por meio de uma versão discreta do algoritmo *Particle Swarm Optimization*. Os resultados, validados em constelações reais, demonstram que a abordagem é eficaz em distribuir carga de forma equilibrada sem superdimensionar a infraestrutura.

(ZHANG *et al.*, 2024) explora o uso de DT como entidades ativas na gestão de redes, propondo uma arquitetura que integra o conceito de DT a *Wireless Computing Power Networks*, voltada a ambientes altamente dinâmicos e heterogêneos. O estudo aborda dois

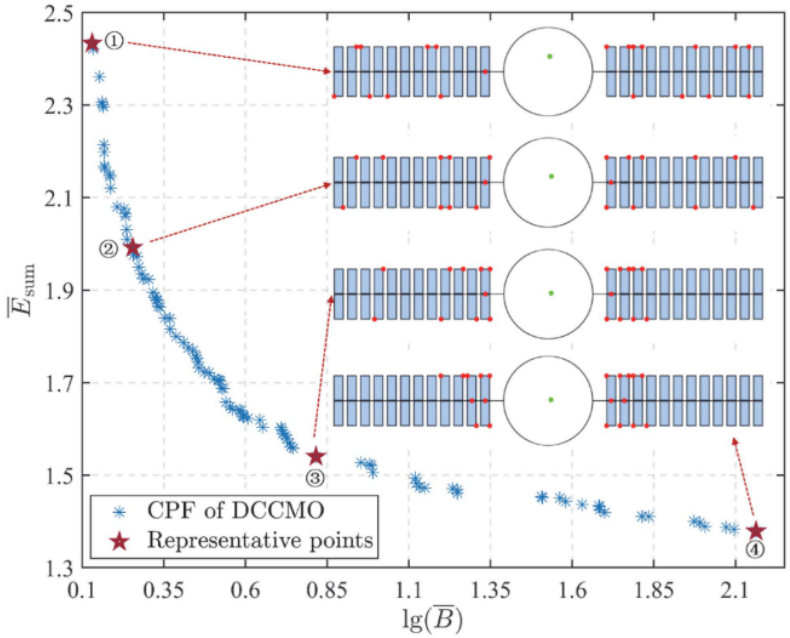
desafios centrais: o posicionamento ótimo dos DT e a transferência adaptativa desses gêmeos em resposta às variações temporais da demanda computacional e da topologia da rede. Para tal, o problema é modelado como um jogo cooperativo, empregando o valor de Shapley para quantificar a contribuição relativa de cada entidade computacional no suporte aos DT, garantindo decisões eficientes e justas. Além disso, é proposto um mecanismo de migração dinâmica, combinando teoria dos jogos e esquemas de leilão duplo, com o objetivo de reduzir a latência de sincronização, minimizar erros de mapeamento e melhorar a utilização global dos recursos. Os resultados obtidos demonstram ganhos consistentes em atraso médio, precisão e eficiência do sistema.

Em (YU *et al.*, 2023) é apresentado um modelo de otimização de posicionamento do *gateway* e dos sensores sem fio, que podem ser comparados à otimização de posicionamento de nodos de uma rede RSFI. Este estudo é voltado para sensores de difícil acesso, que apresentam baixa manutenabilidade, devido à complexidade de tais operações. Portanto, a maior parte dos sensores dentro da rede analisada pode ser considerada com tempo de vida limitado ao tempo da bateria em si. Para definir o posicionamento dos componentes da rede sem fio, o estudo utiliza como método o algoritmo de otimização multiobjetivo co-evolucionário de população dupla restrito. Na Figura 8 é possível observar a Frente de Pareto Restrita (*Constrained Pareto front* - CPF) dos resultados obtidos pelo algoritmo proposto de Otimização Multiobjetivo com Restrição de Dupla População (DCCMO, do inglês *Dual-population Constrained Multiobjective Optimization*), onde $lg(\overline{B})$ representa a eficácia da informação padronizada, e $\overline{E}_{sum}$ representa o consumo de energia padronizado. Os pontos em destaque na figura (representados por estrelas vermelhas) evidenciam como estavam posicionados os elementos da rede analisada, nos sentidos leste-oeste e norte-sul. Os *gateways* são os pontos em verde, e os sensores são os pontos em vermelho.

Implantar DT permite interação em tempo real e comunicação confiável, o que pode aprimorar o desempenho dos sistemas físicos. Em (CHUKHNO *et al.*, 2022) foi estudado o posicionamento dinâmico de DTs sociais na *Edge Internet of Things* (EIoT) para reduzir o atraso na transmissão de dados. O esquema forneceu uma solução sob a mobilidade do dispositivo *Internet of Things* (IoT) e levou em conta as especificidades da implantação da borda da rede, os tipos de dispositivos e suas características sociais.

(CHUKHNO *et al.*, 2022) propõem uma abordagem para o posicionamento dinâmico de DT com capacidades sociais em ambientes de computação de borda voltados a redes de *Internet of Things* (IoT) além do 5G. O trabalho parte do conceito no qual dispositivos físicos estabelecem relações sociais, como co-localização, propriedade comum ou pertencimento a um mesmo lote, e introduz os chamados *Social Digital Twins*, responsáveis por representar virtualmente esses dispositivos e suas interações. Os autores argumentam que, para garantir baixa latência, eficiência na descoberta de serviços e uso adequado de recursos computacionais limitados na borda, não é suficiente posicionar os DT apenas com base na proximidade física aos dispositivos reais, sendo necessário também considerar a

Figura 8 – CPF do DCCMO e configurações do sensor sem fio para pontos em destaque.



Fonte: (YU *et al.*, 2023).

intensidade das interações sociais entre eles. O problema é formulado como um problema de atribuição quadrática, no qual se busca minimizar conjuntamente a latência entre dispositivos físicos e seus respectivos DT e a latência entre DT de dispositivos socialmente relacionados, respeitando restrições de recursos e mobilidade. Devido à complexidade computacional do problema, os autores propõem uma heurística baseada em teoria dos grafos, que reduz significativamente o custo computacional ao aproximar a solução ótima por meio da construção de subgrafos geradores e mapeamentos eficientes. Resultados de simulação demonstram que a estratégia proposta alcança reduções expressivas na latência, mantendo a proximidade com os dispositivos físicos e apresentando melhor escalabilidade em comparação com abordagens tradicionais baseadas apenas em proximidade.

3.2 DTN

A crescente complexidade das redes de comunicação em ambientes industriais exige soluções inovadoras capazes de lidar com requisitos de confiabilidade, eficiência e segurança. Nesse cenário, surge o conceito de DT, que permite a criação de representações virtuais da rede física para análise, simulação e suporte à tomada de decisão.

Alguns estudos buscam aprimorar a ferramenta de DTN, com o intuito de desenvolver a aplicação em si e, portanto, escolhem uma rede específica para realizarem seus estudos, mas esclarecem que podem ser utilizadas em outros formatos de redes, como apresentado em (GüEMES-PALAU *et al.*, 2022), que utilizou uma Rede de Transporte Óptica (OTN, do inglês *Optical Transport Networks*), e (CHEN *et al.*, 2022), que utilizou uma Rede

de Área Local (LAN, do inglês *Local Area Network*), que serão abordadas com mais detalhes a seguir. Os estudos existentes até então sobre DTNs de comunicação industrial tratam de tecnologias 5G e *Industrial Internet of Things* (IIoT), e serão abordados com mais detalhes em 3.2.2.

3.2.1 DTN em aplicações não industriais

(GüEMES-PALAU *et al.*, 2022) investiga a aplicação de técnicas de Aprendizado por Reforço Profundo (DRL, do inglês *Deep Reinforcement Learning*) no contexto de DTN, com foco na aceleração do processo de treinamento por meio de estratégias evolutivas. Os autores partem da premissa de que o DTN permite a execução segura de tarefas de otimização de rede, como engenharia de tráfego e planejamento, sem impacto direto sobre a infraestrutura real. Embora o aprendizado por reforço profundo apresente bom desempenho nesses cenários, seu custo computacional e baixa escalabilidade representam limitações práticas para redes de grande porte. Para contornar esse problema, o trabalho propõe substituir o treinamento tradicional baseado em retropropagação por estratégias evolutivas altamente paralelizáveis, capazes de otimizar diretamente os pesos das redes neurais. A abordagem é combinada com redes neurais gráficas para capturar de forma eficiente a estrutura topológica da rede. Os experimentos, realizados em cenários de otimização de roteamento em redes ópticas de transporte, demonstram reduções expressivas no tempo de treinamento, alcançando acelerações superiores a duas ordens de grandeza em determinadas topologias.

(CHEN *et al.*, 2022) aborda o problema da modelagem em DTN a partir de uma perspectiva sistemática de classificação, construção e orquestração de modelos, destacando que o modelo de rede constitui o núcleo funcional de um DTN. O trabalho propõe a divisão dos modelos em dois grandes grupos: modelos básicos e modelos funcionais. Os modelos básicos são responsáveis por representar elementos físicos da rede e suas topologias, incluindo estados de fluxo e desempenho, enquanto os modelos funcionais são voltados a aplicações específicas, como análise, diagnóstico, predição e otimização. Os autores discutem diferentes técnicas de construção dos modelos básicos, comparando abordagens baseadas em simulação, virtualização e abstração matemática, e apontam esta última como a mais adequada para redes de grande escala devido ao menor consumo de recursos e maior escalabilidade. Um dos principais diferenciais do trabalho é a introdução de mecanismos de orquestração de modelos, que permitem a associação automática entre modelos básicos e funcionais por meio de três estratégias: orquestração de espaços de modelo, orquestração de fluxos e gerenciamento do ciclo de vida dos modelos. Essa abordagem possibilita a execução simultânea de múltiplos cenários de verificação e interação, mantendo a coerência entre o gêmeo digital e a rede física. O estudo consolida a visão do DTN como um sistema fechado em laço, capaz de realizar simulação, dedução lógica e otimização contínua de desempenho de forma coordenada e automatizada.

(ZHU *et al.*, 2021) propõe um método de construção de DTN fundamentado em grafos de conhecimento, com o objetivo de lidar com a crescente complexidade e escala das redes de comunicação modernas. O trabalho apresenta uma arquitetura de DTN composta por quatro camadas principais: rede física, *Data Lake*, camada de DT e camada de aplicações de rede, estabelecendo um fluxo bidirecional contínuo de dados e decisões. Um dos principais desafios abordados refere-se à coleta eficiente de dados em cenários de grande escala e alta dinamicidade, para o qual os autores introduzem o uso de algoritmos do tipo *Sketch*, capazes de reduzir custos de armazenamento e processamento sem comprometer significativamente a precisão estatística. Para a construção do modelo digital da rede, o estudo emprega grafos de conhecimento baseados em ontologias OWL, permitindo representar entidades físicas, atributos, relações topológicas e regras operacionais de forma estruturada e semântica. Além disso, técnicas de extração de relações baseadas em redes neurais são utilizadas para identificar automaticamente relações complexas entre elementos da rede. A viabilidade da abordagem é demonstrada em um cenário de autorecuperação de falhas, no qual políticas de reparo são testadas e validadas no ambiente virtual antes de serem aplicadas à rede real.

DTN aparece em outras áreas, como carros autônomos, satélites, Veículo Aéreo não Tripulado (UAV, do inglês *Unmanned Aerial Vehicle*), cidades inteligentes, etc, o que indica que é uma tecnologia de grande aplicação e em expansão.

3.2.2 DTN na Indústria

(ITANI; SHARAFEDDINE, 2024) apresenta uma abordagem para o desenvolvimento de um DT de alta fidelidade aplicado a cenários de *Industrial Internet of Things* (IIoT) no contexto do Metaverso Industrial e da Indústria 5.0. O trabalho parte da premissa de que a utilidade de um DT está diretamente associada ao grau de sincronização e à precisão com que o modelo virtual reflete o estado do sistema físico. Para capturar esse aspecto, os autores introduzem a métrica denominada *Age of Digital Twin*, derivada do conceito de *Age of Information*, que quantifica o atraso entre o estado real de uma entidade física e sua representação no DT. O sistema proposto utiliza veículos aéreos não tripulados para coletar dados de dispositivos IIoT distribuídos em uma planta industrial, processar essas informações na borda da rede e atualizar o DT de forma periódica. O problema é formulado como uma otimização conjunta da trajetória do UAV, do escalonamento dos dispositivos, da alocação de recursos de comunicação e computação e da quantidade de dados coletados, buscando maximizar a acurácia do gêmeo digital sem violar limites de sincronização impostos pela métrica de idade do gêmeo. Devido à complexidade do problema, os autores propõem uma decomposição em subproblemas, permitindo sua resolução de forma eficiente. Resultados de simulação demonstram um compromisso claro entre acurácia e sincronização, evidenciando que a coleta excessiva de dados pode comprometer a atualização oportuna do gêmeo digital.

(KRAUSE *et al.*, 2023) propõe a construção de um DT do ambiente rádio como suporte à detecção de anomalias em RSFI, motivados pela crescente necessidade de resiliência em cenários de Indústria 4.0. O trabalho explora a integração de informações contextuais, como a localização precisa de transmissores regulares e o conhecimento do ambiente físico, para construir um modelo digital capaz de estimar os níveis esperados de potência recebida em diferentes pontos da rede. A abordagem baseia-se na comparação entre os valores de *Received Signal Strength* estimados pelo DT e aqueles medidos por unidades de sensoriamento distribuídas, sendo a discrepância entre esses valores utilizada como entrada para algoritmos de detecção de anomalias. Diferentemente de métodos tradicionais baseados exclusivamente em análise espectral ou métricas de erro de pacotes, o estudo incorpora explicitamente o modelo do ambiente rádio, aproximando-se de um conceito de DT orientado ao contexto físico da rede. Os autores avaliam diferentes técnicas de detecção não supervisionada, incluindo *One-Class SVM*, *Local Outlier Factor* e um detector de energia adaptado, demonstrando que a abordagem proposta é capaz de identificar a presença de interferências, como *jammers*, mesmo sem conhecimento prévio de suas características. Os resultados de simulação indicam que a densidade das unidades de sensoriamento e o nível de incerteza do modelo de propagação influenciam diretamente o desempenho da detecção.

Dentro do estudo de DTN aplicado às RSFI existe uma linha de pesquisa voltada às tecnologias de 5G e 6G, que busca integrar o modelo de DT à IIoT. Estes estudos detêm algumas ferramentas já construídas para outras aplicações, que estão sendo incorporadas ao ambiente industrial, como *Deep Learning* e Realidade Aumentada. Entretanto, como essas ferramentas são oriundas de outras aplicações, os pesquisadores encontram dificuldades de adaptação ao ambiente fabril, entre elas a própria segurança da informação (em relação à privacidade da informação e em relação à confiança de que o dado está correto), e a incorporação de sensores com capacidade de serem integrados à rede, principalmente em processos de modernização de uma indústria já existente.

Os trabalhos de (BOKHTIAR AL ZAMI *et al.*, 2025) e (XU *et al.*, 2023), além de tratar dos mesmos assuntos mencionados no parágrafo anterior, o estudo também comenta sobre a possibilidade de integração com o sistema de *Big Data*, o que reforça que utilizar DTs dentro do ambiente industrial possibilita a conexão com outras ferramentas existentes e em expansão. A partir disto surgiu o interesse em desenvolver uma ferramenta que utiliza o conceito de DTN para uma RSFI de campo. O monitoramento da rede, realizado por meio de um ambiente simulado que possibilita a execução de testes comparativos entre diferentes métodos de intervenção e que evolui continuamente em consonância com a própria rede, tem como finalidade contribuir para o aprimoramento da escalabilidade e o aumento da robustez do sistema.

3.3 Resumo

A Tabela 2 apresenta a síntese da revisão bibliográfica realizada. Nela são apresentadas as principais diferenças entre as referências e a proposta desenvolvida neste trabalho. Ao considerar a pesquisa bibliográfica, observa-se que este trabalho se difere dos demais pelo fato de virtualizar uma RSFI com foco em protocolos de redes de campo (*Fieldbus*), e a partir dos dados obtidos através de simulações de intervenções na RSFI virtual, é possível mensurar quais técnicas de intervenção propostas (análise de *links*, posicionamento de nodos, e roteamento da rede) mais impactam a robustez da rede. Desse modo, é possível estudar soluções para uma rede de campo que já está em operação, e comparar diferentes cenários de intervenção no modelo virtual desenvolvido.

Nota-se que os estudos existentes que abordam o posicionamento dos dispositivos, em especial do elemento de maior complexidade de instalação (o ponto de acesso) em sua maioria não contemplam o contexto específico de uma RSFI de campo. Uma vez instalado o ponto de acesso em um local fixo, não é pertinente realizar mudanças frequentes em sua localização, em função de sua baixa mobilidade e da elevada complexidade envolvida em alterar seu posicionamento. Dessa forma, a otimização do posicionamento do *gateway* constitui um procedimento realizado previamente à implantação da rede. No entanto, alterações significativas na configuração de posicionamento dos demais componentes podem igualmente justificar a redefinição da localização do *gateway*.

Os estudos que implementaram a tecnologia DTN concentraram-se, em sua maioria, na otimização da taxa de transmissão de dados, especialmente por estarem direcionados a redes de IoT, cujos usuários apresentam demandas cada vez mais rigorosas quanto à velocidade de comunicação. Entretanto, no contexto das aplicações industriais analisadas nesta pesquisa, a confiabilidade da rede assume maior relevância em comparação à taxa de transmissão. Nesse sentido, o presente estudo propõe a implementação de ferramentas que viabilizem o uso de um DTN em RSFI, priorizando a confiabilidade e a segurança da comunicação. Ademais, este trabalho propõe investigar o posicionamento de dispositivos críticos da rede e simular a inserção de novos dispositivos próximos a pontos estratégicos, com o intuito de mitigar gargalos e potencializar a robustez da infraestrutura.

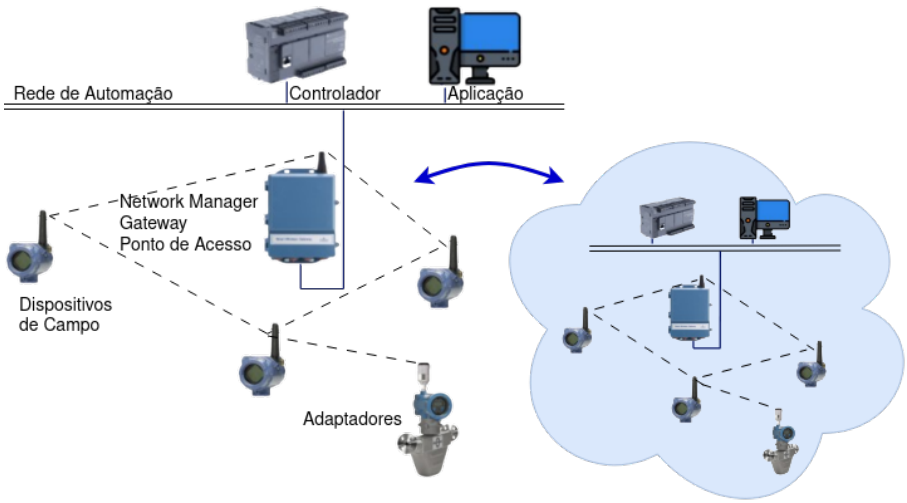
Tabela 2 – Comparação entre os estudos

Referência	DTN	Análise de pos.	Interv. na rede	IIoT	RSFI de campo
(CHUKHNO *et al.*, 2022)	✓	✓	✓	✓	
(GUO *et al.*, 2021)		✓			
(ZHANG *et al.*, 2024)	✓	✓	✓		
(YU *et al.*, 2023)		✓			
(ZHU *et al.*, 2021)	✓				
(GüEMES-PALAU *et al.*, 2022)	✓				
(CHEN *et al.*, 2022)	✓				
(ITANI; SHARAFEDDINE, 2024)	✓			✓	
(KRAUSE *et al.*, 2023)	✓			✓	
(XU *et al.*, 2023)	✓			✓	
(BOKHTIAR AL ZAMI *et al.*, 2025)	✓				
(BALOGH; FöLDVáRI; VARGA, 2023)	✓				
(CHEN *et al.*, 2024)	✓				
(FERNáNDEZ-CARAMéS; FRAGA-LAMAS, 2024)	✓			✓	
(HAN *et al.*, 2023)	✓			✓	
(TIMM, 2022)			✓		✓
Proposta	✓	✓	✓	✓	✓

4 MATERIAIS E MÉTODOS

Nesta seção são apresentadas as metodologias e ferramentas desenvolvidas a fim de implementar a virtualização da rede, simular intervenções, comparar os resultados com a rede real, de modo a cooperar com o processo de tomada de decisões na rede. Para a condução deste trabalho e a realização dos testes experimentais, tornou-se necessária a implementação de uma rede de testes dedicada. A Figura 9 mostra uma RSFI típica, em nível de barramento de campo, como o WH por exemplo, virtualizada como um DT. A escolha do protocolo WH deve-se ao fato de que o laboratório onde o projeto foi desenvolvido dispõe de toda a infraestrutura e dos recursos necessários para a implementação, desenvolvimento e validação dos experimentos propostos, bem como o fato de que esta pesquisa foi desenvolvida a partir de trabalhos que também utilizaram o WH como ferramenta.

Figura 9 – Rede *Wireless*HART e seu DT.



Fonte: autor.

A Figura 10 apresenta o diagrama de sequência que descreve as interações entre os componentes envolvidos na arquitetura proposta. O diagrama evidencia o fluxo de mensagens entre a aplicação HART-IP, o gerenciador de rede, os dispositivos de campo e a rede virtual, representando o ciclo completo de coleta, processamento e retroalimenta-

ção de dados. Inicialmente, a aplicação solicita ao gerenciador a lista de dispositivos e suas informações operacionais, que são obtidas junto aos dispositivos de campo. Em seguida, essas informações são transferidas para o ambiente virtual, onde ocorre a criação do roteamento, a avaliação da confiabilidade e a execução das intervenções simuladas. Os resultados obtidos são comparados entre os diferentes métodos de intervenção.

Uma vez identificado o método de intervenção mais adequado a partir das simulações realizadas no ambiente virtual, o sistema encaminha ao gerenciador de rede as alterações propostas nos enlaces entre os dispositivos, utilizando a aplicação HART-IP como interface de comunicação. Essas alterações correspondem, por exemplo, à criação, remoção ou reconfiguração de enlaces lógicos, as quais são então efetivamente aplicadas aos dispositivos de campo pelo gerenciador da rede. Após a aplicação das modificações na rede física, inicia-se um novo ciclo de coleta de dados. A aplicação HART-IP solicita novamente a lista de dispositivos ativos e as informações atualizadas da rede, refletindo o estado corrente após a intervenção. Esses dados são então encaminhados à rede virtual, de modo a possibilitar a atualização do modelo digital e a reavaliação das métricas de desempenho e confiabilidade. Essa etapa é fundamental para verificar se os efeitos observados na simulação correspondem ao comportamento efetivamente obtido na rede real.

A partir dessa atualização contínua, torna-se possível comparar de forma sistemática os dados históricos, os valores atuais medidos e os resultados preditivos fornecidos pelo DT. Esse processo fecha o ciclo de análise do DTN e reforça seu caráter iterativo, no qual o modelo virtual é constantemente realimentado com dados reais, mantendo-se alinhado à evolução da rede física ao longo do tempo. Esse procedimento evidencia a atuação do DT como um instrumento de suporte à tomada de decisão, permitindo que modificações estruturais sejam previamente avaliadas no domínio virtual antes de sua implementação na rede real, reduzindo riscos operacionais e intervenções empíricas.

4.1 Setup RSFI

Para validar o comportamento e o desempenho da rede proposta, é essencial a implementação de um ambiente de testes controlado, que simule de forma representativa as condições operacionais reais. Esse tipo de configuração permite observar o funcionamento dos dispositivos em situações próximas às encontradas em campo, além de possibilitar a coleta de dados relevantes para análises quantitativas e qualitativas. A seguir, é apresentada a estrutura do ambiente experimental utilizado neste trabalho, bem como a descrição dos componentes envolvidos.

A escolha da tecnologia *Wireless*HART para esta pesquisa fundamenta-se tanto em sua ampla adoção em aplicações industriais quanto na continuidade de trabalhos prévios realizados no mesmo contexto. Além disso, a infraestrutura disponível no laboratório, composta por dispositivos compatíveis com esse protocolo, viabilizou a implementação

prática dos experimentos sem a necessidade de adaptações significativas. Dessa forma, a utilização da rede *Wireless*HART mostrou-se adequada para os objetivos do estudo, permitindo a replicação de cenários reais e a obtenção de resultados coerentes com aplicações industriais típicas. O ambiente de testes é constituído por um gerenciador de rede, dispositivos de campo, e um *sniffer*, conforme destacado na Figura 11. Também foi utilizado um computador pessoal que opera com o sistema Ubuntu 18.04.2 LTS (*Bionic Beaver*). Nas subseções a seguir, são descritos os dispositivos que compõem a estrutura da rede, bem como suas principais funções.

O gerenciador de rede utilizado é o modelo 1420 *Smart Wireless Gateway* da marca Emerson como apresentado na Figura 11, e é responsável pela criação e manutenção da RSFI, bem como pela gestão dos dispositivos que a integram. Esse dispositivo tem as funções de *gateway* e ponto de acesso integrado ao seu sistema também. No contexto deste trabalho, os dispositivos de campo não estão fisicamente integrados a uma planta industrial. As variáveis de processo que trafegam pela rede são geradas e manipuladas por meio de simulação em software, com o objetivo de emular o comportamento típico de uma rede operacional. Os demais dispositivos utilizados foram desenvolvidos em trabalhos anteriores do grupo de pesquisas (MULLER *et al.*, 2010).

4.2 Comandos WH Implementados no Sistema

Foi desenvolvido um software em linguagem de programação *Python*, que coleta dados da rede WH através de alguns comandos específicos. Nesta seção são apresentados os principais comandos utilizados durante o desenvolvimento do projeto. Alguns deles empregados apenas como forma de validação, e outros usados de forma contínua. Os comandos apresentados são extraídos da norma *Wireless Command Specification* (FOUNDATION, 2008):

- O comando 814 é solicitado ao *Gateway* e relata a lista de todos os dispositivos de campo existentes da rede. Os *bytes* com os dados de requisição são apresentados na Figura 12 e os *bytes* com os dados de resposta são apresentados na Figura 13.

- O comando 780 é solicitado para um dispositivo de campo e relata a lista de integridade dos seus vizinhos ao gerenciador de rede (ZHU *et al.*, 2009). Os *bytes* com os dados de requisição são apresentados na Figura 14. Os dados de retorno são a média do RSL *Receive Signal Level* recebido, quantidade de pacotes transmitidos para este vizinho, quantidade de pacotes que falharam a transmissão e quantidade de pacotes recebidos deste vizinho. Os *bytes* com os dados de resposta são apresentados na Figura 15.

- O comando 781 é solicitado para um dispositivo de campo e não é necessário enviar *bytes* de dados de requisição. O dispositivo retorna o *Nickname* do próprio dispo-

sitivo, conforme apresentado na Figura 16. Este comando é relevante pois os comandos enviados aos dispositivos de campo na sequência deste comando retornam informações dos seus vizinhos através da referência do *Nickname* dos vizinhos.

- O comando 787 é solicitado para os dispositivo de campo, e os *bytes* com os dados de requisição são apresentados na Figura 17. Os *bytes* com os dados de resposta relatam os níveis de sinal de vizinhos sem enlace, conforme apresentado na Figura 18.

Os dados são armazenados em arquivos externos, com o intuito de viabilizar a utilização das informações coletadas de uma rede real, e adaptar para que sejam fonte de dados para uma versão adaptada do software de roteamento e escalabilidade *uplink* desenvolvido em (TIMM, 2022).

4.3 Leitura da Rede

Para se conectar com o gerenciador de rede, foi desenvolvida uma ferramenta somente para a comunicação, que envia comandos ao *gateway*, recebe os dados de resposta dele e os armazena em um banco de dados. O software da ferramenta desenvolvida foi criado em linguagem *Phyton*, e utiliza o protocolo HART *over Internet Protocol* (HART-IP), que é o tunelamento do HART no protocolo TCP/IP, para realizar a comunicação entre o computador e o *gateway*.

Através do software desenvolvido, são enviados os comandos necessários para leitura da rede existente. O primeiro comando enviado é o comando 814 que pergunta diretamente ao gerenciador quantos dispositivos compõem a rede, e na sequência é enviado o comando 781 para cada dispositivo, para ler seus *nicknames*. Com esses dados é possível configurar os próximos comandos e analisar os dados que eles retornam, os comandos 780 e 787.

O comando 780 é enviado para cada dispositivo da rede e traz dados detalhados de cada *link* ativo desse dispositivo. Os dados fornecidos por este comando são essenciais para a construção da réplica digital à rede existente. Já o comando 787 fornece informações pertinentes a possíveis alterações na rede existente, pois fornece dados de possíveis *links*. Estes *links* são testados em simulação, de modo que seja analisada a possibilidade de inclusão destes e, com isso, aprimorar a rede e aumentar sua robustez.

O código desenvolvido é apresentado no Algoritmo 1. O primeiro comando a ser enviado é o 814, e ele é tratado dentro da função *tratar_814*. A partir deste comando, o código obtém informações como a quantidade de dispositivos da rede e os endereços deles. De posse dessas informações, ainda dentro da função *tratar_814* os demais comandos são chamados, em *loop* até que todos os dispositivos sejam verificados, conforme apresentado no Algoritmo 2.

Algoritmo 1: Comunicação HART-IP com dispositivos de rede

Entrada: Endereço do dispositivo, código do comando, comando em hexadecimal, dados adicionais, auxiliar

Saída: Respostas tratadas e dados armazenados em planilhas

Inicializar bibliotecas, parâmetros e variáveis;

Criar comando de inicialização do HART-IP;

Criar comando principal com `hip_cmd_create(addr, cmd, data);`

Abrir socket TCP/IP e conectar ao gateway (HOST, PORT);

Enviar comando de inicialização;

Receber resposta via função `socket_resp();`

enquanto *verdadeiro* **faça**

- Registrar horário atual;
- Enviar comando montado ao dispositivo;
- Receber resposta via `socket_resp();`
- **se** *código de resposta for 33 ou 34* **então**
  - Continuar aguardando resposta válida;
- **senão**
  - Interpretar dados de resposta;
  - Chamar `Response()` para extrair payload;
  - Verificar qual comando foi enviado (`cmd`);
  - **se** *cmd == 780* **então**
    - Chamar `tratar_780(...)`
  - **senão se** *cmd == 781* **então**
    - Chamar `tratar_781(...)`
  - **senão se** *cmd == 787* **então**
    - Chamar `tratar_787(...)`
  - **senão se** *cmd == 814* **então**
    - Chamar `tratar_814(...)`
  - **senão**
    - Imprimir “Comando não tratado”
  - **break**

Algoritmo 2: tratar_814(`Response_data_bytes`)

Entrada: Bytes de resposta do comando 814

Saída: Execução sequencial dos comandos 781, 780 e 787 para cada dispositivo

Calcular `Qtd_disp` com base nos bytes 4 e 5 da resposta;

Inicializar `aux` como 0;

enquanto *`aux < Qtd_disp`* **faça**

Extrair endereço do dispositivo a partir dos bytes da posição `(5*aux)+6`;

```
// Enviar comando 781 - Obter nickname do
   dispositivo
```

Definir `cmd = 781`, `cmd_hex = 0x030d`, `data = []`;

Chamar `call_comando(addr, cmd, cmd_hex, data, aux);`

```
// Enviar comando 780 - Obter vizinhos vinculados
```

Definir `cmd = 780`, `cmd_hex = 0x030c`, `data = [0x00, 0xff]`;

Chamar `call_comando(addr, cmd, cmd_hex, data, aux);`

```
// Enviar comando 787 - Obter vizinhos não
   vinculados
```

Definir `cmd = 787`, `cmd_hex = 0x0313`, `data = [0x00, 0xff]`;

Chamar `call_comando(addr, cmd, cmd_hex, data, aux);`

Incrementar `aux`;

4.4 Classes do Gêmeo Digital de Rede de uma RSFI

O DTN de uma RSFI baseada no protocolo WH é estruturado a partir de uma modelagem orientada a objetos, cujo objetivo é representar, de forma organizada e coerente, os elementos físicos, lógicos e operacionais que compõem a rede real. Essa abordagem permite abstrair o comportamento da RSFI em classes bem definidas, facilitando a análise, a simulação de intervenções e a comparação de cenários, ao mesmo tempo em que preserva a correspondência entre o domínio físico e o virtual. Embora a implementação computacional do DTN tenha sido realizada em ambiente MATLAB, a organização em classes independe da linguagem utilizada, tratando-se de uma escolha conceitual que visa garantir modularidade, escalabilidade e clareza na representação da rede virtual.

A classe Rede representa a entidade central do DTN responsável por agregar todos os demais elementos que compõem a RSFI virtualizada. Essa classe corresponde à visão sistêmica da rede, integrando dispositivos, topologia, estado operacional e parâmetros de configuração. Do ponto de vista conceitual, a classe Rede mantém: o conjunto de dispositivos que participam da RSFI; a estrutura de conectividade entre esses dispositivos; as informações globais de desempenho e confiabilidade; e as configurações necessárias para simulação e análise. Além disso, essa classe atua como ponto de entrada para a aplicação de intervenções, uma vez que qualquer modificação na topologia, no roteamento

ou na composição da rede é refletida inicialmente em sua representação global.

A classe Dispositivo modela os nós que compõem a RSFI WH, estabelecendo uma correspondência direta entre cada elemento físico da rede e sua contraparte virtual no DTN. Essa classe representa sensores, atuadores, repetidores e demais nós de campo, independentemente de sua função específica. Cada dispositivo é caracterizado por atributos que descrevem sua identidade, papel na rede, estado operacional e capacidade de comunicação. Além disso, a classe contempla informações relacionadas à vizinhança, isto é, quais outros dispositivos podem ser alcançados diretamente, bem como os enlaces disponíveis para transmissão de dados. Conceitualmente, a esta classe constitui o elemento fundamental para análises locais da rede, como identificação de nós críticos, sobrecarga de tráfego, saturação de *buffers* e impacto de falhas individuais sobre a confiabilidade global.

Dentro da hierarquia de dispositivos, destacam-se classes especializadas associadas à infraestrutura da RSFI, como o *gateway*, que representa o nó de destino final das comunicações, atuando como ponto central de coleta dos dados transmitidos pelos dispositivos de campo. No DTN, essa classe assume papel estratégico na análise de rotas, latência e confiabilidade, uma vez que todas as comunicações convergem para esse elemento.

A classe Enlace representa a conexão lógica entre dois dispositivos da RSFI, sendo responsável por modelar a qualidade da comunicação entre eles. Diferentemente do dispositivo, que é uma entidade estática, o enlace reflete características dinâmicas do ambiente de comunicação sem fio. Essa classe incorpora métricas como nível de sinal recebido, probabilidade de entrega de pacotes e disponibilidade do enlace, permitindo que o DTN represente variações temporais da qualidade da comunicação. Os enlaces constituem a base para a construção do grafo da rede e para a avaliação de caminhos alternativos e redundantes. No contexto do DTN, a classe Enlace é essencial para identificar gargalos, enlaces frágeis e potenciais pontos de falha que comprometem a confiabilidade da RSFI.

A classe Topologia descreve a organização estrutural da RSFI a partir do conjunto de dispositivos e enlaces disponíveis. Essa classe abstrai a rede como um grafo, no qual os nós representam dispositivos e as arestas representam enlaces de comunicação. A partir dessa representação, tornam-se possíveis análises baseadas em teoria de grafos, como cálculo de centralidades, identificação de nós críticos e determinação de caminhos preferenciais entre dispositivos e o *gateway*. A topologia da rede é continuamente atualizada no DTN à medida que novas medições são incorporadas ou intervenções são simuladas. Conceitualmente, essa classe conecta a representação física da RSFI a métodos analíticos que permitem compreender o comportamento global da rede.

A classe Rota modela os caminhos lógicos percorridos pelos pacotes desde um dispositivo de origem até o *gateway*. No DTN, uma rota pode ser composta por um caminho principal e por rotas redundantes, refletindo os mecanismos de confiabilidade típicos das RSFI baseadas em WH. Cada rota é associada a métricas agregadas que permitem avaliar

seu custo, robustez e impacto no desempenho da rede. A classe Rota é particularmente importante para simulações de intervenções relacionadas a mudanças de roteamento, balanceamento de tráfego e tolerância a falhas.

A classe Estado da Rede representa a condição operacional do DTN em um determinado instante ou intervalo de tempo. Essa classe consolida indicadores globais de desempenho, como confiabilidade, perdas por TTL, perdas por *buffer* e outros parâmetros relevantes para a análise da RSFI. Além de fornecer uma visão instantânea do comportamento da rede, o estado da rede permite comparações diretas entre diferentes cenários simulados, servindo como base para a avaliação da efetividade das intervenções propostas.

A classe Intervenção representa modificações planejadas na RSFI virtual, como alteração de rotas, inclusão de dispositivos, criação de novos enlaces ou reconfiguração de parâmetros operacionais. No DTN, as intervenções são tratadas como entidades conceituais independentes, permitindo que diferentes estratégias sejam comparadas de forma sistemática. Essa classe desempenha papel central no processo de tomada de decisão, pois viabiliza a avaliação prévia dos impactos de cada intervenção antes de sua aplicação na rede física.

A definição das classes do DTN para uma RSFI WH estabelece uma base conceitual sólida para a virtualização da rede, permitindo representar de forma integrada seus elementos físicos, lógicos e operacionais. Ao organizar o DT em classes bem definidas, torna-se possível analisar o comportamento da rede, identificar gargalos, simular intervenções e apoiar decisões de forma estruturada e reprodutível. Essa organização conceitual independe da plataforma computacional adotada, embora neste trabalho o MATLAB tenha sido utilizado como ambiente de implementação, reforçando que o foco do DTN reside na estrutura lógica e na representação fiel da RSFI, e não na ferramenta específica empregada.

4.5 Roteamento na DTN

Em uma rede real de interesse que esteja em operação, o roteamento é gerado originalmente pelo gerenciador de rede e já está implementado. Uma base de dados é coletada desta rede real, e a partir desses dados, é desenvolvido o roteamento da cópia da rede dentro do software criado nesta pesquisa. Os comandos utilizados para criar a base de dados e as informações de rede que eles fornecem foram detalhados e discutidos em 4.2.

Após a realização de testes em laboratório com o dispositivo *sniffer* (Figura 11), foi possível encontrar uma característica pertinente do roteamento da rede real, que contribuiu para a construção do roteamento do DTN. Os nodos têm vários *links* com diferentes vizinhos, entretanto, não distribuídos de maneira uniforme. Algumas rotas têm mais *links* configurados dentro do *superframe* em detrimento das demais. Isto implica que, inde-

pendentemente da quantidade de dispositivos com que cada nodo se comunica, existe um dispositivo vizinho com maior probabilidade de receber os dados que se destinam ao *gateway* (rota *uplink*). Ao observar as mensagens coletadas pelo dispositivo *sniffer* foi possível observar que, geralmente, os dispositivos vizinhos com maior recepção de dados apresentavam maiores RSL em seus enlaces em comparação aos demais. Com isto, é possível inferir que, para cada nodo existe uma rota *uplink* mais utilizada, e os demais enlaces podem ser considerados rotas redundantes, previstas pelo protocolo WH. Portanto, o RSL é uma métrica pertinente para quantificar o *link* e auxiliar na construção do roteamento da cópia digital da rede.

É obtido um valor de RSL para cada vizinho de um nodo específico, cujo valor do RSL foi calculado previamente pelo gerenciador da rede por meio de um filtro do tipo *Infinite Impulse Response* (IIR), e a equação utilizada está descrita em (8) (FOUNDATION, 2008).

$$RSL = RSL - \frac{RSL}{RSLDamp} + \frac{MeasuredRSL}{RSLDamp} \tag{8}$$

O parâmetro MeasuredRSL representa o RSL referente ao pacote atual, enquanto RSLDamp corresponde ao fator de amortecimento utilizado no cálculo. Esse fator deve ser uma potência de 2, sendo o valor padrão igual a 64. Para vizinhos descobertos, ou seja, aqueles com os quais o dispositivo ainda não estabeleceu comunicação, é atribuído o maior valor de RSL registrado. Esse valor é ponderado, dando maior peso às comunicações mais recentes, de modo a refletir de forma mais fiel a qualidade atual do enlace.

Periodicamente, cada dispositivo transmite ao gerenciador de rede relatórios contendo informações sobre a integridade dos enlaces com seus vizinhos. A principal métrica reportada é o RSL dos dispositivos vizinhos. Após o envio de cada relatório, os valores anteriores são reinicializados, de modo a permitir que o gerenciador obtenha uma visão atualizada da qualidade da comunicação, essencial para a otimização contínua da configuração da rede. A cada relatório, o dispositivo pode incluir informações de até quatro vizinhos, mas o gerenciador de rede pode requisitar dados adicionais, se necessário..

Os valores referentes ao RSL dos enlaces compõem uma matriz, onde cada linha representa o nodo e as colunas são os vizinhos. As intersecções da matriz RSL que representam nodos que não têm *link* entre si são preenchidas com o valor zero. A base de dados coletada da rede informa todos os nodos existentes e o custo de cada *link* existente, mensurado pelo RSL. Estes dados são utilizados para alimentar o algoritmo que simulará o roteamento da rede, baseado no algoritmo Dijkstra, apresentado em 2.2.3. O algoritmo desenvolvido difere-se do algoritmo Dijkstra pelo fato de não atribuir valor infinito aos caminhos desconhecidos. Primeiro, todos os caminhos possíveis são encontrados, sem repetição de nodos no mesmo caminho, para evitar *loops*, e somente depois é mensurado o custo de cada caminho. O caminho com menor custo é definido como o caminho principal. Os demais *links*, que não estão no caminho principal, são salvos na matriz de rotas

redundantes. A partir do RSL, é definido o parâmetro PDR, que também é utilizado pelo algoritmo desenvolvido. O algoritmo 3 apresenta a lógica do roteamento desenvolvido para a cópia virtual da rede.

4.6 Simulação de desempenho da RSFI

Baseado no trabalho desenvolvido em (TIMM, 2022), o modelo de simulação proposto introduz uma componente de interferência aleatória que reduz a potência do sinal entre pares de dispositivos. Essa abordagem visa representar, de forma verossímil, os efeitos de atenuações causadas por barreiras físicas e interferências eletromagnéticas oriundas de maquinários e equipamentos comumente encontrados em ambientes industriais. A magnitude dessa interferência influencia diretamente o PDP, o que caracteriza cenários com maior ou menor nível de ruído externo.

Esse fator de interferência foi definido como uma probabilidade de 5% de ocorrência no software de simulação do desempenho da rede. Tal configuração foi adotada considerando que, nesta pesquisa, outras características da rede já foram intencionalmente modificadas com o objetivo de reduzir sua confiabilidade, de modo a evidenciar os gargalos existentes e analisar os efeitos das intervenções propostas. Valores acima de 15% para a taxa de interferência implicam redução desproporcional na confiabilidade da rede simulada. Como a média RSL percebida por cada dispositivo já sofre influência das interferências, para este trabalho, 5% de interferência são suficientes para coletar os dados de interesse. Entretanto, como tais variações não impactam diretamente a análise de escalabilidade, que é o foco central deste estudo, a introdução das interferências cumpre função exclusivamente contextual, para garantir maior realismo à simulação em relação ao ambiente fabril.

A simulação desenvolvida faz uso da técnica *Time Division Multiple Access* (TDMA), como mecanismo adotado para o controle de acesso ao meio, e é muito utilizada em protocolos de redes de campo. Uma rede particiona o tempo em intervalos fixos denominados *slots*. Em cada *slot*, um ou mais pares de dispositivos são autorizados a se comunicar, com funções de emissor e receptor previamente definidas para cada par. Ao final de cada *slot* e da tentativa de comunicação correspondente, os dispositivos envolvidos realizam uma mudança de canal através da técnica de salto de canais sincronizado no tempo (TSCH, do inglês *Time Slotted Channel Hopping*). Esse procedimento visa reduzir interferências e aumentar a confiabilidade do enlace ao explorar diferentes canais de comunicação. Os *slots* são organizados em uma estrutura cíclica chamada *slotframe* ou *superframe*, que define a sequência ordenada de comunicação na rede, conforme ilustrado na Figura 19.

A organização temporal da rede é estruturada por meio do conceito de *superframe*, definido como uma sequência periódica de *slots* de tempo consecutivos. O período de um *superframe* corresponde à soma da duração de todos os seus *slots* constituintes. Todos os

Algoritmo 3: Roteamento baseado em RSL

Dados: Matriz PDR.

Resultado: Rotas *uplink* entre cada nodo e o *gateway*.

início

- Inicializar matrizes: `links`, `possiveis_caminhos`, `aux_links` ;
- Inicializar contadores e vetores auxiliares ;

para cada *par* (i, j) *na matriz* `pdr` **faça**

- **se** `pdr(i, j)` $\neq 0$ **então**
  - Armazenar $(i \rightarrow j)$ e `pdr(i, j)` em `links` ;

Remover linhas nulas da matriz `links` ;

Obter apenas os pares $(disp, vizinho)$ em `so_links` ;

para cada *linha em* `so_links` **faça**

- **se** *o destino do link for o gateway (nó 1)* **então**
  - Armazenar caminho direto em `possiveis_caminhos` ;
- **senão**
  - Inicializar variáveis auxiliares e contadores ;
  - Criar entrada inicial do caminho com o link atual ;
  - **para cada** *caminho a ser testado* **faça**
    - **para cada** *extensão possível do caminho* **faça**
      - Obter próximo dispositivo a partir de `links` ;
      - **se** *dispositivo não estiver no caminho atual* **então**
        - Adicionar ao caminho ;
        - **se** *dispositivo for o gateway* **então**
          - Armazenar caminho completo em `possiveis_caminhos` ;
        - **senão**
          - Clonar caminho atual para ramificações futuras ;
      - **senão**
        - Ignorar (para evitar ciclos) ;
    - **se** *nenhum novo caminho foi gerado* **então**
      - Encerrar laço `enquanto` ;
    - Atualizar variáveis para próxima iteração ;

superframes em uma rede iniciam a partir do ASN igual a zero, que marca o instante de criação da rede. A partir desse ponto, os *superframes* são repetidos ciclicamente ao longo do tempo, conforme o período previamente estabelecido. O tipo de comunicação que ocorre em um determinado *slot* de tempo é definido pelos *links* configurados na camada de enlace.

O software desenvolvido para simular o desempenho da rede tem um número limitado de ciclos, que é definido pelo usuário. A cada novo ciclo, todos os dispositivos de campo que compõem a rede geram um novo pacote de dados destinado ao *gateway*. Cada ciclo corresponde a um *superframe* e uma unidade de TTL. O software também permite configurar a quantidade de *links* redundantes dentro do *superframe*. Com isto, dentro de um mesmo ciclo, um pacote pode dar mais de um salto, a depender da quantidade de *links* redundantes dentro do *superframe* e do ordenamento dos dispositivos na sua rota *uplink*.

Nesse estudo, o objetivo é testar uma rede em condições críticas, para analisar se a ferramenta desenvolvida fornece resultados pertinentes relacionados à rede antes e após as intervenções sugeridas. Então, as características acima citadas foram fixadas em valores que forçaram a diminuir a confiabilidade da rede. Foram fixados o total de 3 *links* redundantes dentro do *superframe*, ou seja, são 4 *links* da rota *uplink* dentro do mesmo *superframe* para cada dispositivo, e o número de ciclos de *superframe* foi fixado em 100, para testar a rede. Ao fim da simulação, são gerados um total de 100 pacotes multiplicados pela quantidade de dispositivos de campo da rede.

A métrica PDP proposta neste trabalho corresponde à probabilidade percentual de sucesso na transmissão de pacotes entre um par de dispositivos a e b. Para fins de objetividade e simplificação do modelo, considera-se que o maior fator determinante para o sucesso ou fracasso de uma tentativa de transmissão é a potência do sinal percebido entre os dispositivos. A cada tentativa de envio, um número aleatório percentual é gerado e comparado com a probabilidade de sucesso previamente determinada com base nessa potência.

A relação entre a potência do sinal recebido, denotada como $P_{r(a,b)}$ (em dBm), e a probabilidade de sucesso da transmissão, é descrita pela Equação (9). Nessa equação, os parâmetros Lim_{inf} e Lim_{sup} representam, respectivamente, os limites inferior e superior de potência adotados para simular cenários nos quais a chance de entrega bem-sucedida varia de 0,1% a 99,9%. Essa modelagem permite mapear de forma contínua a potência de sinal em uma função probabilística que reflete a confiabilidade da comunicação em diferentes condições de interferência.

$$PDP_{(a,b)} = \frac{P_{r(a,b)} - Lim_{inf}}{Lim_{sup} - Lim_{inf}} \tag{9}$$

O padrão IEEE 802.15.4 estabelece que a sensibilidade mínima exigida para os transceptores utilizados em RSFI é de -85 dBm. Contudo, alguns transceptores, como o empregado neste trabalho, apresentam desempenho significativamente superior, atingindo

níveis de sensibilidade em torno de -100 dBm. Essa diferença representa um ganho substancial na capacidade de recepção de sinais de baixa potência, ampliando a robustez da comunicação mesmo em ambientes sujeitos a interferências e atenuações. Dessa forma, a faixa de operação considerada neste estudo, compreendida entre -100 dBm e -30 dBm, reflete o intervalo realista de intensidade de sinal recebido, englobando tanto o limite inferior (Lim_{inf}) de sensibilidade do dispositivo quanto o limite superior (Lim_{sup}) associado à saturação do receptor. A variação desses parâmetros no ambiente de simulação influencia diretamente o grau em que a distância entre dispositivos afeta a ocorrência de perdas de pacotes. Em outras palavras, os ajustes realizados determinam o quão sensível é a relação entre o afastamento físico dos nós da rede e a degradação no PDR, de modo a refletir diferentes condições de propagação do sinal.

4.7 Métricas de desempenho da RSFI

O presente trabalho tem como principal objetivo analisar o impacto da escalabilidade sobre métricas de desempenho em RSFI. Observa-se que todas as métricas consideradas, direta ou indiretamente, são afetadas por um fenômeno fundamental: a perda de pacotes.

De modo geral, a comunicação ponto a ponto entre nós vizinhos em redes WH não se limita à transmissão unidirecional de dados; ela envolve também a recepção de uma resposta curta e padronizada, denominada *Acknowledgement* (ACK), enviada pelo nó de destino como forma de reconhecimento da entrega bem-sucedida do pacote. A perda de pacotes, no contexto do protocolo WH, é caracterizada principalmente pela ausência de recepção de uma mensagem ACK após a transmissão de um pacote por parte do nó de origem. É importante observar que algumas mensagens não requerem ACK, mas tais casos específicos não são abordados no escopo deste estudo. O ACK atua como mecanismo de confirmação utilizado pelo transmissor para validar que o pacote foi corretamente entregue e compreendido pelo receptor, sendo fundamental para o cálculo de métricas como o PDR e o PDP, em níveis superiores, para a construção de indicadores de desempenho global da rede, como a confiabilidade.

Após definir a matriz PDR com base nas informações obtidas da rede, o software estima o PDP. Este parâmetro foi desenvolvido especificamente para esta ferramenta com o intuito de ser o equivalente virtual do existente PDR (TIMM, 2022). Além disso, o software permite que seja arbitrado um valor entre 0% e 100% de probabilidade de não entregar os pacotes enviados entre cada par de dispositivos, para simular interferências externas de sinal na forma de decréscimos na potência de sinal percebido. Essa ferramenta visa simular com mais verossimilhança o ambiente fabril que apresenta obstáculos físicos e eletromagnéticos interagindo com a transmissão em rádio-frequência.

No protocolo WH, o ACK deve ser recebido dentro do mesmo *slot* de comunicação da mensagem original, conforme o tempo reservado no agendamento entre os dispositi-

vos envolvidos. Para os propósitos desta análise, não se distingue se a perda de pacote decorre da falha na transmissão do pacote original ou da ausência do ACK de confirmação. Ambas as situações são tratadas como equivalentes, e são contempladas de forma unificada no cálculo do PDR como eventos de falha na comunicação ponto a ponto. Importa destacar, no entanto, que a ocorrência de perdas de pacotes ponto a ponto em redes de campo não implica necessariamente em comprometimento direto da confiabilidade fim a fim. A arquitetura do protocolo prevê mecanismos de tolerância a falhas, como enlaces redundantes e múltiplas rotas, que possibilitam a retransmissão de pacotes perdidos. Tais estratégias, embora aumentem a robustez da rede, acarretam custos adicionais em termos de ocupação da largura de banda disponível, uma vez que retransmissões consomem *slots* que poderiam ser utilizados para o envio de novos pacotes.

No contexto da simulação proposta neste trabalho, a análise é centrada em dois mecanismos principais responsáveis por perdas definitivas de pacotes fim a fim: perda por esgotamento do *buffer* e perda por obsolescência (vencimento do tempo de vida útil do pacote). Esses modos de falha são considerados críticos, pois representam eventos em que a retransmissão não é possível ou não é mais válida, de modo que impactam diretamente a confiabilidade da rede como um todo.

4.7.1 Perda de pacotes por *buffer* cheio

Cada dispositivo de campo possui uma memória embarcada destinada tanto ao armazenamento do *firmware* de operação quanto ao gerenciamento dos pacotes transmitidos e recebidos em comunicações ponto a ponto com dispositivos vizinhos. A porção dessa memória reservada especificamente para o armazenamento temporário de pacotes é comumente referida como *buffer*. Trata-se de uma estrutura de dados organizada em forma de fila, cujos espaços são destinados à alocação sequencial de pacotes recém-recebidos ou gerados localmente. O tamanho efetivo do *buffer* depende da capacidade de memória disponível no dispositivo e do tamanho individual dos pacotes manipulados.

Para os propósitos da simulação desenvolvida neste trabalho, não se faz necessário utilizar unidades de medida de memória convencionais, como *bytes*. Adota-se, em seu lugar, a abstração de que cada pacote ocupa uma unidade fixa de memória, de modo a permitir o tratamento da capacidade do *buffer* em termos de número de pacotes armazenáveis. Essa simplificação contribui para a análise do comportamento da rede sem comprometer a generalidade dos resultados. Na Figura 20 é apresentada uma representação esquemática do funcionamento de um *buffer* de dispositivo de campo, configurado, neste exemplo, com capacidade para armazenar até dez pacotes simultaneamente.

Na figura apresentada, considera-se irrelevante a origem dos pacotes armazenados no *buffer*, se provenientes do próprio dispositivo ou recebidos de vizinhos, uma vez que a política de priorização de pacotes não constitui objeto de análise neste estudo. Dessa forma, adota-se uma política de atendimento do tipo FIFO, pela qual o primeiro pacote

armazenado é também o primeiro a ser encaminhado. Assim, o próximo pacote a ser transmitido será o Pacote |A|.

No instante de tempo representado no detalhe (a) da Figura 20, observa-se que 50% das posições do *buffer* encontram-se livres, de modo a permitir que o dispositivo ainda possa gerar ou receber até cinco pacotes adicionais sem exceder sua capacidade de armazenamento. Durante o próximo *slot* de transmissão no *superframe*, o dispositivo tentará encaminhar o Pacote |A| ao vizinho seguinte na rota de *uplink*. Em caso de sucesso, o pacote será removido do *buffer* de origem e inserido na primeira posição disponível do *buffer* do dispositivo receptor. Consequentemente, o Pacote |B| torna-se o novo elemento de maior prioridade na fila FIFO, agora com seis posições disponíveis para novos pacotes. No entanto, ao considerar que o modelo de simulação incorpora perdas de pacotes, caso a probabilidade de entrega indique falha na transmissão do Pacote |A| durante o *slot* correspondente, o pacote permanecerá armazenado no *buffer* do dispositivo de origem. Nesse caso, o pacote será novamente elegível para retransmissão em futuros *slots* redundantes, seja por enlaces alternativos ou por rotas diversas. Essa lógica implica que um pacote poderá permanecer indefinidamente no *buffer* enquanto não for transmitido com sucesso. Essa permanência prolongada, contudo, pode implicar dois problemas críticos: (i) a obsolescência do pacote, caso este ultrapasse TTL, e (ii) a saturação do *buffer*. Como demonstrado no detalhe (b) da Figura 20, falhas recorrentes na transmissão do Pacote |A| podem comprometer a vazão de pacotes no dispositivo, e levam ao acúmulo de novos pacotes (oriundos do próprio dispositivo ou de seus vizinhos) e à saturação da memória. Caso um novo pacote seja gerado ou recebido enquanto todas as posições do *buffer* estiverem ocupadas, como ilustrado no detalhe (c), com o Pacote |K|, o novo pacote será descartado imediatamente. Se o Pacote |K| descartado for originado de uma tentativa de recepção de um vizinho, o evento configura uma perda ponto a ponto: o vizinho remetente detecta a falha e retém o pacote para retransmissão posterior. Por outro lado, se o Pacote |K| for gerado localmente pelo próprio dispositivo cujo *buffer* se encontra cheio, não há alternativa viável senão seu descarte definitivo, o que acarreta a perda de confiabilidade fim a fim.

Importa destacar que esse tipo de falha pode comprometer gravemente o desempenho da rede. A redução da vazão em um único nó impacta diretamente os *buffers* dos dispositivos a jusante na rota de *uplink*, mesmo que esses vizinhos apresentem elevados índices de PDP. A saturação do *buffer* inibe o recebimento de pacotes, resultando em um efeito cascata que se propaga pela cadeia de comunicação. Esse fenômeno torna-se ainda mais crítico quando afeta dispositivos próximos aos pontos de acesso, dos quais diversos outros nós dependem para a entrega de dados em esquemas de *convergecast*.

Para as simulações realizadas neste trabalho, a capacidade do *buffer* foi estabelecida em cinco pacotes para cada nodo durante as simulações. Este padrão reduziu a capacidade de entregas de pacotes da rede e evidenciou os gargalos existentes para rotas *uplink*.

4.7.2 Perda de pacotes por obsolência de TTL

Ao considerar o exemplo apresentado na Figura 20, é possível observar que, em cenários nos quais um pacote sofre sucessivas falhas de transmissão ou quando o *buffer* se encontra congestionado por outros pacotes, a informação contida nesse pacote pode tornar-se obsoleta do ponto de vista da aplicação da rede. Tal situação é particularmente evidente em sistemas de monitoramento contínuo, como os que envolvem sensores de processo que geram dados periodicamente. Caso o encaminhamento de um pacote seja reiteradamente malsucedido ao longo do trajeto até o coletor, existe a possibilidade de que um novo dado, mais recente, já tenha sido produzido e transmitido, o que torna desnecessário e até contraproducente o esforço de retransmissão do pacote anterior. Em tais casos, redes industriais podem adotar uma política de descarte definitivo desses pacotes considerados obsoletos, de modo a evitar alocar *slots* de comunicação para retransmissões ineficazes. No contexto de falhas por *buffer* cheio, o descarte de pacotes obsoletos configura uma estratégia de mitigação, que visa reduzir perdas mais críticas que poderiam ocorrer em razão do acúmulo de pacotes e da consequente saturação da capacidade de armazenamento dos dispositivos. Como discutido anteriormente, a saturação de *buffers* não impacta apenas o dispositivo local, mas também compromete a confiabilidade de todos os nós posicionados a jusante na cadeia de *uplink*. Dessa forma, o descarte deliberado de pacotes obsoletos representa uma perda de confiabilidade que, no entanto, atua preventivamente na contenção de falhas mais abrangentes, e preserva a estabilidade e a performance da rede. A parametrização do critério de obsolescência deve ser cuidadosamente definida conforme os requisitos da aplicação, uma vez que existem cenários em que não se admite o descarte de pacotes sob nenhuma hipótese, mesmo diante de atrasos ou congestionamentos. Neste trabalho, adota-se a obsolescência como uma das causas de perda ponto a ponto, sendo o TTL o parâmetro utilizado para determinar a validade temporal de um pacote.

Redes com alta exigência de atualização tendem a operar com TTLs mais curtos, já que, nesses contextos, os dados tornam-se obsoletos em intervalos mais curtos. Neste trabalho, o TTL é adotado como parâmetro de descarte configurável pelo usuário. A cada ciclo de *superframe*, cada dispositivo analisa seu *buffer*, e avalia a idade de cada pacote armazenado. Caso a idade ultrapasse o TTL especificado, o pacote é automaticamente descartado. Adicionalmente, foi implementada uma lógica de descarte preventivo, na qual o dispositivo avalia a viabilidade de entrega do pacote com base na distância restante até o destino e no TTL remanescente. Por exemplo, se um pacote se encontra a três saltos do ponto de acesso, mas possui apenas dois *slots* restantes de validade, torna-se evidente que não há tempo suficiente para sua entrega dentro da janela de validade, e justifica seu descarte antecipado. Para fins de simulação, o valor do TTL de cada pacote foi fixado em 5, para possibilitar a observação dos gargalos da rede. A análise dos impactos deste indicador será apresentada no Capítulo 5.

4.8 Identificação de nodos críticos e intervenções

Após a execução da simulação de desempenho da rede, os dados gerados de perda de pacotes e confiabilidade da rede são analisados sob o conceito de centralidades, para encontrar os nodos faltosos (que descartaram pacotes em caráter definitivo) e nodos que geraram pacotes perdidos.

A CI tende a apontar quais cadeias são os principais gargalos para fluxo de dados. Nessas cadeias, a CG aponta os nodos que mais recebem pacotes de vizinhos e, consequentemente, são os primeiros a apresentar *buffer* cheios, enquanto a CP aponta quais nodos nas cadeias geraram maior quantidade de pacotes perdidos.

O software desenvolvido encontra esses três nodos e, se algum deles se repete em mais de um tipo de centralidade, então ele é estabelecido como o nodo crítico da rede. Caso os nodos não se repitam, fica estabelecido como dispositivo crítico aquele que é o dispositivo com maior grau de CI, já que provavelmente tem mais rotas que passam por ele.

A informação de qual é o dispositivo que mais influencia a confiabilidade da rede é armazenada e utilizada no método de intervenção da rede que adiciona mais dispositivos de campo próximo ao nodo crítico. Este é um dos métodos de intervenção utilizados no software desenvolvido, que visam aumentar a confiabilidade de uma RSFI que já esteja em operação.

Os métodos de intervenção foram escolhidos considerando as características da ferramenta DTN para uma RSFI em operação. A aplicação desenvolvida permite que o usuário configure quais métodos quer utilizar, e isso significa que pode ser selecionado mais de um método por simulação. Entretanto, para esta pesquisa, os métodos foram testados isoladamente para permitir a compreensão dos efeitos de cada método sem interferência dos demais. Ao fim de cada reconfiguração da rede simulada, uma nova simulação de desempenho é realizada para analisar a confiabilidade da rede e as métricas utilizadas para tal. Foram definidos três modelos de métodos de intervenção, descritos a seguir.

4.8.1 Simulação de adição de *links*

Uma das informações que a própria rede fornece através do envio do comando 787 está relacionada aos dispositivos que se percebem (estão suficientemente próximos para envio de dados) mas, por alguma razão da lógica inerente ao gerenciador de rede, não são criados enlaces entre eles. Portanto, eles se percebem próximos, mas não enviam pacotes de dados entre si. O comando 787 também informa o RSL recebido deste nodo vizinho. Criar novos enlaces em dispositivos que já estão instalados e pertencem à rede é um método de intervenção que atende aos critérios buscados para a aplicação desenvolvida no trabalho, visto que os métodos definidos devem exigir mínimas intervenções físicas, e oferecer melhor custo-benefício em comparação a instalação de uma rede nova, uma vez

que a aplicação visa otimizar redes que já estão instaladas.

A partir dos dados recebidos de resposta do comando 787, são adicionados todos estes enlaces à matriz PDR e o roteamento da rede é refeito, agora com estes novos enlaces. A depender do RSL recebido, estes novos enlaces podem entrar para a rota principal *uplink* dos dispositivos, ou entrar para a matriz de rotas redundantes. Depois de reconfigurar novamente o roteamento da rede, a RSFI é submetida à simulação de desempenho e os dados são armazenados em arquivos externos.

4.8.2 Simulação de novo roteamento

Outro método que se utiliza de informações fornecidas pela rede e exige mínimas intervenções físicas é definir outro algoritmo de roteamento. Este novo algoritmo de roteamento deve atender às necessidades de uma RSFI (alta confiabilidade, baixo consumo de energia) e ser alimentado com as informações já disponíveis. Existem alguns algoritmos que atendem a esses critérios, e o escolhido foi o algoritmo RPL, devido à sua disponibilidade de implementação, pois já fora testado e implementado em uma RSFI com configurações semelhantes às desta pesquisa em (TIMM, 2022).

Para configurar o novo roteamento, o RSL que cada vizinho informou alimenta a nova base de dados. A partir dela, será gerada uma nova técnica de roteamento na simulação, baseada no algoritmo RPL, formalmente descrito em (ALEXANDER *et al.*, 2012) mas anteriormente utilizado, de forma adaptada, para análise de cargas de pontos de acesso em (ZATS *et al.*, 2011), que utiliza como uma de suas principais variáveis o PDR. Depois de reconfigurar o novo roteamento da rede e as novas rotas redundantes, a RSFI é submetida novamente à simulação de desempenho e os dados obtidos são armazenados em arquivos externos.

4.8.3 Simulação de adição de nodos redundantes

Por fim, o último método escolhido é o único que exige necessariamente intervenção física para ser implementado. Porém, ele foi escolhido por se tratar de adicionar dispositivos sem fio, e que podem ser outros dispositivos de campo, o que permite que seja uma adição que não atenda exclusivamente à otimização da rede em si, já que o dispositivo de campo pode ter outras funcionalidades (sensor, atuador, roteador). Ao considerar um ambiente industrial em constante alteração de *layout*, implementar mais dispositivos de campo em locais estratégicos não é algo que demande uma logística complexa para a maioria dos casos.

No software desenvolvido, o usuário pode configurar quantos dispositivos deseja adicionar próximo ao nodo crítico. A aplicação não limita a quantidade de dispositivos adicionados, entretanto, adicionar dispositivos indefinidamente, além de aumentar o custo da intervenção, não necessariamente traz resultados positivos para a confiabilidade da rede. Em 5.3 serão discutidos com mais detalhes os efeitos de acrescentar muitos dispositivos

próximos ao nodo crítico.

Após a ferramenta identificar o nodo crítico, a quantidade de nodos adicionais informadas pelo usuário é integrada às bases de dados da ferramenta. As características destes novos nodos são semelhantes ao nodo crítico, com leves oscilações para mais ou para menos, para tornar a base de dados mais verossímil. O roteamento da rede é novamente realizado, com esta nova base de dados, porém é forçado a distribuir de maneira uniforme os *links* de rotas *uplinks* do nodo crítico com os novos nodos adicionados.

Após a reconfiguração do roteamento com a adição dos novos dispositivos, a RSFI é submetida novamente à simulação de desempenho e os dados obtidos nesta simulação são armazenados em arquivos externos.

4.9 *Setup* das RSFI utilizadas

Foi implementada uma RSFI em laboratório para estudo de caso, de modo que favorece a formação de gargalos na rede e a redução do RSL entre os dispositivos que compõem a rede. A rede criada é composta pelo gerenciador de rede/*gateway* comercial modelo Emerson 1420, e oito dispositivos de campo. A figura 21 é um esboço de uma planta baixa e exibe a disposição dos elementos da RSFI utilizada no *setup* de testes, onde cada região cinza está separada das demais por alguma barreira física, como lajes de concreto, paredes em alvenaria, portas metálicas e vãos de passagem. Os nomes dos ambientes estão sinalizados, assim como as regiões que se encontram em outros níveis diferentes do andar térreo (onde se encontra o *gateway*) também estão indicadas.

Os dispositivos foram posicionados de modo a ficar o mais distante possíveis do *gateway*, mas conectados à rede por meio de algum enlace, seja diretamente ao *gateway* ou aos demais dispositivos de campo, limitados apenas pelas instalações elétricas e características da edificação. Apenas para fins de comparação, estima-se que o *gateway* e o dispositivo de campo 1015 estejam separados por 4 m, e a distância do andar térreo para a laje seja de 4,5 m. Os dispositivos posicionados no 2° andar estavam próximos ao piso. As regiões apresentadas na Figura 21 tiveram suas proporções mantidas, com margens de erro pequenas o suficiente para não impactar o entendimento da disposição dos elementos da rede. Também é possível observar que somente um dispositivo foi instalado no mesmo ambiente que o *gateway*, entretanto ele não teve facilidade de se conectar com os demais dispositivos da rede, provavelmente devido às características do ambiente do laboratório, que abriga muitos equipamentos eletrônicos, e com isso, acrescentando barreiras para as conexões.

Os enlaces criados entre os dispositivos de campo e o *gateway* são apresentados na Figura 22, de modo a formar a topologia de rede. A figura evidencia que o dispositivo posicionado no mesmo ambiente do gerenciador se conectou apenas a ele e ao dispositivo 1023. Este, por sua vez, estava no andar superior, o que lhe permitiu criar enlaces com

os demais dispositivos e também criou um enlace com o *gateway*, o que implicou em sua inclusão nas rotas *uplink* de vários dispositivos da rede.

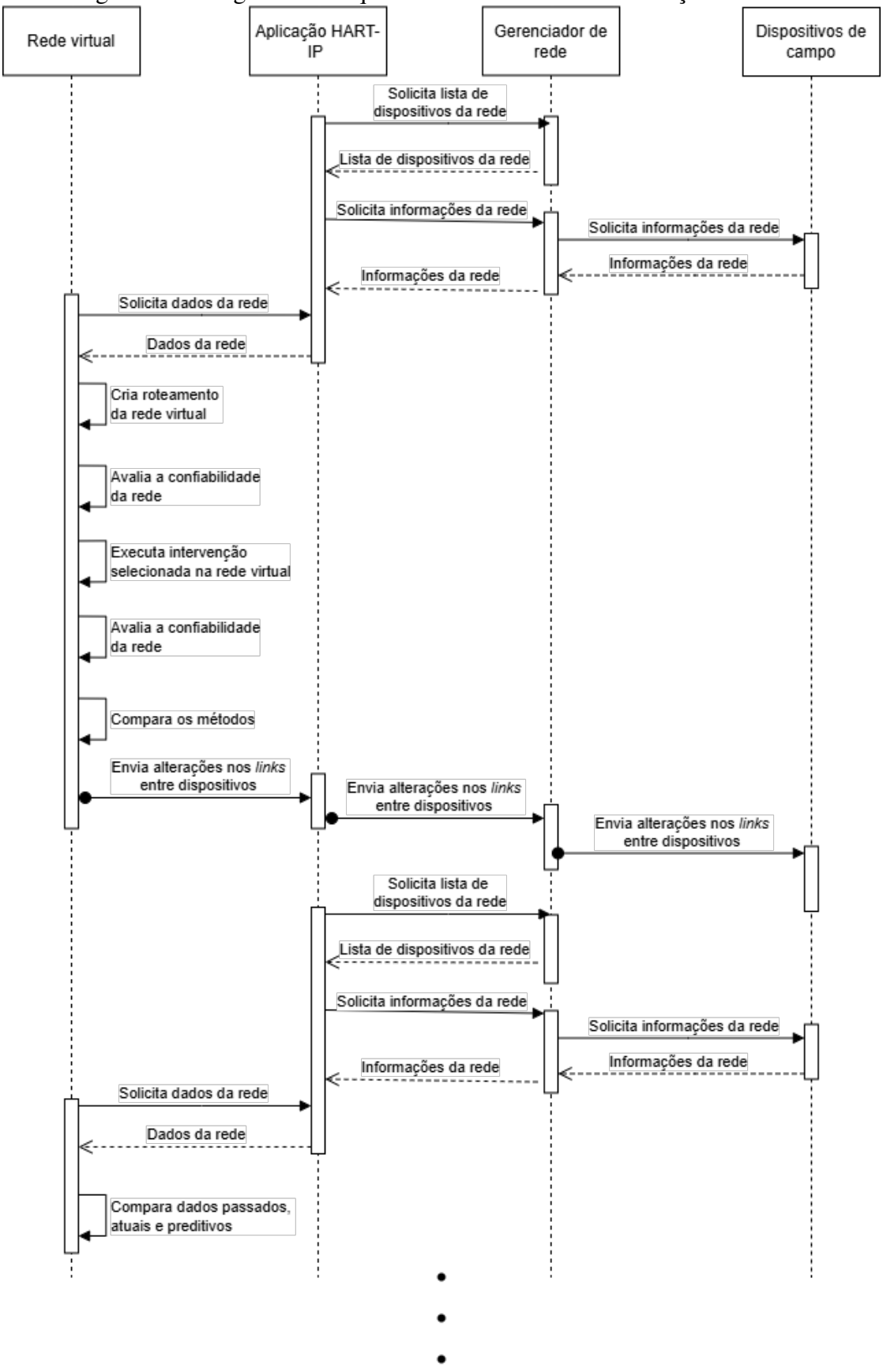
Outro dispositivo que também criou vários enlaces, se comparado aos demais, foi o dispositivo 1022. Entretanto, ele era um dos dispositivos mais afastado do *gateway* nesse teste, o que o colocou em um potencial de rota alternativa para vários dispositivos, de modo que ele também se tornou um ponto de atenção da topologia gerada.

O dispositivo 1015, apesar de estar praticamente equidistante dos dispositivos 1022, 1010 e 1007, criou enlace somente com o dispositivo 1022, bem como criou um enlace com o dispositivo 1005 e não com o dispositivo 1008, o que reforça ainda mais que o dispositivo 1008 tenha sofrido mais interferências para criar seus enlaces, ou ainda pode ter ocorrido o fato de que o gerenciador não dispensou mais banda e criou somente esses enlaces.

O gerenciador criou um número de enlaces para o dispositivo 1007 bem inferior ao número de enlaces do dispositivo 1022, o que pode implicar alguma diferença no *front/back end* entre os dois, já que ambos estavam praticamente na mesma posição. Outra possibilidade, é o que o algoritmo do gerenciador tenha optado por não criar tantas rotas redundantes para poupar *slots* no *superframe*, o que é o mesmo caso dos dispositivos 1010 e 1003.

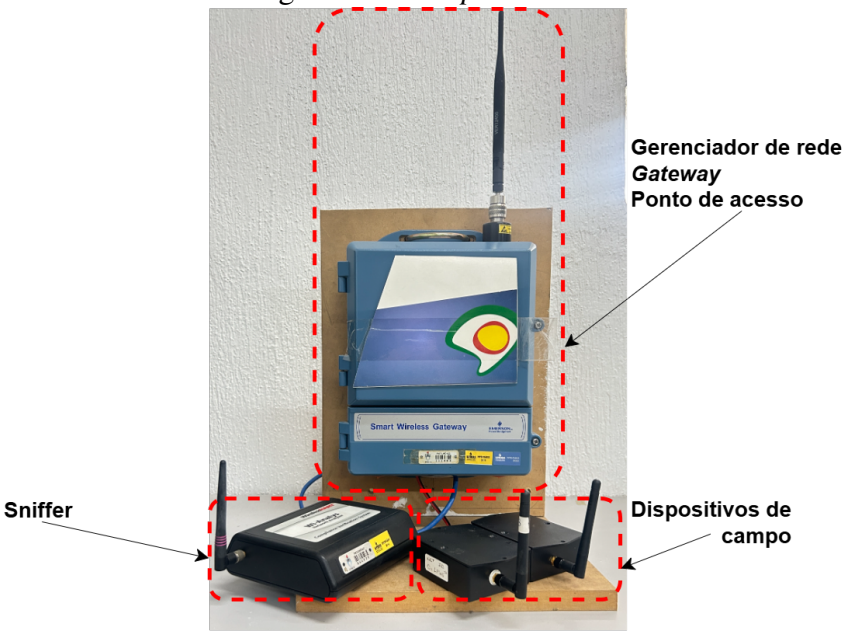
O sistema desenvolvido nesta pesquisa foi submetido a testes em duas RSFI diferentes: a RSFI elaborada conforme apresentado na Figura 21; e uma RSFI ampliada desenvolvida baseada na RSFI implementada. Para a rede ampliada foram acrescentados quarenta dispositivos na rede virtual com características semelhantes aos dispositivos não críticos, ou seja, novos dispositivos que sobrecarregaram ainda mais os dispositivos críticos. O objetivo é observar os impactos dos métodos de intervenção em uma rede maior e com dispositivos críticos ainda mais sobrecarregados.

Figura 10 – Diagrama de sequência do sistema de virtualização da RSFI.



Fonte: autor.

Figura 11 – *Setup* utilizado.



Fonte: autor.

Figura 12 – Ler entradas de dispositivos (*Bytes* de dados de requisição).

0	1	2 3
Código da lista de dispositivos	Número de entradas lidas	Índice da lista inicial

Fonte: autor.

Figura 13 – Ler entradas de dispositivos (*Bytes* de dados de resposta).

0	1	2 3	4 5
Código da lista de dispositivos	Número de entradas lidas	Índice da lista inicial	Número total de entradas na lista

6 7 8 9 10 11
ID exclusivo do dispositivo

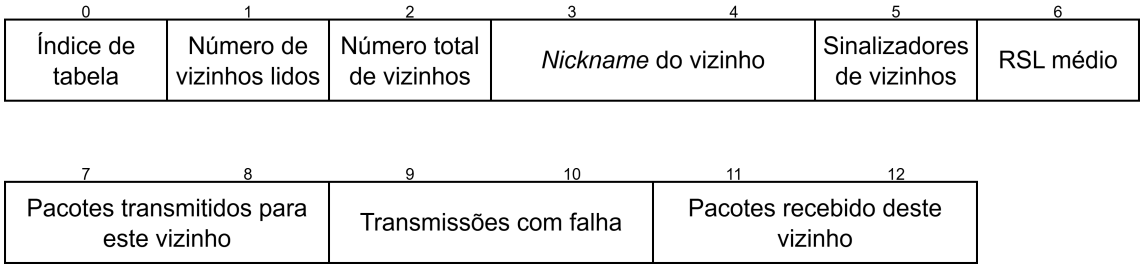
Fonte: autor.

Figura 14 – Relatório de lista de saúde dos vizinhos (*Bytes* de dados de requisição).

0	1
Índice de tabela	Número de vizinhos lidos

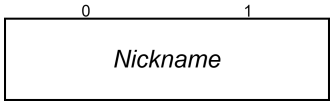
Fonte: autor.

Figura 15 – Relatório de lista de saúde dos vizinhos (*Bytes* de dados de resposta).



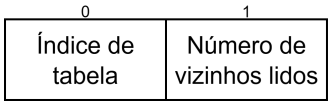
Fonte: autor.

Figura 16 – Ler apelido do dispositivo (*Bytes* de dados de resposta).



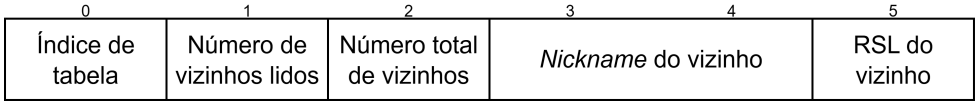
Fonte: autor.

Figura 17 – Relatório de níveis de sinal dos vizinhos (*Bytes* de dados de requisição).



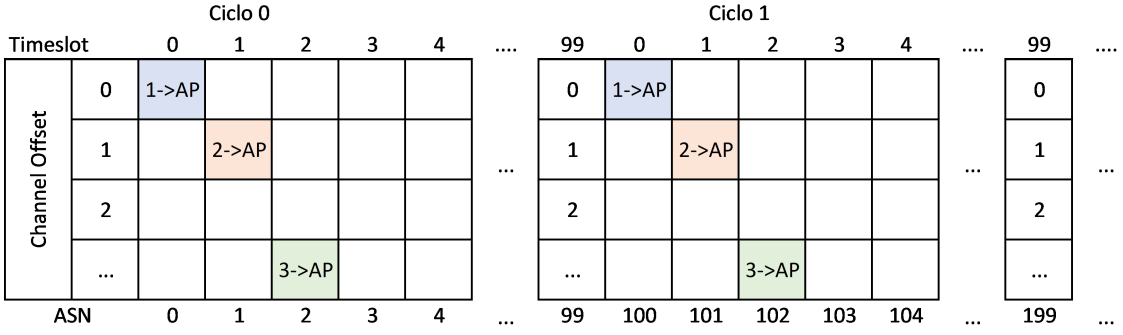
Fonte: autor.

Figura 18 – Relatório de níveis de sinal dos vizinhos (*Bytes* de dados de resposta).



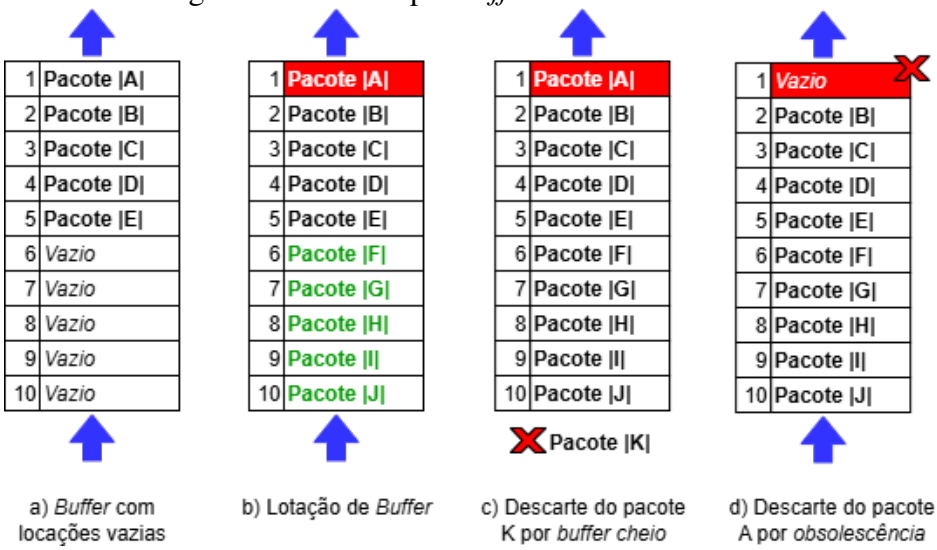
Fonte: autor.

Figura 19 – Ilustração de um *superframe* de 100 *slots* com salto de canais.



Fonte: autor.

Figura 20 – Perdas por *buffer* cheio e obsolência.



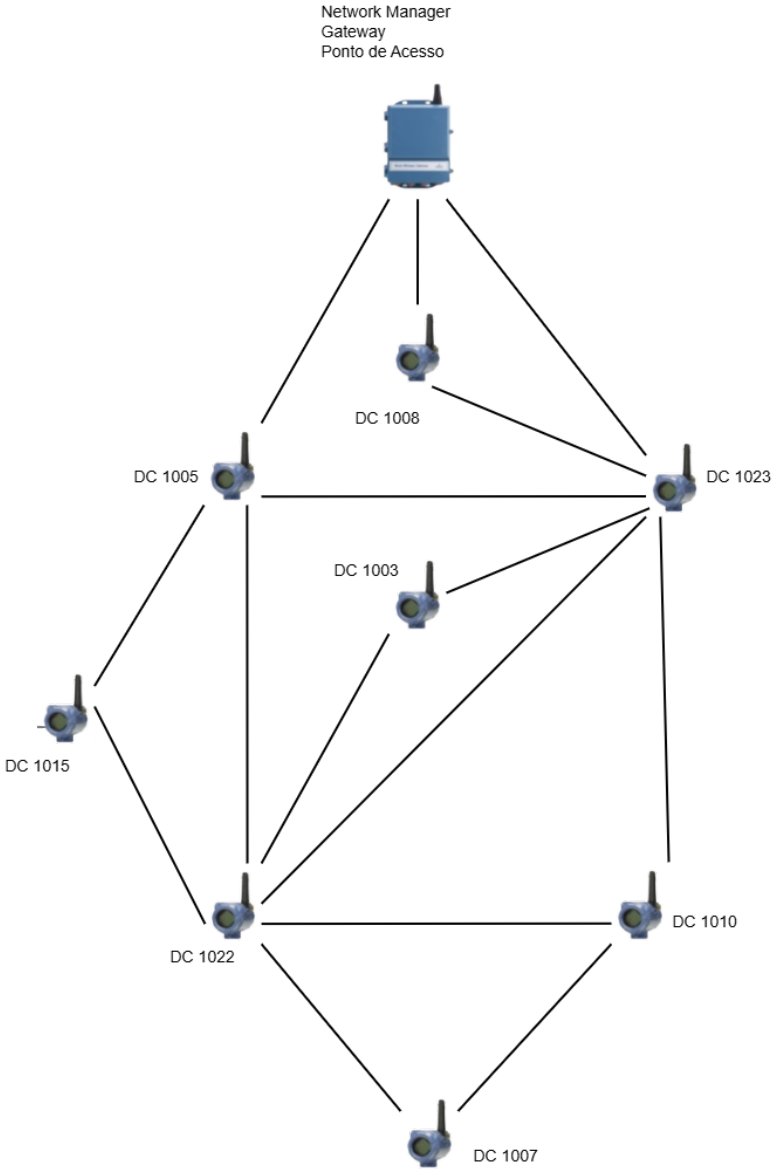
Fonte: Adaptado de (TIMM, 2022).

Figura 21 – Posicionamento dos dispositivos de campo em relação ao *gateway*.



Fonte: autor.

Figura 22 – Grafo gerado pelo Gerenciador da rede.



Fonte: autor.

5 RESULTADOS

Este capítulo apresenta e discute os principais resultados obtidos a partir da aplicação dos métodos e procedimentos descritos anteriormente. São expostos os dados experimentais, as métricas de avaliação e as análises comparativas entre os cenários estudados, com destaque para as contribuições e implicações dos resultados do trabalho.

Os métodos de intervenção na rede foram testados de forma isolada, com o intuito de observar a implicação de cada um deles à confiabilidade da rede. Também foram analisados os impactos dos métodos de intervenção em cada métrica utilizada para mensurar a confiabilidade da rede, a fim de verificar qual métrica teve maior influência na confiabilidade, e com isso, possibilitar análise mais detalhada dos resultados. Foram analisados quatro dados referentes à entrega de pacotes da rede ao final de cada teste:

Pacotes em trânsito: Proporção de pacotes que ainda estavam em trânsito ao final do teste em relação ao total de pacotes criados.

Pacotes perdidos por TTL: Proporção de pacotes descartados por TTL até o final do teste em relação ao total de pacotes que concluíram sua trajetória, seja por alcançarem o dispositivo fim ou por serem descartados de alguma forma. Os pacotes que concluíram sua trajetória são todos os pacotes criados, exceto os que ainda estão em trânsito.

Pacotes perdidos por *buffer* cheio: Proporção de pacotes descartados por *buffer* cheio até o final do teste em relação ao total de pacotes que concluíram sua trajetória, seja por alcançarem o dispositivo fim ou por serem descartados de alguma forma.

Confiabilidade da rede: Proporção de pacotes que alcançaram seu destino final até o final do teste em relação ao total de pacotes que concluíram sua trajetória, seja por alcançarem o dispositivo fim ou por serem descartados de alguma forma.

5.1 Experimentos realizados na rede virtual

Foram realizadas vinte simulações de intervenção em uma rede virtual que espelhava as configurações da rede real mencionada na seção 4.9, a qual foi utilizada para coleta de dados. Considerando que os resultados experimentais sobre a confiabilidade da rede virtualizada apresentaram média igual a $62,223\%$ e desvio padrão de $1,538\%$, a definição

da quantidade de experimentos foi realizada de modo a assegurar um *nível de confiança* de 99%, associado a uma *margem de erro relativa* de $0{,}9\%$. Para este nível de confiança, o valor crítico da distribuição normal padrão é $z = 2{,}576$. A margem de erro absoluta E é definida como uma fração da média observada, sendo expressa por

$$E = 0{,}009 \times 0{,}62223.$$

A relação entre a margem de erro, o desvio padrão e o número de experimentos é dada por

$$E = z \cdot \frac{\sigma}{\sqrt{n}}, \tag{10}$$

em que $\sigma = 0{,}01538$ representa o desvio padrão amostral e n o número de repetições experimentais. Com base nesses parâmetros, foi definido um total de $n = 20$ experimentos, valor suficiente para atender simultaneamente ao nível de confiança de 99% e à margem de erro estabelecida. Observa-se que o baixo valor do desvio padrão em relação à média indica reduzida variabilidade dos dados, o que contribui para a obtenção de um intervalo de confiança estreito mesmo sob critérios estatísticos mais conservadores. Dessa forma, a escolha de realizar vinte experimentos assegura que o valor verdadeiro do parâmetro analisado esteja contido, com alta probabilidade, em uma faixa limitada ao redor da média estimada, conferindo confiabilidade estatística e consistência às análises e conclusões derivadas dos resultados experimentais.

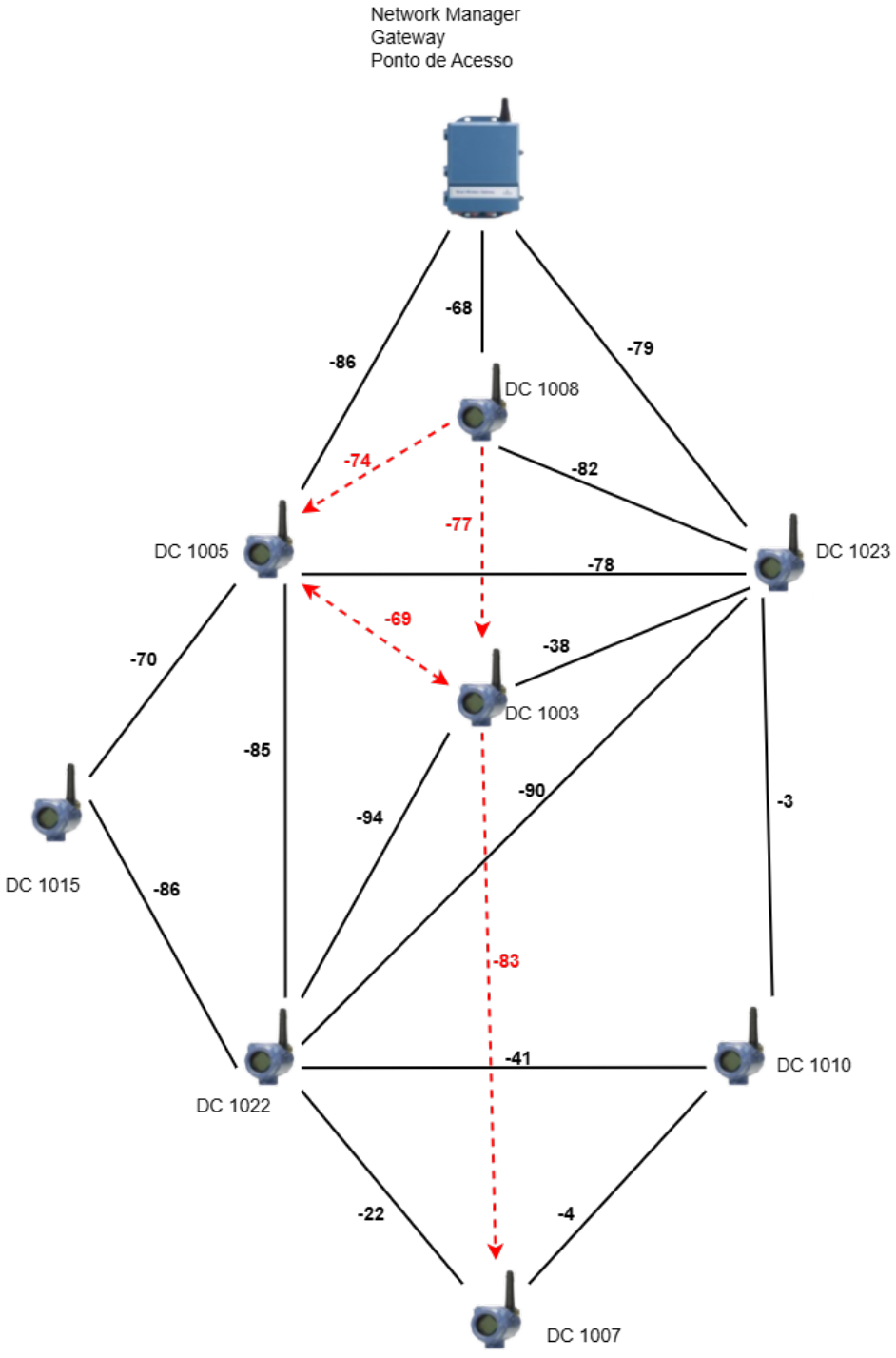
A Figura 23 mostra todos os enlaces existentes da RSFI, juntamente com o peso de cada enlace estabelecido pelo RSL em dBm. A figura também evidencia em linhas tracejadas vermelhas os enlaces não estabelecidos pelo gerenciador de rede, ainda que os dispositivos se percebam. Esses enlaces não estabelecidos representam situações em que o nível de sinal recebido é detectável, porém o gerenciador não configurou uma rota de comunicação. As setas indicam o sentido da tentativa de comunicação e, ao lado de cada linha tracejada estão os valores de RSL associados a cada enlace.

5.1.1 Nodos críticos

No ambiente de simulação da rede virtual foi conduzido um teste com o objetivo de identificar os nodos mais críticos da RSFI. A simulação foi elaborada com base em dados representativos da rede real, como intensidade de sinal e perdas de pacotes. O intuito foi verificar quais nós se configuram como gargalos na transmissão de dados e quais apresentam maior probabilidade de impactar negativamente a confiabilidade global do sistema. Para a CI o sistema identificou o dispositivo de campo 1023; já para a CG o sistema identificou o dispositivo de campo 1022; e, por fim, para a CP o sistema identificou o dispositivo de campo 1010, conforme pode ser observado na Figura 24.

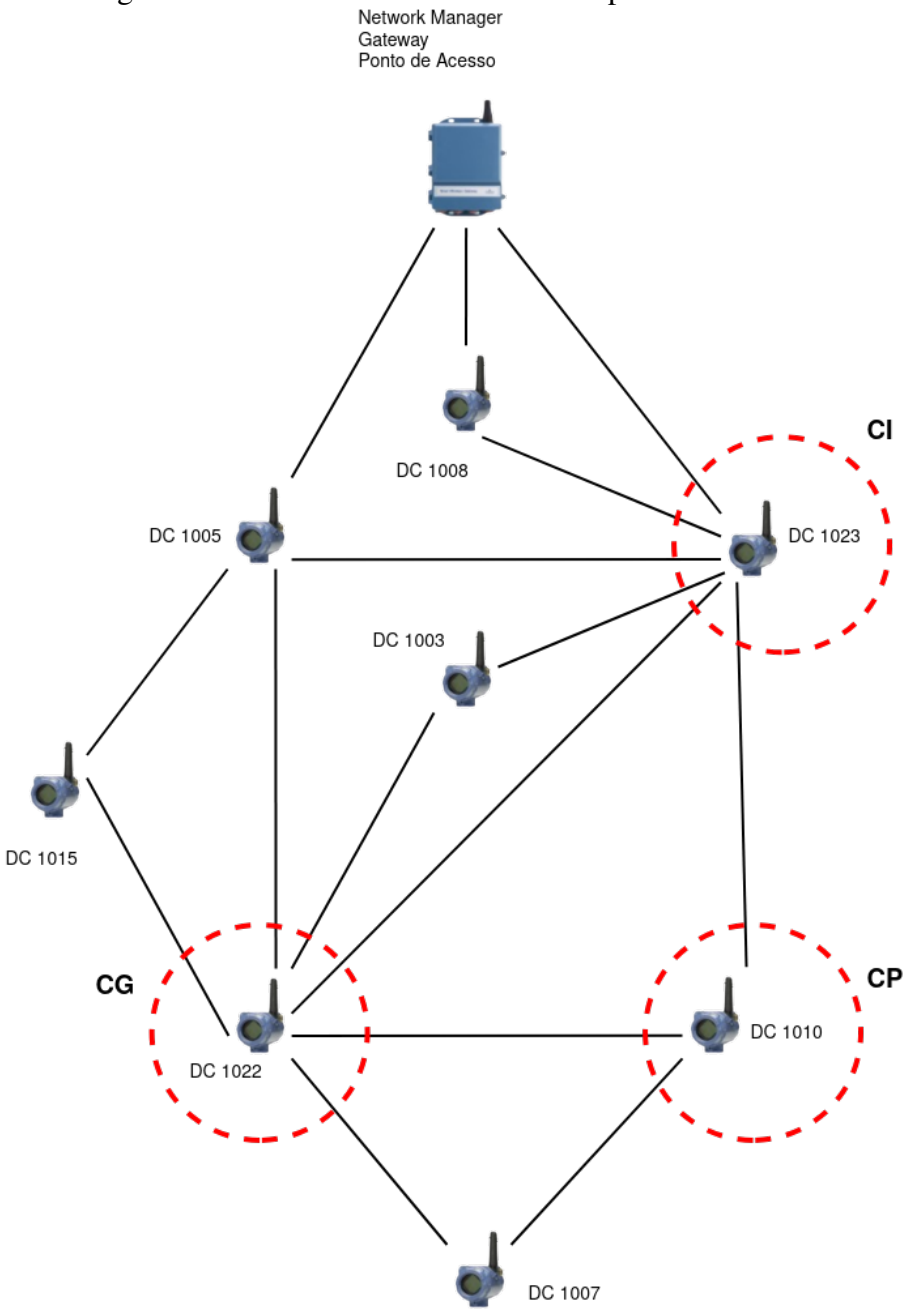
É possível observar que o nodo 1023 tem *links* que o colocam numa posição estratégica entre o Ponto de Acesso e os demais dispositivos da rede. Um detalhe relevante é que

Figura 23 – RSFI evidenciando os enlaces não estabelecidos pelo gerenciador de rede.



Fonte: do autor.

Figura 24 – Resultado das centralidades para a rede simulada.



Fonte: do autor.

este dispositivo foi um dos que mais perdeu pacotes na rede física, ficando atrás apenas do dispositivo 1005 que apresentou um RSL abaixo do dispositivo 1023.

O nodo identificado com maior CG tem a mesma quantidade de enlaces que o 1023, porém os valores de RSL dos seus enlaces estão maiores. O nodo 1022 apresenta RSL com seus vizinhos em média acima de -40 dBm, já o nodo 1023 apresenta RSL com seus vizinhos em média próximos de -78 dBm. Portanto, o nodo 1022 tem, de fato, maior probabilidade de que seus vizinhos criem mais *links* com ele. Também é possível observar na Figura 22 que o dispositivo de campo 1010 tem apenas três *links*, e o enlace mais favorável à rota *uplink*, o dispositivo 1023, tem o RSL de -85 dBm, quase próximo do limite inferior, o que condiz com sua classificação de nodo com maior grau de CP.

Para a realização da simulação, é necessário determinar o nó mais crítico da rede, cuja análise serve como referência para avaliar o impacto das intervenções. Como cada centralidade apontou para um dispositivo diferente, a simulação define que o nodo mais crítico é o nodo identificado com maior CI, que neste caso é o dispositivo 1023. Este nodo identificado como crítico no ambiente simulado coincidiu com aquele que apresentava maior número de falhas e acúmulo de tráfego na rede física dentre os dispositivos que também apresentaram as maiores quantidades de *links* da rede, assim como apresentou qualidade de sinal um pouco acima dos nodos com distâncias semelhantes em relação ao *gateway*. Isso evidencia que a simulação está alinhada com as características físicas da rede real.

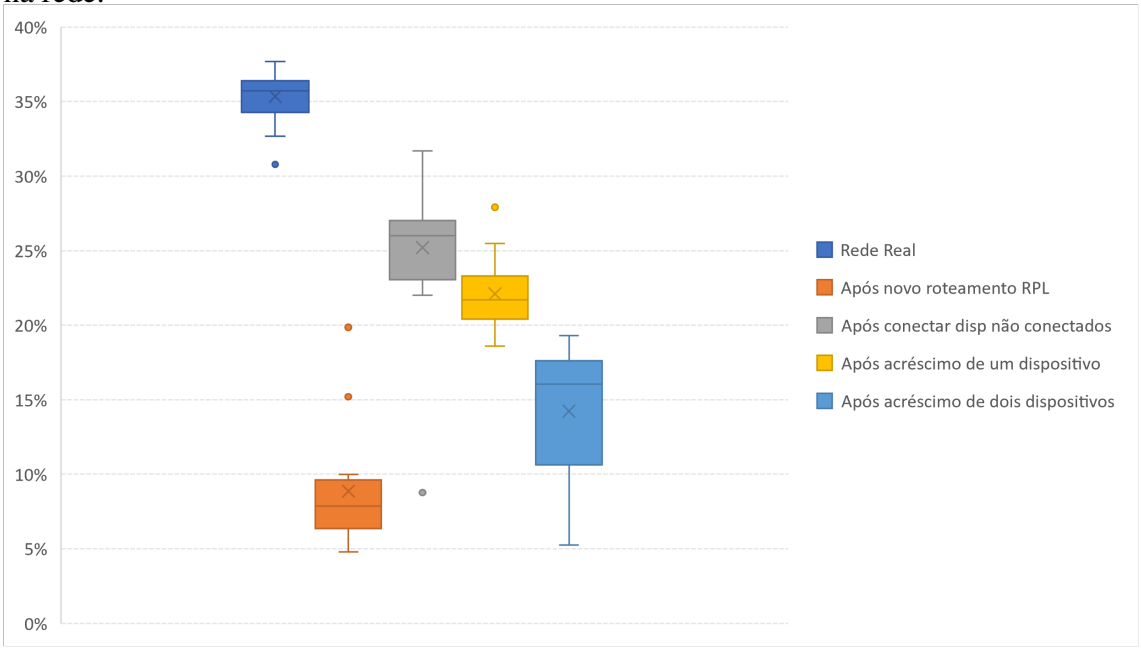
Essa aproximação entre os resultados simulados e a situação real reforça o potencial do uso de DT ou ambientes virtuais de teste para apoiar a tomada de decisão em redes industriais. A identificação prévia do nodo crítico em um modelo simulado possibilita a proposição de intervenções, como a produção de um novo roteamento ou a inserção de dispositivos redundantes, antes da aplicação na rede física. Dessa forma, o processo contribui para reduzir custos, minimizar riscos e aumentar a confiabilidade do sistema, o que configura-o como uma abordagem eficaz e relevante para estudos em redes sem fio industriais.

5.1.2 Pacotes perdidos por TTL

A análise a seguir busca comparar o impacto de diferentes métodos de intervenção sobre as perdas de pacotes decorrentes do TTL dos pacotes na rede. Esse parâmetro é um indicativo importante da eficiência do roteamento, uma vez que valores elevados de perda por TTL sugerem trajetórias excessivamente longas ou ineficientes. Dessa forma, a Figura 25 apresenta uma avaliação quantitativa do comportamento da rede diante das estratégias propostas, permitindo observar como cada método influencia a taxa de entrega e a estabilidade da comunicação entre dispositivos.

O método de intervenção que menos perdeu pacotes por TTL proporcionalmente ao total de pacotes que concluíram sua trajetória, foi o novo roteamento RPL. A conexão de

Figura 25 – Porcentagem de pacotes perdidos por TTL para cada método de intervenção na rede.



Fonte: autor.

dispositivos que se reconhecem mutuamente, mas não possuem um enlace direto entre si, resulta em um desempenho ligeiramente superior ao da rede real. No entanto, este método apresenta o pior desempenho quando comparado às demais abordagens de intervenção. Por outro lado, a introdução de novos dispositivos próximos ao dispositivo crítico gera resultados positivos, com o desempenho melhorando à medida que o número de dispositivos adicionados aumenta.

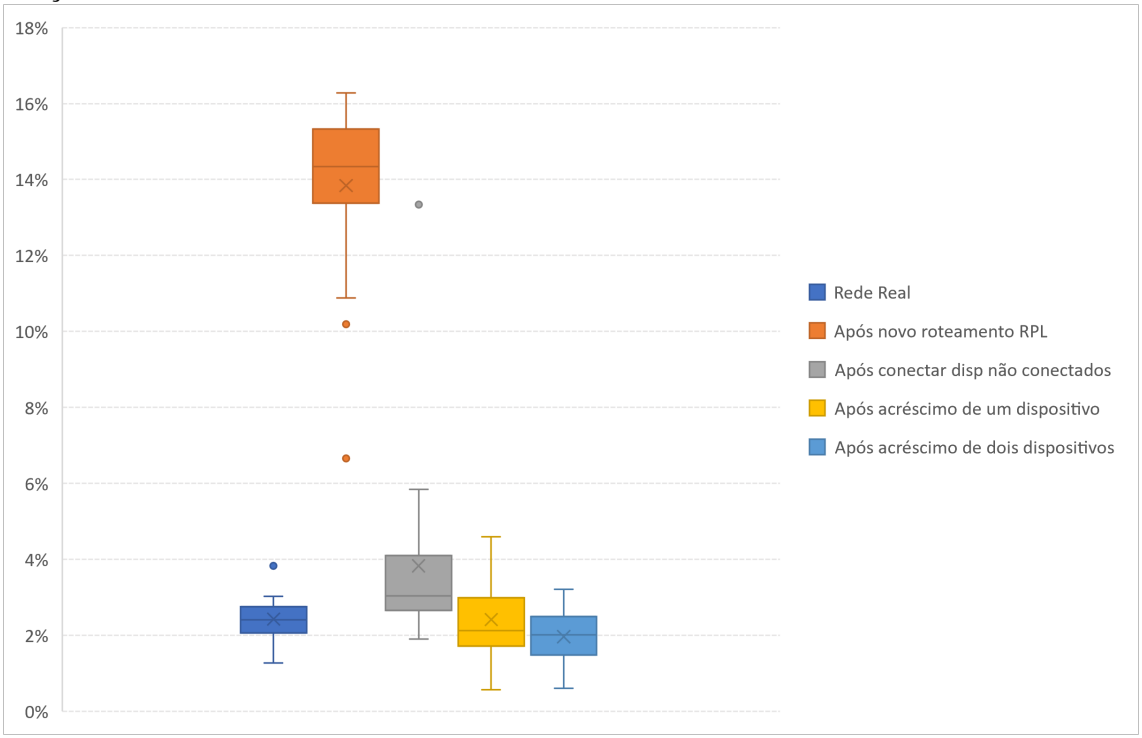
Um detalhe que deve ser mencionado é que metade dos dados obtidos para o acréscimo de dois dispositivos se concentra entre 16% e 19% de perda de pacotes por TTL, enquanto a outra metade está mais dispersa e fica entre 5% e 16% de perda de pacotes por TTL. Com isto, infere-se que este método pode chegar a ter resultados parecidos com o método de intervenção do novo roteamento RPL, entretanto, em média, perde mais pacotes. Este resultado é esperado, pois o roteamento RPL descartou enlaces com baixas taxas de entrega, então diminuiu a possibilidade dos pacotes extrapolarem o TTL, enquanto os demais métodos de intervenção acrescentaram dispositivos e *links* à rede.

5.1.3 Pacotes perdidos por *buffer* cheio

A seguir, é analisado o comportamento da rede em relação às perdas de pacotes causadas por *buffer* cheio, um indicador diretamente associado à capacidade de armazenamento temporário dos dispositivos e ao balanceamento de carga entre os enlaces. Esse tipo de perda está intimamente ligado à eficiência do roteamento e à distribuição do tráfego de dados na rede. Assim, a Figura 26 apresenta a comparação entre os diferentes métodos

de intervenção, destacando como cada abordagem impacta a ocupação dos *buffers* e a consequente estabilidade da comunicação.

Figura 26 – Porcentagem de pacotes perdidos por *buffer* cheio para cada método de intervenção na rede.



Fonte: autor.

A maior proporção de pacotes perdidos por *buffer* cheio em relação ao total de pacotes que concluíram sua trajetória ocorreu no método de intervenção do novo roteamento RPL. Inclusive, também é neste método que os dados estão mais dispersos. Isto ocorreu devido à diminuição de rotas alternativas, o que sobrecarregou os *buffers* dos dispositivos.

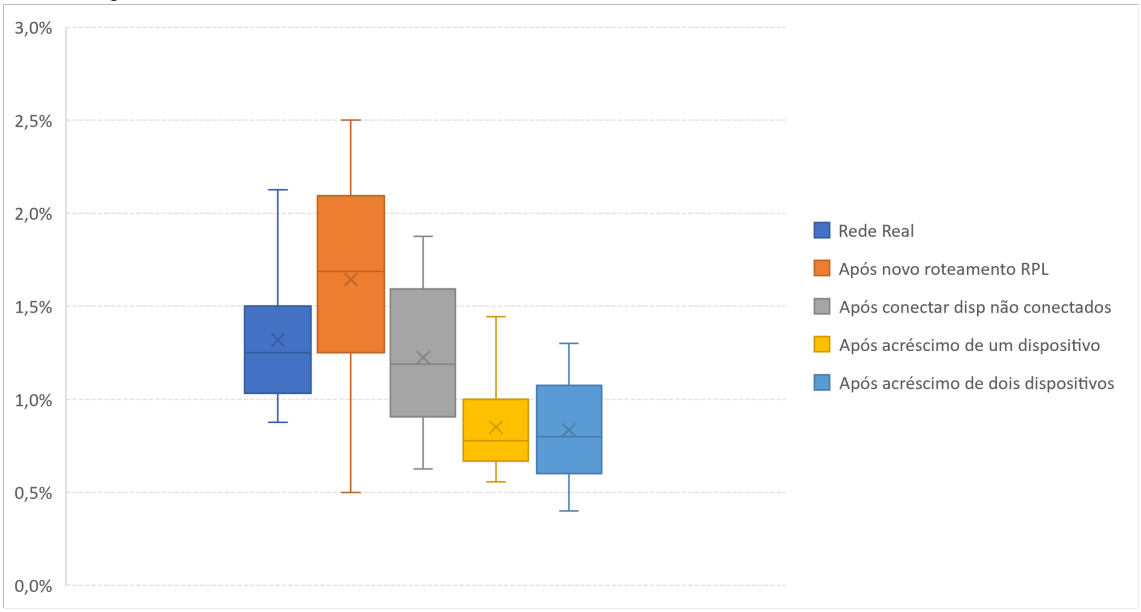
O método de intervenção que enlaça dispositivos que se percebem apresentou maior perda de pacotes por *buffer* cheio, em média, se comparado à rede original. Além disso, os dados estão mais dispersos se comparados à rede original. Isto pode ter ocorrido devido ao acréscimo de dispositivos com enlaces com problemas para entregar os pacotes, o que pode ter sobrecarregado os dispositivos que tentaram enviar por essas novas rotas.

Já o método de acréscimo de novos dispositivos próximos ao dispositivo crítico perdeu, em média, menos pacotes por *buffer* cheio se comparados à rede real. E a dispersão dos dados diminuiu conforme aumentou a quantidade de dispositivos acrescentados, porém ainda mais dispersa que a rede original. Infere-se então que este método diminui a sobrecarga nos *buffers* dos dispositivos da rede, conforme adicionam-se mais dispositivos em pontos estratégicos.

5.1.4 Pacotes em trânsito

Analisar o número de pacotes que permanecem em trânsito ao final da simulação permite avaliar a eficiência global do processo de roteamento, indicando o grau de congestionamento e a capacidade da rede em concluir as transmissões dentro do tempo esperado. Esse parâmetro é relevante para compreender o comportamento dinâmico da rede e a eficácia das intervenções propostas. A Figura 27 apresenta a proporção de pacotes que não alcançaram o destino durante o período de teste, possibilitando comparar o desempenho entre os diferentes métodos de intervenção aplicados. É possível ver que o método que permaneceu com mais pacotes em trânsito foi o novo roteamento RPL, superando o roteamento da rede original. O método de conectar dispositivos que não estão interconectados apresenta uma média de resultados semelhante à da rede real, contudo, com uma maior dispersão nos dados.

Figura 27 – Porcentagem de pacotes em trânsito ao final do teste para cada método de intervenção na rede.



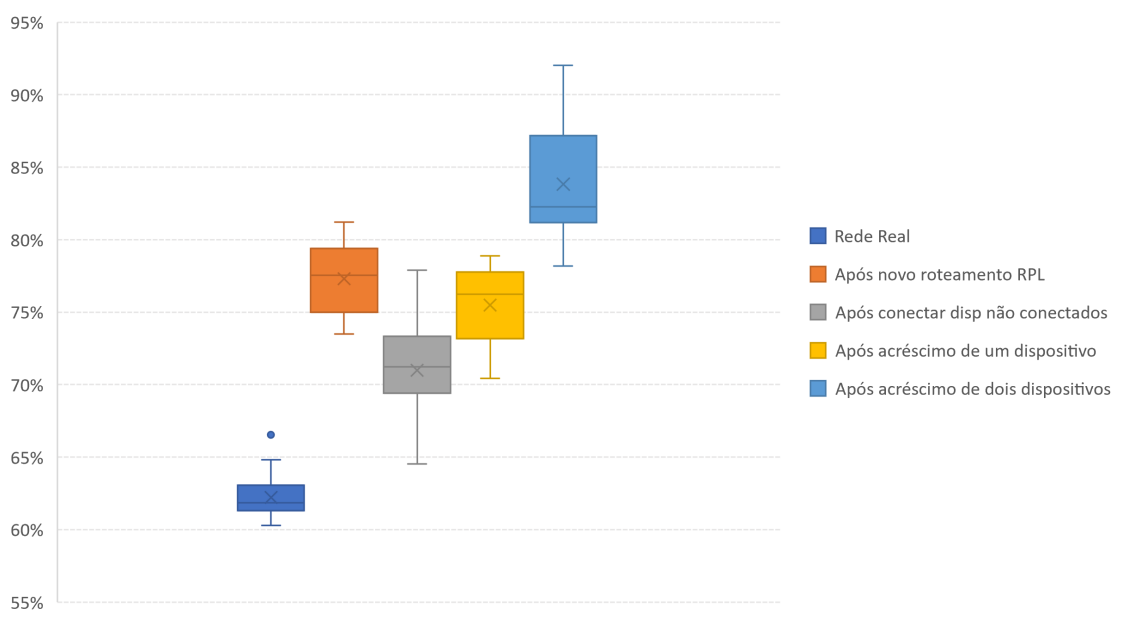
Fonte: autor.

Os métodos que acrescentam novos dispositivos à rede apresentam menos pacotes em trânsito do que a rede real. Exclusivamente neste critério analisado, o acréscimo de mais um dispositivo não impactou positivamente o gráfico, pois a média e a dispersão dos resultados obtidos aumentaram com o acréscimo de mais um dispositivo. Esta observação é um indicador de que aumentar a quantidade de dispositivos próximos ao nodo crítico indefinidamente pode impactar negativamente a rede. O resultado deste efeito é analisado com mais profundidade na seção 5.3.

5.1.5 Confiabilidade da rede

A confiabilidade reflete diretamente a proporção de pacotes entregues com sucesso em relação ao total transmitido. Avaliar esse parâmetro após a aplicação dos diferentes métodos de intervenção permite verificar a efetividade de cada estratégia na melhoria da comunicação e na redução de falhas. A Figura 28 apresenta a comparação entre os resultados obtidos, evidenciando o impacto positivo das intervenções sobre a confiabilidade global da rede. É possível observar que todos os métodos de intervenção tiveram resultados superiores aos da rede real, ou seja, todas as intervenções propostas impactaram positivamente a confiabilidade da rede.

Figura 28 – Confiabilidade da rede após cada método de intervenção.



Fonte: autor.

O método que teve o menor desempenho se comparado aos demais, foi o método de conectar dispositivos que se percebem, mas não estão conectados. Seguido do acréscimo de um dispositivo próximo ao dispositivo crítico, e então o novo roteamento RPL, e por fim o acréscimo de dois dispositivos próximos ao dispositivo crítico. Neste último caso, foi observado um aumento de 92% na confiabilidade da rede.

Os dados obtidos após as intervenções aumentaram a dispersão em relação à rede real, com destaque para o método de conectar dispositivos que se percebem, mas não estão conectados, que variou entre 63% e 78%, a maior dispersão dos métodos, além de ter o menor impacto positivo, em média, na confiabilidade da rede.

5.2 Ampliação da rede virtual

$$E = 0{,}0024 \times 0{,}31548,$$

e sua relação com o desvio padrão e o número de experimentos é dada pela Equação (10) em que $\sigma = 0{,}00288$ representa o desvio padrão amostral e $n = 10$ o número de repetições experimentais.

Diferentemente do caso anterior, em que um maior número de experimentos foi necessário para compensar uma variabilidade mais elevada, os valores obtidos neste conjunto indicam um comportamento altamente estável do sistema analisado. Essa característica permite a utilização de um número reduzido de experimentos sem comprometer a precisão da estimativa da média, uma vez que o intervalo de confiança resultante permanece estreito em relação à magnitude do parâmetro avaliado. Assim, a realização de dez experimentos mostrou-se estatisticamente suficiente para atender ao critério de erro estabelecido, reforçando que a definição do tamanho amostral deve considerar não apenas o nível de confiança desejado, mas também a variabilidade intrínseca dos dados. Essa comparação direta com o estudo anterior evidencia a coerência metodológica adotada e demonstra a adaptação do planejamento experimental às características específicas de cada conjunto de resultados.

A RSFI ampliada utiliza características da mesma rede física já apresentada anteriormente, então os nodos críticos têm os mesmos aspectos detalhados na seção 5.1.1. A Figura 29 ilustra a ampliação da RSFI. O diagrama permite identificar a coexistência dos dispositivos de campo, bem como o papel central desempenhado pelo *gateway* e pelo ponto de acesso na mediação do tráfego de dados e no gerenciamento da rede, evidenciando a disposição espacial dos dispositivos de campo, bem como os enlaces estabelecidos e recém-adicionados após o processo de expansão. As linhas que interligam os dispositivos representam os enlaces ativos da rede, enquanto os valores de RSL estão indicados junto a essas linhas, permitindo a análise direta da intensidade do sinal em cada conexão, e as linhas dos dispositivos que estão agrupados tem o mesmo valor de RSL entre si, pois os dispositivos foram replicados, juntamente com seus enlaces. Essa representação facilita a identificação de enlaces mais robustos ou mais suscetíveis a interferências, contribuindo para a avaliação da qualidade geral da comunicação.

Observa-se que a topologia resultante apresenta maior densidade de conexões e aumento da redundância de algumas rotas, fatores diretamente relacionados à elevação da confiabilidade da comunicação. Essa representação gráfica permite verificar a redistribuição das cargas de transmissão e o surgimento de enlaces adicionais, aspectos que sobrecarregaram os gargalos já existentes impactaram ainda mais a confiabilidade da rede, que está sujeita a interferências eletromagnéticas e obstáculos físicos.

5.2.1 Pacotes perdidos por TTL

Na Figura 30 é apresentado o gráfico *box plot* que analisa os métodos de intervenção, através da métrica de perda de pacotes por TTL proporcionalmente ao total de pacotes que concluíram sua trajetória. Para este caso particular, o método de roteamento RPL perdeu em média 1% menos pacotes que a rede real, enquanto o método de conectar dispositivos que se percebem, mas não têm enlace entre si perdeu mais pacotes que a rede real em média. O método de acréscimo de novos dispositivos próximos ao dispositivo crítico diminui a perda de pacotes por TTL conforme a quantidade de dispositivos acrescentados aumenta.

5.2.2 Pacotes perdidos por *buffer* cheio

A maior proporção de pacotes perdidos por *buffer* cheio em relação ao total de pacotes que concluíram sua trajetória ocorreu no método de intervenção que acrescenta dois dispositivos próximos ao dispositivo crítico.

O único método que obteve resultados positivos em relação à rede real foi o método de conectar dispositivos que se percebem mas não têm enlace entre si, conforme apresentado na Figura 31, o que implica que rotas alternativas têm mais impactos positivos em redes sobrecarregadas, do que em redes equilibradas. Os demais métodos perderam mais pacotes que a rede real, ainda assim são valores baixos, que podem não impactar negativamente em grandes proporções o resultado da confiabilidade da rede, a depender dos demais indicadores.

Um detalhe relevante é que a perda de pacotes por *buffer* cheio cresceu conforme o número de dispositivos acrescidos à rede aumentou, o que pode indicar que existe a possibilidade de diminuir a confiabilidade da rede caso sejam acrescentados dispositivos próximos ao dispositivo crítico indefinidamente. Esse assunto será abordado na seção 5.3.

5.2.3 Pacotes em trânsito

Conforme explanado na seção 5.1.4, analisar os pacotes que ainda estavam em trânsito ao final do teste tem o intuito de monitorar a entrega de pacotes para o destino ou o seu descarte. Na Figura 32 é possível observar que os métodos que permaneceram com mais pacotes em trânsito, em média, foram o método de conectar dispositivos não conectados e o método que acrescenta um dispositivo à rede, sendo que o primeiro apresentou maior dispersão dos dados.

Os métodos do novo roteamento e de acrescentar dois dispositivos à rede obtiveram os melhores resultados com menor média de pacotes em trânsito, com destaque para a média do método de acrescentar dois dispositivos, que foi ligeiramente melhor, com aproximadamente 0,01% menos pacotes em trânsito, porém apresentou dados mais dispersos.

5.2.4 Confiabilidade da rede

Por fim, é apresentado na Figura 33 o gráfico *box plot* dos dados que mensuram a confiabilidade da rede real após cada método de intervenção. É possível observar que, para uma rede sobrecarregada, o método de conectar dispositivos não conectados e o método do novo roteamento RPL não aumentaram significativamente a confiabilidade da rede. Com isso, infere-se que, em redes extremamente sobrecarregadas, somente métodos de alterações de rotas podem não oferecer os resultados esperados.

Por sua vez, os métodos que acrescentam novos dispositivos à rede próximo dos dispositivos críticos aumentaram a confiabilidade da rede conforme foram acrescentados mais dispositivos. O acréscimo de um dispositivo aumentou a média de confiabilidade da rede em quase 4%, enquanto acrescentar dois dispositivos aumentou a média de confiabilidade da rede em quase 6% em relação à rede real.

Num primeiro momento, conforme acrescentam-se dispositivos estratégicos à rede, a confiabilidade da rede aumenta. Porém, como foi mostrado em testes anteriores, alguns indicadores apresentam resultados que pioram conforme são acrescentados mais dispositivos, conforme apresentado a seguir.

5.3 Acréscimo de dispositivos

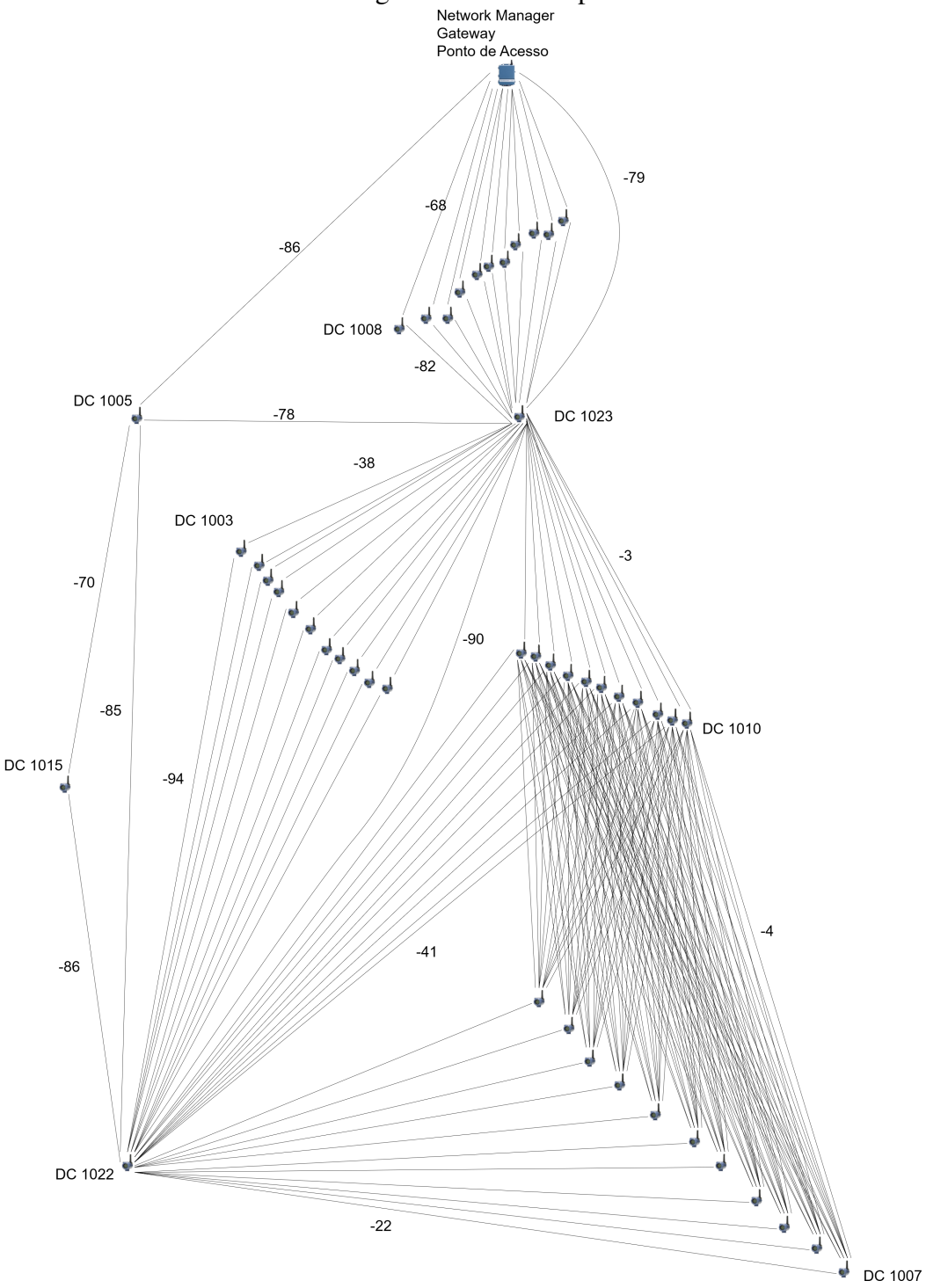
Como mencionado anteriormente, foram realizados vários testes nas redes utilizadas como estudo de caso e, em ambos os casos, a confiabilidade da rede aumentou conforme aumentou a quantidade de dispositivos estratégicos adicionados à rede. Entretanto, alguns indicadores apresentaram resultados que pioraram conforme aumentou a quantidade de dispositivos. Dessa forma, elaborou-se um ensaio experimental com o objetivo de observar se, e em que momento, a confiabilidade da rede deixa de apresentar crescimento proporcional ao acréscimo de novos dispositivos. Tal análise justifica-se pelo fato de que a inserção de dispositivos adicionais implica custos financeiros e logísticos, demandando, portanto, uma estratégia criteriosa para garantir que os benefícios obtidos superem os investimentos realizados. Então, é pertinente avaliar se em algum momento a curva de subida diminui a inclinação ou até regride, a fim de analisar o custo-benefício de tal intervenção.

Na Figura 34 é apresentado o gráfico obtido no ensaio que considerou o acréscimo de novos dispositivos à mesma rede sobrecarregada utilizada no teste anterior. O gráfico apresenta a curva de confiabilidade da rede em relação à quantidade de dispositivos acrescentados. Nota-se que a curva da confiabilidade é quase uma reta até a quantidade de onze dispositivos acrescentados. A partir deste ponto, a curva sobe com oscilações até começar a decrescer a partir de 16 dispositivos acrescentados.

Este experimento evidenciou o que os demais testes indicaram, em que aumentar a quantidade de dispositivos estratégicos à rede deve ser feito com critério e estudado caso

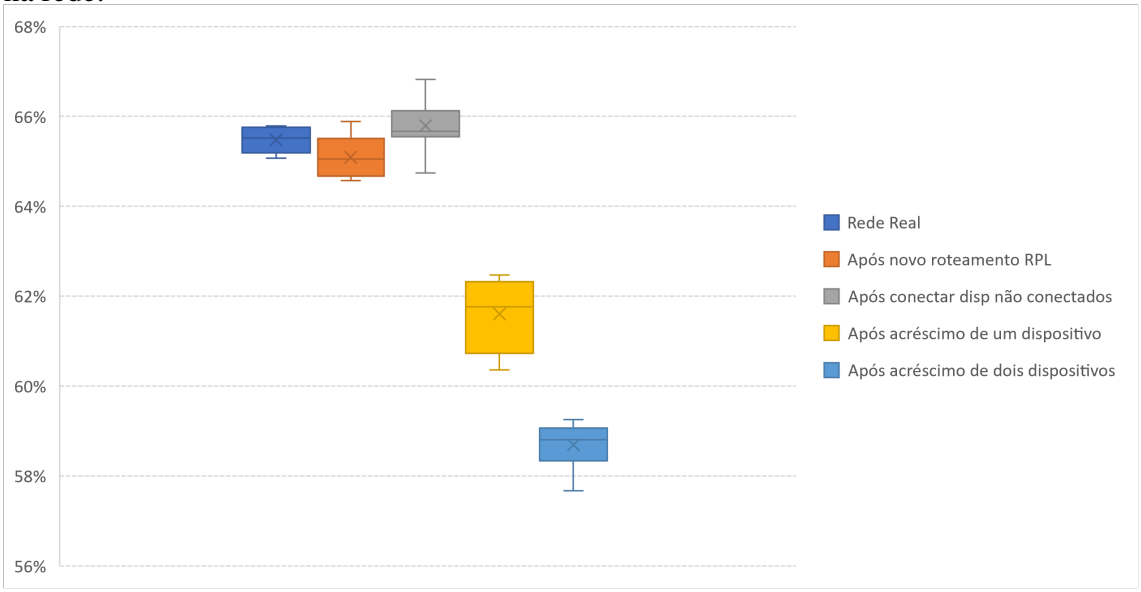
a caso, dentro das possibilidades disponíveis, pois este método satura em algum momento. Para este caso, saturou em quinze dispositivos acrescentados.

Figura 29 – rede ampliada.



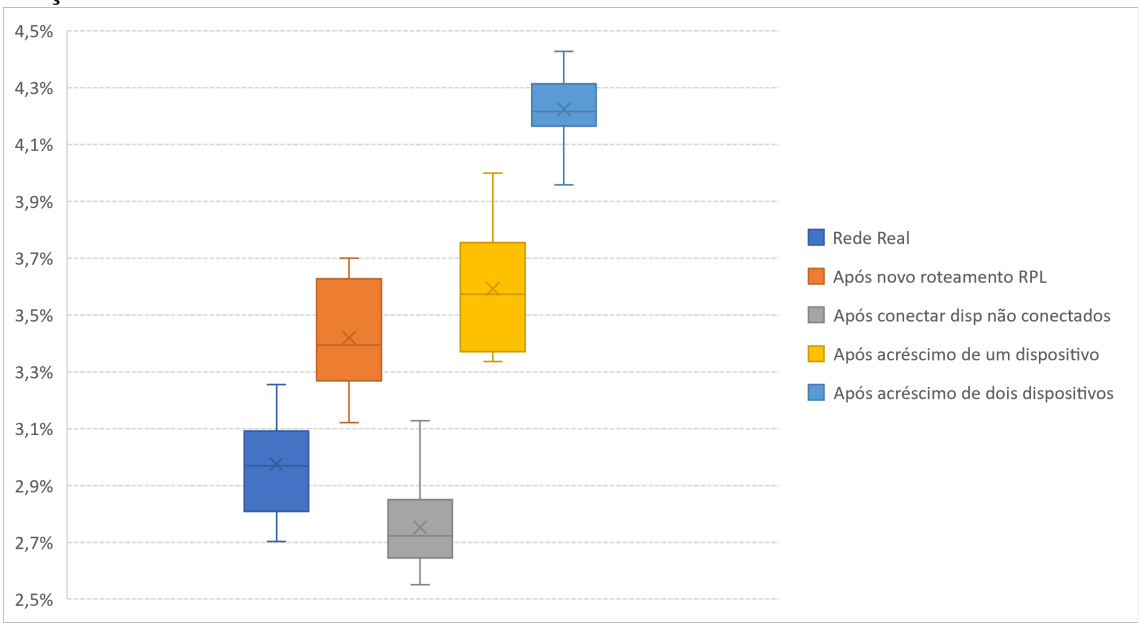
Fonte: autor.

Figura 30 – Porcentagem de pacotes perdidos por TTL para cada método de intervenção na rede.



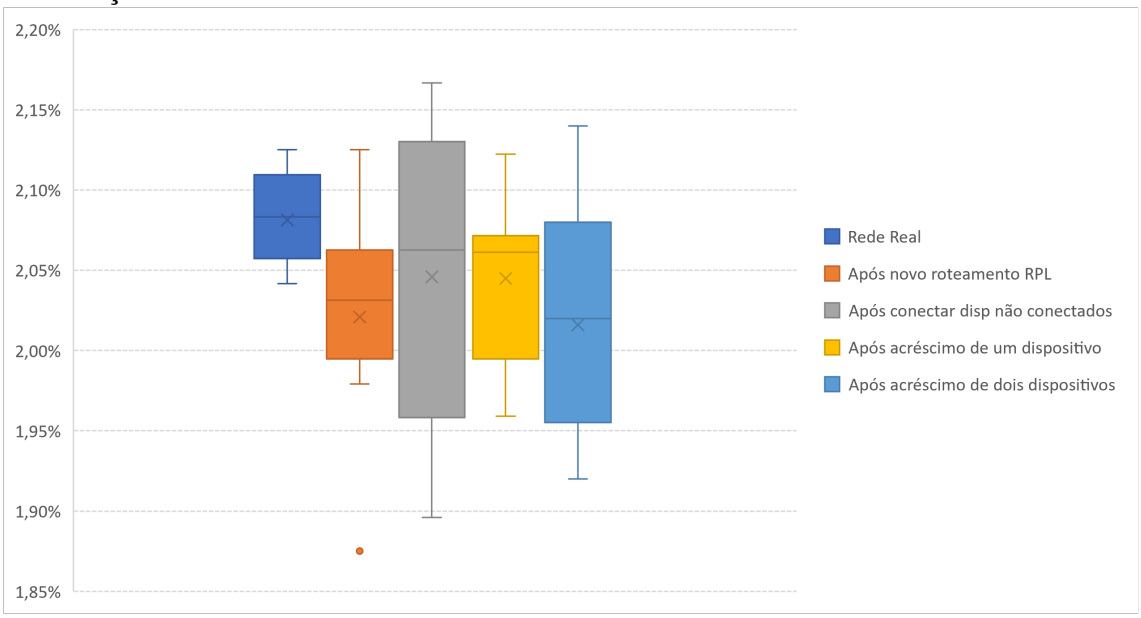
Fonte: autor.

Figura 31 – Porcentagem de pacotes perdidos por *buffer* cheio para cada método de intervenção na rede.



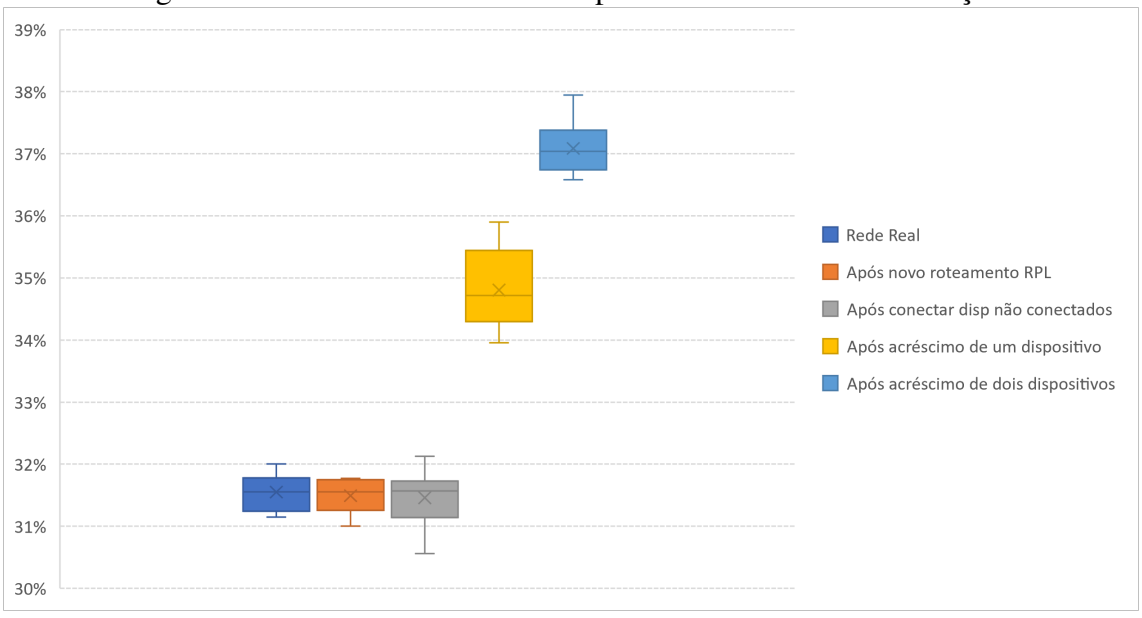
Fonte: autor.

Figura 32 – Porcentagem de pacotes em trânsito ao final do teste para cada método de intervenção na rede.



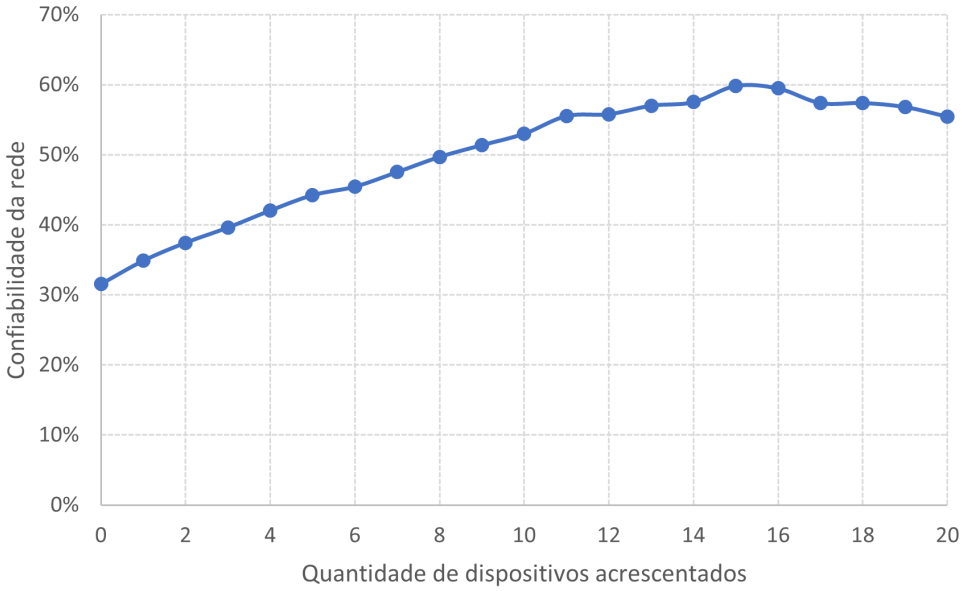
Fonte: autor.

Figura 33 – Confiabilidade da rede após cada método de intervenção.



Fonte: autor.

Figura 34 – Confiabilidade da rede em relação ao total de dispositivos acrescentados.



Fonte: autor.

6 CONCLUSÕES

O uso de DTN em RSFI traz uma série de benefícios que abrangem desde a análise de desempenho até a tomada de decisão estratégica. A principal vantagem está na capacidade de simular e prever o comportamento da rede sob diferentes condições, permitindo a detecção precoce de falhas, gargalos e interferências sem comprometer a operação real. Essa abordagem possibilita testar algoritmos de roteamento, ajustar parâmetros de enlace e avaliar topologias alternativas de forma segura e controlada, resultando em maior confiabilidade e eficiência. Além disso, o DTN reduz custos e riscos operacionais ao eliminar a necessidade de experimentos físicos e minimizar paradas de produção, uma vez que as intervenções podem ser previamente validadas no ambiente virtual. Também oferece uma visão integrada e dinâmica do sistema, combinando dados históricos e em tempo real para subsidiar decisões baseadas em desempenho, custo e confiabilidade. O uso do DTN fortalece a integração entre os domínios físico e virtual, promovendo a retroalimentação contínua e criando bases para a adoção de tecnologias emergentes, como automação avançada, análise preditiva e aprendizado de máquina.

Com o intuito de viabilizar a integração entre a rede física e a rede virtual, foi proposto um sistema capaz de coletar dados de uma RSFI real e armazená-los. Paralelamente, desenvolveu-se um sistema complementar responsável por interpretar estes dados armazenados, criar uma cópia virtual da rede e simular intervenções plausíveis de serem implementadas em curto prazo e com alterações físicas de rápida execução. Os métodos de intervenção estudados foram:

1. Criar enlaces entre dispositivos vizinhos atualmente não conectados;

2. Aplicar novo roteamento com base no algoritmo RPL;

3. Adicionar dispositivos próximos ao nodo mais crítico da rede.

Esses métodos de intervenção foram escolhidos por razões distintas, mas todos compartilham um aspecto fundamental: a viabilidade de implementação em ambientes industriais reais. Em outras palavras, cada método foi concebido considerando as limitações

operacionais, o custo de aplicação e a compatibilidade com os mecanismos de gerenciamento presentes nas RSFI, garantindo que as soluções propostas possam ser reproduzidas sem demandar alterações estruturais significativas na rede física. Assim, além de representarem cenários de simulação consistentes, os métodos adotados refletem estratégias plausíveis de otimização, capazes de serem efetivamente aplicadas na prática para melhorar a confiabilidade e o desempenho da rede. O custo associado a cada método depende diretamente dos resultados alcançados. Os dois primeiros implicam alterações nas rotas de comunicação e demandam o envio de comandos específicos aos elementos da rede. O terceiro, por sua vez, exige a aquisição e instalação de novos dispositivos de campo, além da criação de enlaces adicionais pelo gerenciador de rede. Assim, este último método apresenta maior custo e complexidade logística. Entretanto, por envolver dispositivos sem fio, sua implementação ainda pode ser considerada relativamente simples quando comparada a intervenções em sistemas cabeados.

Com base nas redes utilizadas como estudo de caso, foi possível coletar dados reais, realizar simulações e comparar os resultados obtidos em diferentes cenários de intervenção. As simulações revelaram que o desempenho dos métodos de intervenção varia conforme as características específicas de cada rede, reforçando a relevância da metodologia de desenvolvimento de um DTN, uma vez que cada sistema apresenta particularidades próprias e requer estratégias individualizadas.

6.1 RSFI Implementada

Os experimentos realizados com a rede virtual que reproduziu a RSFI implementada demonstraram que os três métodos de intervenção propostos impactaram positivamente a confiabilidade da rede, ainda que em diferentes magnitudes. O método de acréscimo de dispositivos próximos ao nodo crítico apresentou os melhores resultados, elevando em até 92% a confiabilidade média da rede. O novo roteamento baseado no algoritmo RPL também se destacou por reduzir significativamente as perdas de pacotes por TTL, embora tenha gerado maior descarte de pacotes por *buffer* cheio. Já o método de conectar dispositivos que se percebem, mas não possuem enlace direto, apresentou desempenho inferior, com elevada dispersão nos resultados e impacto positivo mais modesto.

Os resultados confirmam que intervenções físicas e lógicas, mesmo simples, podem aumentar substancialmente a confiabilidade de uma RSFI, especialmente quando aplicadas de forma estratégica e orientadas por métricas de desempenho. A forte correspondência entre os dados simulados e o comportamento da rede real valida o uso da modelagem virtual como instrumento eficaz de apoio à tomada de decisão em RSFI. Assim, a aplicação do conceito de DTN mostrou-se adequada para prever e otimizar o comportamento do sistema antes da implementação de mudanças físicas, reduzindo custos e riscos operacionais.

6.2 RSFI Ampliada

Na RSFI ampliada, observou-se que os métodos de intervenção mantiveram o comportamento geral identificado na rede inicial, porém com variações mais sutis devido à maior complexidade e densidade da topologia. O método de acréscimo de dispositivos próximos ao nodo crítico continuou apresentando os melhores resultados, elevando a confiabilidade média em até 6%. Contudo, verificou-se que, à medida que mais dispositivos são acrescentados, alguns indicadores, como perdas por *buffer* cheio, tendem a se degradar, sugerindo um ponto de saturação.

Os métodos de novo roteamento RPL e de conexão entre dispositivos não conectados apresentaram menor ganho de confiabilidade e maior dispersão nos resultados, indicando que, em redes sobrecarregadas, alterações apenas lógicas nas rotas não são suficientes para restaurar o desempenho. Esses resultados reforçam que a escolha do método de intervenção deve considerar o estado atual da rede, suas limitações de tráfego e a distribuição espacial dos dispositivos. Assim, os testes realizados na RSFI ampliada confirmam a relevância de um processo de análise contínua via DTN para ajustar e equilibrar os parâmetros da rede ao longo do tempo.

6.3 Avaliação dos resultados

A análise dos resultados obtidos nas diferentes topologias avaliadas evidencia que o uso de métodos de intervenção orientados por simulação digital é uma abordagem promissora para o aprimoramento da confiabilidade de RSFI. Todos os métodos testados demonstraram potencial de melhoria, mas o acréscimo de dispositivos próximos aos nodos críticos destacou-se como o mais eficaz, principalmente até o limite de quinze dispositivos adicionais, ponto em que foi observada a saturação da curva de confiabilidade.

O método baseado no algoritmo RPL apresentou desempenho consistente na redução de perdas por TTL, mas também revelou limitações decorrentes da sobrecarga dos *buffers*, especialmente em topologias mais densas. Já o método de conexão entre dispositivos próximos, embora apresente implementação mais simples, mostrou ganhos modestos e maior variabilidade nos resultados. Esses achados indicam que a combinação de intervenções físicas (adição de dispositivos) e lógicas (ajustes de roteamento) tende a produzir melhores resultados quando aplicada de forma integrada e sob análise supervisionada por um ambiente DTN.

Os experimentos comprovaram a validade da abordagem proposta, pois as simulações apresentaram forte correlação com os dados da rede real, confirmando a fidelidade do modelo virtual. Além de contribuir para a previsão do comportamento da rede frente a diferentes cenários de intervenção, a rede virtualizada mostrou-se uma ferramenta eficaz para o planejamento estratégico, reduzindo custos e riscos associados a intervenções diretas na planta física.

Em síntese, os resultados obtidos demonstram que a metodologia desenvolvida é tecnicamente viável e aplicável ao contexto das RSFI. O uso do DTN possibilitou a análise detalhada da confiabilidade, a identificação de gargalos e a simulação de soluções adaptadas a cada cenário, consolidando-se como uma ferramenta de apoio à decisão e otimização contínua de RSFI.

6.4 Trabalhos Futuros

Como trabalho futuro, torna-se relevante avaliar o custo temporal associado ao uso do DTN, considerando tanto o tempo decorrido nas etapas de coleta de dados, análise, simulação e tomada de decisão no ambiente virtual quanto o tempo necessário para que a rede real assimile e reflita as alterações derivadas do DTN. A caracterização desses intervalos temporais permitirá analisar o impacto direto do DTN sobre a confiabilidade da rede, uma vez que atrasos excessivos entre a identificação de gargalos, a definição de intervenções e sua aplicação podem resultar na persistência de condições degradadas, como congestionamento de enlaces, perdas de pacotes e saturação de dispositivos críticos. Além disso, a avaliação do custo temporal torna-se essencial para a escalabilidade da abordagem, pois o aumento do número de dispositivos e enlaces tende a ampliar o tempo de processamento do modelo digital e o ciclo de realimentação entre rede física e virtual. Dessa forma, a análise temporal contribui para identificar limites práticos de aplicação do DTN em redes industriais de maior porte, bem como para orientar o dimensionamento de recursos computacionais e a definição de ciclos de atualização compatíveis com os requisitos de confiabilidade e desempenho operacional da rede.

Como continuidade desta pesquisa, propõe-se o desenvolvimento de uma ferramenta de simulação interativa, capaz de dialogar com o administrador da rede a fim de identificar suas prioridades operacionais, restrições técnicas e metas de desempenho. Com base nessas informações, o sistema poderá comparar automaticamente os resultados das simulações e recomendar o método de intervenção mais apropriado ao perfil e aos objetivos do usuário. Tal aprimoramento visa tornar o processo de análise mais intuitivo, automatizado e alinhado à realidade operacional das redes industriais.

Adicionalmente, recomenda-se o desenvolvimento de uma aplicação destinada ao envio de comandos de escrita ao gerenciador da rede, completando, assim, o ciclo de comunicação do DTN. Essa funcionalidade permitirá a troca bidirecional de informações entre a rede física e sua contraparte virtual, consolidando o conceito de retroalimentação contínua. Embora esta etapa não tenha sido implementada neste trabalho, ela representa um avanço fundamental para o fechamento do ciclo de integração entre os domínios físico e virtual. Como exemplo, em uma RSFI WH existem alguns comandos de escrita, entre eles destacam-se: (i) **Comando 967**, responsável pela criação de novos enlaces; (ii) **Comando 968**, destinado à remoção de enlaces existentes; (iii) **Comando 974**, que permite

criar ou modificar rotas; e (iv) **Comando 975**, utilizado para excluir rotas previamente definidas.

Além disso, propõe-se a exploração da integração do conceito de DTN com técnicas de DRL, as quais possibilitam que agentes autônomos aprendam políticas de decisão em ambientes complexos a partir de interações contínuas e recompensas otimizadas. A combinação entre o DTN e o DRL tem potencial para elevar o nível de autonomia e inteligência da rede, reduzindo o espaço de busca por soluções e priorizando intervenções alinhadas aos critérios de desempenho, custo e logística estabelecidos pelo administrador. Essa integração representa um caminho promissor rumo à implementação de redes industriais cognitivas e autoadaptativas.

Por fim, todos os *scripts* desenvolvidos em *Matlab* e em *Phyton* leitura da rede, simulações e algoritmos de otimização apresentados nesta pesquisa encontram-se disponíveis em repositório público, acessível em:

https://gitlab.com/cristianeprado/dtn.

REFERÊNCIAS

ALEXANDER, R. *et al.* **RPL**: IPv6 Routing Protocol for Low-Power and Lossy Networks. Disponível em: https://datatracker.ietf.org/doc/html/rfc6550. Acesso em: 31 mar. 2024.

AUSIELLO, G.; FIRMANI, D.; LAURA, L. The (betweenness) centrality of critical nodes and network cores. *In*: INTERNATIONAL WIRELESS COMMUNICATIONS AND MOBILE COMPUTING CONFERENCE (IWCMC), 2013., 2013. **Proceedings [...]** [S.l.: s.n.], 2013. p. 90–95.

BALOGH, M.; FöLDVáRI, A.; VARGA, P. Digital Twins in Industry 5.0: challenges in modeling and communication. *In*: NOMS 2023-2023 IEEE/IFIP NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, 2023. **Proceedings [...]** [S.l.: s.n.], 2023. p. 1–6.

BOKHTIAR AL ZAMI, M. *et al.* Digital Twin in Industries: a comprehensive survey. **IEEE Access**, [S.l.], v. 13, p. 47291–47336, 2025.

BONACICH, P. Power and Centrality: a family of measures. **American Journal of Sociology**, [S.l.], v. 92, n. 5, p. 1170–1182, 1987.

BORGATTI, S. P. Centrality and network flow. **Social Networks**, [S.l.], v. 27, n. 1, p. 55–71, 2005.

CHEN, D.; NIXON, M.; MOK, A. **WirelessHART™**: real-time mesh network for industrial automation. [S.l.]: Springer, 2010. 1-276 p.

CHEN, D. *et al.* WirelessHART and IEEE 802.15.4e. *In*: IEEE INTERNATIONAL CONFERENCE ON INDUSTRIAL TECHNOLOGY (ICIT), 2014., 2014. **Proceedings [...]** [S.l.: s.n.], 2014. p. 760–765.

CHEN, D. *et al.* Classification, Building and Orchestration Management of Digital Twin Network Models. *In*: IEEE 22ND INTERNATIONAL CONFERENCE ON COMMUNICATION TECHNOLOGY (ICCT), 2022., 2022. **Proceedings [...]** [S.l.: s.n.], 2022. p. 1843–1846.

CHEN, J. *et al.* Networking Architecture and Key Supporting Technologies for Human Digital Twin in Personalized Healthcare: a comprehensive survey. **IEEE Communications Surveys e Tutorials**, [S.l.], v. 26, n. 1, p. 706–746, 2024.

CHUKHNO, O. *et al.* Placement of Social Digital Twins at the Edge for Beyond 5G IoT Networks. **IEEE Internet of Things Journal**, [S.l.], v. 9, n. 23, p. 23927–23940, 2022.

DE ARAÚJO, D. R.; BASTOS-FILHO, C. J.; MARTINS-FILHO, J. F. Métricas de redes complexas para análise de redes Ópticas. **Revista de Tecnologia da Informacao e Comunicacao**, [S.l.], v. 4, n. 2, p. 11–18, 2014.

FERNáNDEZ-CARAMéS, T. M.; FRAGA-LAMAS, P. Forging the Industrial Metaverse for Industry 5.0: where extended reality, iiot, opportunistic edge computing, and digital twins meet. **IEEE Access**, [S.l.], v. 12, p. 95778–95819, 2024.

FOUNDATION, H. C. **HCF_SPEC-155 - Wireless command specification**. Austin, TX: HFC, 2008.

FREEMAN, L. C. Centrality in social networks: conceptual clarification. **Social Networks**, [S.l.], v. 1, n. 3, p. 215–239, 1979.

GRIEVES, M. **Digital Twin**: manufacturing excellence through virtual factory replication. Disponível em: https://www.3ds.com/fileadmin/PRODUCTS-SERVICES/DELMIA/PDF/Whitepaper/DELMIA-APRISO-Digital-Twin-Whitepaper.pdf. Acesso em: 31 mar. 2024.

GRIEVES, M.; VICKERS, J. Digital twin: mitigating unpredictable, undesirable emergent behavior in complex systems. In: **Transdisciplinary perspectives on complex systems**: new findings and approaches. [S.l.]: Springer, 2016. p. 85–113.

GUO, J. *et al.* Gateway Placement Optimization in LEO Satellite Networks Based on Traffic Estimation. **IEEE Transactions on Vehicular Technology**, [S.l.], v. 70, n. 4, p. 3860–3876, 2021.

GUTIéRREZ GAITáN, M. *et al.* Impact of network centrality on the gateway designation of real-time TSCH networks. *In*: IEEE INTERNATIONAL CONFERENCE ON FACTORY COMMUNICATION SYSTEMS (WFCS), 17., 2021, Linz, Austria. **Proceedings [...]** [S.l.: s.n.], 2021. p. 139–142.

GüEMES-PALAU, C. *et al.* Accelerating Deep Reinforcement Learning for Digital Twin Network Optimization with Evolutionary Strategies. *In*: NOMS 2022-2022 IEEE/IFIP NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, 2022. **Proceedings [...]** [S.l.: s.n.], 2022. p. 1–5.

HAN, B. *et al.* Digital Twins for Industry 4.0 in the 6G Era. **IEEE Open Journal of Vehicular Technology**, [S.l.], v. 4, p. 820–835, 2023.

HARARY, F. **Graph Theory**. Reading, MA, USA: Addison-Wesley, 1972. Many sources cite the original 1969 edition, but the 1972 edition is also widely referenced.

ITANI, M.; SHARAFEDDINE, S. Toward Industrial Metaverse: a high fidelity digital twin for iiot with optimized age-accuracy tradeoff. **IEEE Access**, [S.l.], v. 12, p. 104242–104253, 2024.

KRAUSE, A. *et al.* Digital Twin of the Radio Environment: a novel approach for anomaly detection in wireless networks. *In*: IEEE GLOBECOM WORKSHOPS (GC WKSHPS), 2023., 2023. **Proceedings [...]** [S.l.: s.n.], 2023. p. 1307–1312.

KüNZEL, G.; INDRUSIAK, L. S.; PEREIRA, C. E. Latency and Lifetime Enhancements in Industrial Wireless Sensor Networks: a q-learning approach for graph routing. **IEEE Transactions on Industrial Informatics**, [S.l.], v. 16, n. 8, p. 5617–5625, 2020.

MULLER, I. *et al.* Development of a WirelessHART compatible field device. **2010 IEEE Instrumentation & Measurement Technology Conference Proceedings**, [S.l.], p. 1430–1434, 2010.

PAPOULIS, A.; PILLAI, U. **Probability, Random Variables and Stochastic Processes**. 4. ed. [S.l.]: McGraw-Hill Education, 2001. 864 p.

TANENBAUM, A. **Redes de computadores**. [S.l.]: Elsevier, 2003.

TENNANT, G. **Six Sigma**: spc and tqm in manufacturing and services. 1. ed. [S.l.]: Gower Publishing, 2001. 160 p.

TIMM, D. M. **Escalabilidade Uplink de Redes Industriais Sem Fio com Técnicas de Centralidade**. 2022. 90 p. Dissertação (Mestrado em Engenharia Elétrica) — Universidade Federal do Rio Grande do Sul - Escola de Engenharia Programa de Pós-graduação em Engenharia Elétrica (PPGEE), Porto Alegre, 2022.

VAEZI, M. *et al.* Digital Twins From a Networking Perspective. **IEEE Internet of Things Journal**, [S.l.], v. 9, n. 23, p. 23525–23544, December 2022.

WEI, Z. *et al.* Data-Driven Routing: a typical application of digital twin network. *In*: IEEE 1ST INTERNATIONAL CONFERENCE ON DIGITAL TWINS AND PARALLEL INTELLIGENCE (DTPI), 2021., 2021. **Proceedings [...]** [S.l.: s.n.], 2021. p. 1–4.

WU, Y.; ZHANG, K.; ZHANG, Y. Digital Twin Networks: a survey. **IEEE Internet of Things Journal**, [S.l.], v. 8, p. 13789–13804, September 2021.

XU, H. *et al.* A Survey on Digital Twin for Industrial Internet of Things: applications, technologies and tools. **IEEE Communications Surveys e Tutorials**, [S.l.], v. 25, n. 4, p. 2569–2598, 2023.

YU, Q. *et al.* Synchronous Wireless Sensor and Sink Placement Method Using Dual-Population Co-evolutionary Constrained Multiobjective Optimization Algorithm. **IEEE Transactions on Industrial Informatics**, [S.l.], v. 19, n. 6, p. 7561–7571, 2023.

ZATS, S. *et al.* Scalability of Time Synchronized wireless sensor networking. *In*: IECON 2011 - 37TH ANNUAL CONFERENCE OF THE IEEE INDUSTRIAL ELECTRONICS SOCIETY, 2011. **Proceedings [...]** [S.l.: s.n.], 2011. p. 3011–3016.

ZHANG, Y. *et al.* Adaptive Digital Twin Placement and Transfer in Wireless Computing Power Network. **IEEE Internet of Things Journal**, [S.l.], v. 11, n. 6, p. 10924–10936, 2024.

ZHU, X. *et al.* A location-determination application in WirelessHART. **15th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications**, [S.l.], p. 263–270, 2009.

ZHU, Y. *et al.* A knowledge graph based construction method for Digital Twin Network. *In*: IEEE 1ST INTERNATIONAL CONFERENCE ON DIGITAL TWINS AND PARALLEL INTELLIGENCE (DTPI), 2021., 2021. **Proceedings [...]** [S.l.: s.n.], 2021. p. 362–365.