

Aprendizado por Reforço para Resiliência de Redes IIoT Diante de Falhas de Enlace

Vitor Fagundes Alves Nogueira , Aldri Luiz dos Santos¹

¹Departamento de Ciência da Computação (DCC)

Instituto de Ciências Exatas (ICEX)

Universidade Federal de Minas Gerais (UFMG)

Junho 2025

{vitorfagundes, aldri}@dcc.ufmg.br

Resumo. A Internet das Coisas Industrial (IIoT) tem se tornado fundamental para a modernização de ambientes produtivos, exigindo redes de comunicação cada vez mais robustas e resilientes. No entanto, falhas de enlace representam uma ameaça constante à continuidade das operações industriais, podendo comprometer a qualidade do serviço e paralisar processos críticos. Este trabalho propõe uma abordagem baseada em Aprendizado por Reforço (Reinforcement Learning – RL) para promover a resiliência topológica em redes IIoT. Um agente é treinado em ambiente simulado para detectar falhas e tomar decisões corretivas de forma autônoma, reorganizando a estrutura da rede diante de alterações na conectividade. A proposta visa reduzir o impacto de falhas de comunicação, melhorar a continuidade dos serviços e demonstrar a viabilidade do uso de inteligência artificial para o gerenciamento adaptativo de redes industriais.

Abstract. The Industrial Internet of Things (IIoT) has become essential for modernizing production environments, demanding increasingly robust and resilient communication networks. However, link failures pose a constant threat to operational continuity, potentially degrading service quality and interrupting critical processes. This work proposes a Reinforcement Learning (RL)-based approach to enhance topological resilience in IIoT networks. An agent is trained in a simulated environment to autonomously detect failures and take corrective actions, dynamically reorganizing the network structure in response to connectivity changes. The proposed solution aims to reduce the impact of communication failures, improve service continuity, and demonstrate the feasibility of using artificial intelligence for adaptive management in industrial networks.

1. Introdução

Com o avanço da digitalização nos ambientes industriais, a Internet das Coisas Industrial (IIoT) tem se consolidado como um pilar importante para a automação e otimização de processos produtivos focados na modernização de processos, integração de equipamentos e ampliação da eficiência operacional. De acordo com Masum [Mas23], a IIoT permite a interconexão entre sensores, atuadores e sistemas de controle, promovendo automação, monitoramento em tempo real e tomada de decisão baseada em dados.

A proliferação massiva de dispositivos nesse ecossistema, no entanto, exige uma arquitetura de rede bem organizada, capaz de garantir que os dispositivos possam se comunicar sem interferências para operar serviços básicos, como a coleta e disseminação de dados de forma contínua e confiável. Entretanto, essa crescente dependência traz também novos desafios para a manutenção da conectividade e da resiliência da rede.

Nesse sentido, um dos principais problemas enfrentados em redes IIoT é a ocorrência de falhas de enlace, causadas por interferência, limitações físicas da infraestrutura ou ataques cibernéticos. Tais falhas comprometem a topologia da rede, prejudicando a troca de informações entre dispositivos e, em casos críticos, paralisando operações industriais. Segundo Berger et al. [BER⁺21], sistemas resilientes devem ser capazes de manter seu funcionamento mesmo diante de falhas e se recuperar rapidamente, garantindo níveis mínimos de desempenho. Por outro lado, abordagens tradicionais baseadas em redundância fixa ou reconfiguração manual nem sempre são eficientes, principalmente em ambientes dinâmicos como os de redes IIoT [ZXW⁺24].

Diante disso, cresce o interesse por soluções inteligentes e adaptativas, especialmente aquelas baseadas em técnicas de inteligência artificial. O Aprendizado por Reforço (Reinforcement Learning – RL) destaca-se por permitir que agentes aprendam, por meio de interação com o ambiente, quais ações tomar em diferentes situações para maximizar a continuidade do sistema [KLM96]. Essa técnica é especialmente adequada em cenários onde o agente não possui conhecimento prévio do ambiente e precisa aprender estratégias por tentativa e erro [ADBB17]. Além disso, o RL é eficaz em ambientes desconhecidos e sujeitos a alterações frequentes na topologia da rede.

A literatura tradicionalmente aborda a quebra de enlaces com métodos reativos ou baseados em redundância. Contudo, vista a alta demanda por conectividade e a natureza dinâmica das redes IIoT, essas abordagens se mostram limitadas. Por isso, pesquisas recentes têm explorado o emprego de técnicas de RL, inclusive com modelos mais avançados como o Deep Reinforcement Learning, para restaurar ou reorganizar topologias de redes sem fio de forma resiliente, como demonstrado por Abdelmoaty et al. [AND⁺22].

Dessa forma, este trabalho propõe a aplicação de Aprendizado por Reforço como uma abordagem para aprimorar a resiliência da conectividade topológica em redes IIoT sujeitas a falhas de enlace. A proposta envolve o desenvolvimento de um ambiente simulado no qual um agente, por meio de interações sucessivas, aprende a identificar e responder a falhas de maneira autônoma. O agente será treinado para explorar possíveis ações sobre a topologia da rede e, com base no retorno de suas decisões, construir estratégias eficazes para reestruturar a comunicação entre os nós mesmo em cenários adversos e anômalos na infraestrutura em questão. Essa abordagem permite avaliar, em ambiente controlado, a eficácia de decisões adaptativas que seriam impraticáveis de testar diretamente em ambientes industriais reais. Ao adotar esse caminho, busca-se não apenas demonstrar a viabilidade técnica da proposta, mas também contribuir para soluções mais autônomas e inteligentes aplicáveis a sistemas críticos, nos quais a manutenção da conectividade contínua é essencial para garantir a robustez, a continuidade operacional e a segurança dos processos industriais.

O restante deste artigo está organizado da seguinte forma: a Seção 3 apresenta os conceitos fundamentais para a compreensão da proposta. A Seção 2 revisa os trabalhos relacionados na literatura. A Seção 3.4 detalha a metodologia desenvolvida. A Seção 5

descreve a avaliação preliminar, os resultados parciais e as perspectivas futuras. Por fim, a Seção 6 conclui o trabalho.

2. Trabalhos relacionados

Garantir a conectividade para serviços básicos, como a coleta e disseminação de dados, é um requisito fundamental em redes IIoT. Atingir essa meta de forma robusta impõe diversos desafios, principalmente quando se considera a necessidade de resiliência contra falhas de enlace. A literatura que aborda este problema busca, portanto, responder a questões complexas, como: (i) assegurar a continuidade dos fluxos de dados essenciais mesmo após a perda de um ou mais enlaces; (ii) reconfigurar dinamicamente a topologia da rede para contornar rotas inoperantes de maneira eficiente; e (iii) desenvolver um mecanismo de tomada de decisão que seja autônomo e adaptativo, capaz de aprender a melhor estratégia de recuperação sem intervenção humana. Para endereçar esses desafios de forma integrada, o Aprendizado por Reforço tem se destacado como uma abordagem promissora. Esta seção revisa os principais trabalhos que aplicam RL e outras técnicas de IA para promover a resiliência topológica em redes industriais.

O artigo de Meng et al. [MIK19], propõe o uso de DRL para otimizar a topologia de redes de sensores sem fio auto-organizadas. O estudo investiga como o DRL pode ser empregado para melhorar a eficiência da rede, ajustando sua estrutura de forma dinâmica para atender a requisitos de desempenho, como consumo de energia e resiliência a falhas de enlace. A pesquisa destaca a capacidade do modelo de aprender a reconfigurar a rede em tempo real, o que é particularmente útil para redes IIoT, onde a manutenção da conectividade é crucial. O trabalho demonstra que o uso de DRL pode otimizar significativamente o desempenho da rede sem a necessidade de intervenções manuais, tornando-a uma solução adaptativa e escalável.

Expandindo essa linha de pesquisa, o estudo [LWP⁺23] introduz o algoritmo Advantage Actor Critic-Graph Searching (A2C-GS). A abordagem combina DRL com Redes Neurais Gráficas (GNNs) para otimizar a topologia em ambientes complexos e dinâmicos. Esse algoritmo se destaca pela capacidade de lidar com espaços de topologia de alta dimensão, mantendo a conectividade da rede mesmo quando a infraestrutura sofre alterações ou falhas. Os resultados, testados em diversas configurações de rede, indicam que a sinergia entre DRL e GNNs leva a uma organização mais eficiente e resiliente, o que é fundamental para a operação contínua de sistemas IIoT.

Desviando o foco da otimização de topologia para a detecção de falhas, o trabalho [ZLY⁺20] aborda a identificação de falhas de dispositivos utilizando aprendizado federado e blockchain. Embora não utilize RL, sua relevância está em propor um mecanismo de detecção de anomalias descentralizado e seguro. O aprendizado federado treina modelos de IA localmente nos dispositivos, preservando a privacidade dos dados, enquanto o blockchain garante a integridade e rastreabilidade dos alertas de falha. O estudo evidencia como técnicas de aprendizado de máquina, combinadas com outras tecnologias, podem aumentar a confiabilidade geral das redes industriais.

Em conjunto, os trabalhos analisados demonstram uma clara tendência no uso de Inteligência Artificial para criar redes mais autônomas e resilientes. As abordagens baseadas em DRL e GNNs são eficazes na otimização da topologia, enquanto outras técnicas avançam na detecção de falhas. No entanto, ainda há uma oportunidade para desenvolver

soluções que se concentrem especificamente na recuperação de falhas de enlace em tempo real dentro de estruturas de clusters dinâmicos, como proposto neste artigo. Nossa abordagem busca, portanto, construir sobre essas fundações, aplicando RL para treinar um agente especializado em reconfigurar a conectividade local de clusters de forma rápida e eficiente, garantindo a continuidade operacional no nível topológico da rede IIoT.

3. Mecanismos para controle de falhas de enlace em redes IIoT

Para que o sistema funcione de forma confiável, é importante definir bem o tipo de rede usada, como a comunicação acontece entre os dispositivos e de que forma as falhas podem surgir. Também é necessário entender qual será a “inteligência” do sistema, ou seja, como o agente toma decisões e quais informações ele utiliza para isso. Outro ponto essencial é a arquitetura do sistema: quantos módulos ela terá, como esses módulos se comunicam e qual modelagem será usada para representar a rede, como grafos ou conjuntos. Definir esses elementos permite criar uma estrutura organizada e preparada para lidar com problemas reais de comunicação. Para construir a base desta proposta, esta seção detalha os conceitos essenciais que a fundamentam. O objetivo é contextualizar o desafio de garantir a resiliência em redes IIoT, explorando desde a definição do ambiente industrial conectado, passando pela natureza das falhas de comunicação, até a apresentação do Aprendizado por Reforço (RL) como a ferramenta escolhida para promover a adaptação autônoma da rede.

3.1. Internet das Coisas Industrial (IIoT)

A Internet das Coisas Industrial (IIoT) representa a aplicação do conceito de IoT em ambientes de produção, como fábricas, refinarias e linhas de montagem automatizadas. Mais do que apenas conectar dispositivos, a IIoT promove a convergência entre a Tecnologia da Informação e a Tecnologia da Operação, integrando sensores, atuadores, Controladores Lógicos Programáveis e sistemas de supervisão. A Figura 1 ilustra um modelo conceitual de uma rede industrial. Nesses cenários, a comunicação constante e de baixa latência é crítica, pois sustenta o monitoramento em tempo real, o controle de processos e a tomada de decisão baseada em dados [Mas23]. Portanto, garantir a continuidade e a estabilidade da conectividade é um pilar para a eficiência e segurança das operações industriais.

3.2. Falhas de Enlace em Redes IIoT

Apesar de seu potencial, a IIoT, como qualquer rede, enfrenta desafios relacionados à conectividade segura e estável [HAAS21]. A presença de dispositivos conectados em larga escala, combinada com a complexidade das operações industriais, torna esses sistemas suscetíveis a falhas de comunicação, ameaças cibernéticas e degradações de infraestrutura [855]. Essas vulnerabilidades impactam diretamente o desempenho da rede, comprometendo sua confiabilidade [Mas23]. As redes IIoT, em especial, sofrem com falhas de enlace (ou link) provocadas por interferências de sinal, sobrecarga de tráfego ou interrupções físicas, como ilustrado na Figura 2. Para lidar com esses problemas, soluções tradicionais baseadas em redundância fixa ou monitoramento reativo já não se mostram suficientes, o que reforça a necessidade de abordagens mais inteligentes e adaptativas.

É nesse contexto que o conceito de resiliência se torna central. A resiliência em redes IIoT é essencial para garantir a continuidade dos serviços mesmo diante de falhas

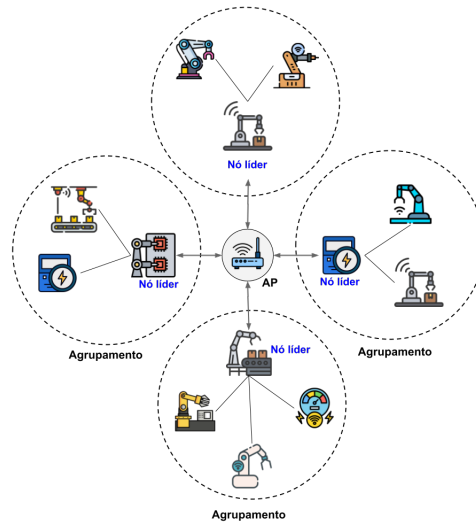


Figura 1. Exemplo de rede IIoT

ou ataques. Segundo Berger et al. [BER⁺21], resiliência consiste na capacidade de um sistema de se recuperar ou se adaptar rapidamente frente a perturbações, mantendo seu funcionamento dentro de níveis aceitáveis. Nesse sentido, a adoção de mecanismos dinâmicos e autônomos, capazes de reagir a falhas de forma eficiente, é fundamental para assegurar a confiabilidade e a disponibilidade das redes IIoT, sustentando a operação contínua de sistemas críticos.

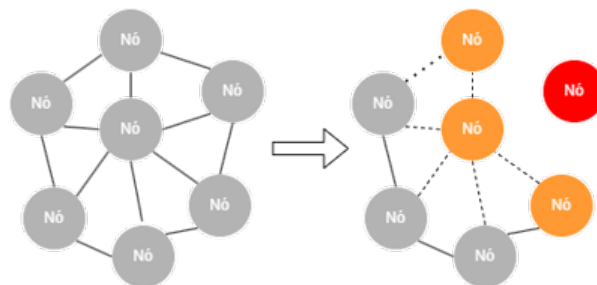


Figura 2. Falha de enlace e sobrecarregamento da rede

3.3. Aprendizado por Reforço (RL)

Dentro do escopo de técnicas de Inteligência Artificial para a construção de sistemas autônomos, o Aprendizado por Reforço (do inglês, Reinforcement Learning - RL) apresenta-se como uma abordagem promissora para o tratamento de falhas de enlace em redes IIoT. O RL é uma área do aprendizado de máquina na qual um agente aprende a tomar decisões por meio da interação com um ambiente. Conforme ilustrado na Figura 3, a cada ação tomada, o agente recebe um feedback na forma de uma recompensa (ou penalidade) e uma observação do novo estado do ambiente. Ao longo do tempo, ele ajusta sua política de decisão para maximizar a recompensa acumulada [ADBB17]. Essa abordagem é especialmente adequada para cenários onde não há um conhecimento prévio completo do ambiente, sendo necessário aprender estratégias por tentativa e erro, como é o caso de topologias de rede IIoT que mudam dinamicamente.

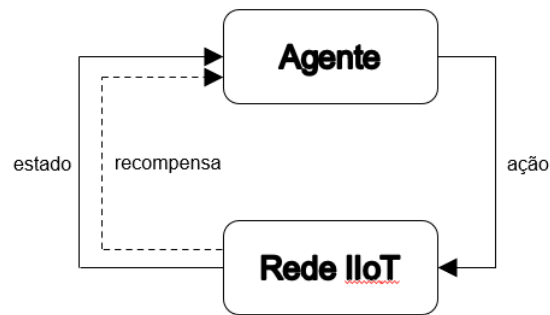


Figura 3. Exemplo de fluxo de agente em aprendizado por reforço

Uma evolução do RL, o Aprendizado por Reforço Profundo (Deep Reinforcement Learning - DRL), utiliza redes neurais profundas para aproximar a função de valor ou a política do agente, permitindo lidar com espaços de estado e ação de alta dimensão. Essa combinação torna o RL aplicável a problemas mais complexos, como a reconfiguração topológica de redes IIoT em tempo real [ADBB17]. Um exemplo de aplicação de DRL foi desenvolvido no trabalho de Abdelmoaty et al. [AND⁺22], no qual os autores propuseram um algoritmo de DRL para projetar uma topologia de backhaul sem fio resiliente. Nesse estudo, o agente foi treinado para decidir quais nós deveriam atuar como hubs e como os enlaces deveriam ser organizados para garantir a conectividade mesmo após falhas. Os resultados demonstraram que a abordagem foi capaz de manter a resiliência da rede com eficiência próxima à de soluções ótimas, mas com menor custo computacional. Esse tipo de aplicação evidencia o potencial do DRL para lidar com falhas em redes IIoT, oferecendo caminhos promissores para manter a conectividade topológica em cenários adversos.

3.4. Funcionamento

Considere uma rede IIoT formada por dispositivos distribuídos em um ambiente industrial simulado. A organização inicial da rede ocorre pela formação dinâmica de agrupamentos, nos quais os dispositivos são classificados com base na sua proximidade espacial, capacidades de comunicação e tipo de dado transmitido. Cada agrupamento, ou cluster, possui um nó líder responsável por coordenar a troca de mensagens internas e estabelecer a comunicação direta com o Access Point (AP). Essa estrutura hierárquica fornece escalabilidade e estabilidade ao tráfego de informações da rede.

No estágio inicial, todos os clusters estão corretamente formados e seus líderes mantêm comunicação estável com o AP. O fluxo de mensagens ocorre de forma contínua: os dispositivos enviam dados, recebem atualizações e executam tarefas sem interrupções aparentes. Essa fase representa o comportamento normal da rede e serve como referência para analisar o impacto de falhas estruturais. A falha considerada neste estudo ocorre no enlace entre o líder de um cluster e o AP. Trata-se de uma falha crítica, pois interrompe a principal rota de comunicação daquele agrupamento. Como consequência, todos os dispositivos daquele cluster tornam-se nós órfãos, perdendo acesso ao restante da rede e deixando de transmitir suas mensagens de forma adequada.

Assim que a falha é detectada, o agente de Aprendizado por Reforço (AR) é acio-

nado. O agente recebe o estado atualizado da rede, identificando o enlace comprometido, o líder afetado e o conjunto de nós órfãos associados. Com base nessas informações, o agente avalia diferentes estratégias de reorganização capazes de restabelecer rapidamente a conectividade da rede. A decisão do agente consiste em selecionar uma nova estrutura de conectividade para integrar novamente os nós órfãos ao fluxo de comunicação. Essa reestruturação pode envolver aproximar dispositivos de clusters vizinhos, redirecioná-los para outro líder próximo ou criar enlaces alternativos por meio de nós intermediários. O agente busca uma solução localizada, intervindo apenas na área afetada pela falha e evitando reconfigurações globais da rede. Essa abordagem reduz significativamente o tempo de recuperação e minimiza o impacto da falha sobre os demais agrupamentos.

Após a seleção da ação, o agente aplica a reorganização proposta. Os nós realocados estabelecem novamente sua conexão com o AP e retomam o fluxo normal de mensagens. Caso a reconfiguração seja eficiente, o tráfego permanece estável e a perda de dados ocasionada pela falha é mínima. A rede continua sua operação com a nova topologia, demonstrando a capacidade adaptativa do sistema diante de interrupções críticas.

3.4.1. Modelagem do Agente de Aprendizado por Reforço

A atuação do agente de AR é formalizada por meio da tripla (S, A, R) , que define o estado observado, o espaço de ações disponíveis e o sistema de recompensas utilizado para guiar o processo de aprendizagem.

Estado (S). O estado da rede no instante t , denotado por S_t , é composto por:

- Topologia atual da rede (G_t), incluindo clusters e líderes;
- Conjunto de nós órfãos (O_t);
- Métricas de conectividade locais (grau, vizinhança, distância ao AP);
- Qualidade de comunicação do enlace antes da falha;
- Custo estimado de mover cada nó (C_{move}).

Formalmente:

$$S_t = (G_t, O_t, \deg(v), \text{dist}(v, AP), C_{move}(v))$$

Ação (A). O agente seleciona uma ação A_t dentre as seguintes possibilidades:

- **ReassignCluster:** realocar nós órfãos para clusters vizinhos;
- **NewLeaderSelect:** eleger novo líder entre nós acessíveis;
- **BridgeCreate:** criar enlace alternativo via nó intermediário;
- **ExpandRange:** mover fisicamente um nó para reaproximação funcional.

Logo:

$$A_t \in \{\text{ReassignCluster}, \text{NewLeaderSelect}, \text{BridgeCreate}, \text{ExpandRange}\}$$

Recompensa (R). A função de recompensa penaliza soluções que causem reestruturações extensas e valoriza ações rápidas e eficientes.

A recompensa é calculada como:

$$R_t = \alpha \cdot \Delta QI - \beta \cdot C_{move} - \gamma \cdot T_{rec}$$

onde:

- ΔQI = ganho no índice de qualidade após a reconfiguração;
- C_{move} = custo total de realocação dos nós órfãos;
- T_{rec} = tempo necessário para restabelecer a conexão com o AP;
- α, β, γ = pesos calibrados empiricamente.

Reforços positivos ocorrem quando o agente restaura a conectividade com custo mínimo; valores negativos aparecem quando a ação aumenta instabilidade ou isola mais dispositivos.

3.4.2. Ciclo de Detecção e Reconfiguração

A seguir apresenta-se o pseudocódigo que descreve o ciclo completo de detecção de falha, avaliação do agente e reconfiguração da rede.

Algorithm 1: Ciclo de Detecção e Reconfiguração da Rede IIoT

```

1 [1] Rede  $G$ , conjunto de clusters  $C$ , agente de AR while rede estiver ativa do
2 end
3 Monitorar enlaces entre líderes e AP if falha detectada em enlace ( $leader, AP$ )
  then
4 end
5 Identificar nós órfãos  $O_t$  Construir estado  $S_t$  Selecionar ação  $A_t = \pi(S_t)$  Aplicar
  ação na topologia  $G$  Atualizar clusters e líderes Avaliar estabilidade da
  comunicação Calcular recompensa  $R_t$  Atualizar política de aprendizado  $\pi$ 

```

4. Avaliação

A metodologia empregada para este trabalho visa o uso de Aprendizado por Reforço para identificar falhas de enlace em redes IIoT e tomar decisões autônomas para realocar os dispositivos da rede, garantindo a continuidade da comunicação e a resiliência topológica. O processo será dividido em três etapas principais: simulação da rede IIoT, treinamento do agente de RL e realocação dinâmica dos dispositivos para restaurar a conectividade da rede. As simulações foram realizadas no simulador NS-3 (versão 3.36), integrado à biblioteca *ns3-gym*, que permite a troca de informações entre o ambiente e o agente de RL. Esse conjunto de ferramentas possibilitou a execução dos cenários em diferentes escalas de rede, incluindo redes com 100, 150 e 200 nós, cada uma executada por 35 rodadas independentes para garantir resultados estatisticamente consistentes. O tempo total de simulação em cada rodada foi de 900 segundos, período suficiente para observar a formação dos clusters, a ocorrência das falhas de enlace e a recuperação realizada pelo agente.

A construção da rede IIoT será feita utilizando uma topologia de clusters dinâmicos, onde os dispositivos serão agrupados com base em suas características semelhantes,

como capacidade de comunicação, proximidade geográfica e tipo de dados transmitidos. Essa estrutura permite uma organização flexível da rede, facilitando a adaptação a falhas de enlace. Quando uma falha de enlace for detectada, o agente de RL avaliará o impacto dessa falha nos clusters existentes e determinará se a realocação de dispositivos é necessária para preservar a conectividade da rede. O modelo de clusters dinâmicos é essencial para garantir que a estrutura da rede possa se adaptar rapidamente às mudanças nas condições de comunicação, mantendo a operação da rede IIoT [PUNS20].

Para definir os clusters dinâmicos, será utilizado um método de similaridade de características entre os dispositivos da rede. As variáveis consideradas incluem a distância entre dispositivos, capacidade de comunicação e os requisitos de processamento de cada dispositivo. A similaridade será calculada utilizando uma métrica de distância, que permite agrupar dispositivos com características semelhantes [PUNS20]. Quando uma falha de enlace é detectada, o agente de RL analisará os clusters afetados e calculará o impacto da falha na conectividade da rede. Com base nesse cálculo, o agente decidirá se os dispositivos precisam ser realocados dentro do mesmo cluster ou se será necessário movê-los para outros clusters próximos, com o objetivo de otimizar a conectividade da rede e minimizar a interrupção na comunicação. Esse processo de realocação será feito de maneira dinâmica, levando em consideração as condições da rede em tempo real.

O treinamento do agente de RL será realizado em um ambiente simulado, onde o agente interage com a rede IIoT para aprender a identificar falhas de enlace e tomar decisões sobre a realocação dos dispositivos [AND⁺22]. Durante o treinamento, o agente receberá uma recompensa ou penalidade com base no sucesso de suas ações, que serão avaliadas em termos de manutenção da conectividade e qualidade do serviço (QoS) da rede. A função de recompensa será projetada para considerar aspectos como o tempo de recuperação da rede, a taxa de falhas detectadas e a eficiência da realocação dos dispositivos. O agente usará técnicas de RL, para aprender as melhores estratégias de realocação. Ele será treinado para mapear a topologia da rede e as falhas de enlace para ações corretivas, como mover dispositivos de um cluster para outro ou reorganizar fluxos de comunicação entre os dispositivos afetados. Durante o treinamento, o agente será exposto a diferentes cenários de falhas de enlace, permitindo que ele aprenda a responder a essas falhas de maneira adaptativa e eficiente.

Uma vez que uma falha de enlace é detectada no sistema, conforme ilustrado na Figura 4, o agente de RL assume a responsabilidade pela recuperação. Sua tarefa é realocar os dispositivos afetados, baseando-se em dois critérios principais: preservar a conectividade e otimizar o desempenho da rede. Para isso, o agente calcula a melhor maneira de redistribuir os dispositivos e executa a realocação dinâmica, como demonstra a Figura 5, onde um novo enlace é estabelecido para contornar a falha. Este processo utiliza funções de agregação, que combinam as informações de conectividade, e de atualização, que ajustam a estrutura da rede, garantindo que a comunicação seja restaurada de maneira rápida e eficiente.

A avaliação do desempenho do agente será realizada com base em diversas métricas de desempenho, incluindo o tempo de recuperação da rede, a taxa de sucesso da realocação e a qualidade da conectividade da rede. As métricas serão analisadas para determinar a eficácia da abordagem proposta em comparação com métodos tradicionais de reconfiguração de rede, como redundância fixa ou reconfiguração manual. O desempenho

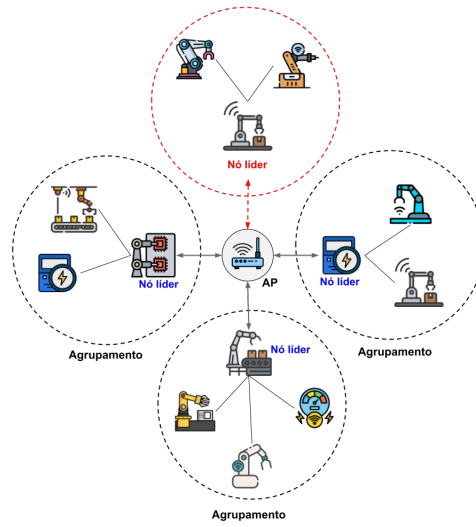


Figura 4. Detecção da falha de enlace

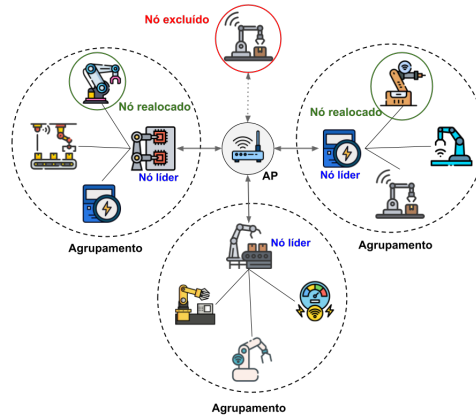


Figura 5. Agente agindo após a identificação da falha

do agente será testado em diferentes cenários simulados para avaliar sua capacidade de se adaptar rapidamente às falhas de enlace e melhorar a resiliência da rede IIoT. O objetivo final é demonstrar que o agente de RL pode não apenas detectar falhas de enlace, mas também realizar a realocação dinâmica de dispositivos de forma autônoma, preservando a continuidade dos serviços e garantindo a resiliência da rede em tempo real.

5. Resultados

Esta seção apresenta os resultados das simulações realizadas com 100, 150 e 200 dispositivos IIoT, considerando três aspectos centrais: (i) a quantidade de tarefas alocadas, (ii) o número de agrupamentos formados, e (iii) o número de nós realocados após a ocorrência de uma falha de enlace. Os resultados ilustrados na Figura 6 mostram que a arquitetura proposta preserva um elevado nível de alocação de tarefas mesmo após a falha. Nos três cenários avaliados, observa-se que o número de tarefas despachadas (TD) permanece muito próximo ao número de tarefas atendidas (TA), com variação mínima entre eles. Essa proximidade entre TD e TA evidencia que o sistema continua processando as tarefas de maneira estável, mesmo diante da interrupção do enlace. Isso indica

que o mecanismo de recuperação atua de forma eficaz, compensando rapidamente a falha e evitando degradação significativa no fluxo operacional. Em outras palavras, o comportamento observado confirma que a estratégia de resiliência implementada é capaz de sustentar tanto o desempenho quanto a continuidade do sistema durante eventos adversos.

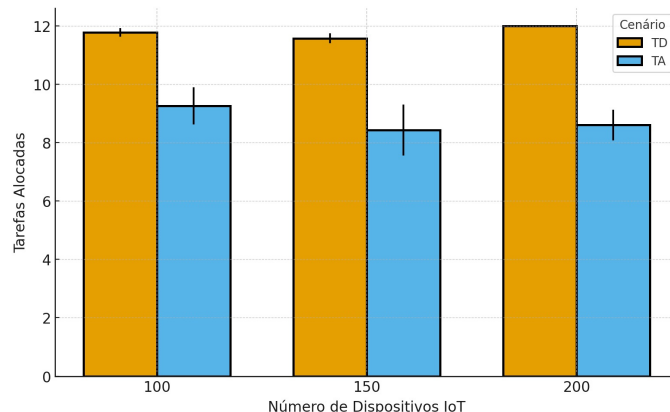


Figura 6. Quantidade de tarefas alocadas nos cenários com 100, 150 e 200 dispositivos IoT.

A Figura 7 evidencia que a maior parte dos agrupamentos formados é composta por clusters Aptos, enquanto os clusters Ociosos aparecem em quantidade significativamente menor nos três cenários analisados. Esse comportamento sugere que o processo de clusterização distribui os dispositivos de maneira estável e equilibrada, evitando tanto a formação de nós isolados quanto a criação de clusters excessivamente desbalanceados. A manutenção dessa proporcionalidade entre grupos Aptos e Ociosos contribui diretamente para a resiliência estrutural da rede, uma vez que a reorganização necessária após uma falha torna-se mínima e localizada. Dessa forma, a rede consegue se recuperar mais rapidamente, preservando seu funcionamento sem exigir alterações profundas na topologia ou realocação massiva de nós.

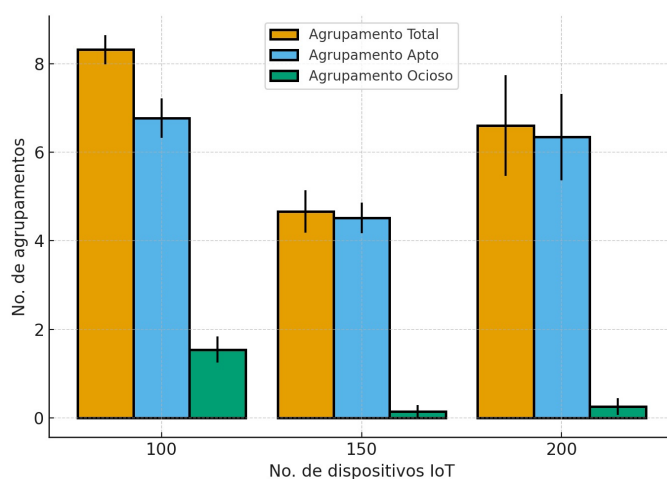


Figura 7. Distribuição dos agrupamentos para diferentes quantidades de dispositivos IoT.

A Figura 8 apresenta o número de nós que precisaram ser realocados após a falha de enlace. Nos cenários com 100 e 150 dispositivos, a média de realocação permaneceu entre 8 e 9 nós, enquanto no cenário com 200 dispositivos esse valor aumentou para apro-

ximadamente 17 nós. Esse crescimento é esperado e proporcional ao tamanho da rede, uma vez que clusters maiores tendem a concentrar mais nós dependentes do líder cujo enlace foi comprometido. Apesar do aumento absoluto, a realocação permanece restrita ao cluster afetado, sem demandar reestruturações globais na topologia. Esse comportamento evidencia que o sistema escala de maneira eficiente, garantindo que o impacto da falha seja contido e que a intervenção necessária permaneça localizada, mesmo em redes de maior porte.

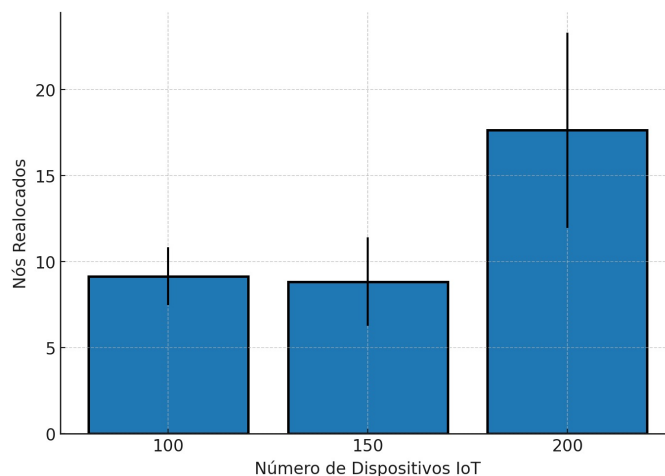


Figura 8. Quantidade de nós realocados após a falha do enlace entre o líder e o AP.

6. Conclusão

Este trabalho apresentou uma metodologia baseada em Aprendizado por Reforço (AR) para aprimorar a resiliência de redes IIoT sujeitas a falhas de enlace. A solução fundamenta-se em uma topologia de clusters dinâmicos, que permite ao agente identificar interrupções na conectividade e reagir de maneira inteligente e adaptativa. Os resultados demonstram que a adaptação dinâmica da topologia, combinada à tomada de decisão autônoma do agente, mantém a continuidade do serviço mesmo diante de falhas, redirecionando eficientemente as demandas de comunicação por rotas alternativas e preservando o funcionamento global da rede. Esse mecanismo de reconfiguração fortalece a operação resiliente da IIoT ao possibilitar ajustes estruturais sem intervenção humana e com impacto mínimo na execução das tarefas industriais. A fase preliminar de simulações validou a viabilidade da abordagem e evidenciou seu potencial para aplicação em cenários industriais mais complexos. Como trabalhos futuros, pretende-se aumentar a fidelidade do ambiente utilizando o simulador NS-3, aperfeiçoar o agente de AR para lidar com múltiplos tipos de falhas e condições adversas, avaliar seu desempenho em topologias mais densas e heterogêneas, e explorar implementações práticas que aproximem a solução de contextos industriais reais.

Referências

- Uma pesquisa sobre a internet das coisas industrial: Uma perspectiva de sistemas ciberfísicos. *Acesso IEEE*, 6.
- Kai Arulkumaran, Marc Peter Deisenroth, Miles Brundage, and Anil Anthony Bharath. Deep reinforcement learning: A brief survey. *IEEE Signal Processing Magazine*, 34(6):26–38, 2017.

- Ahmed Abdelmoaty, Diala Naboulsi, Ghassan Dahman, Gwenael Poitau, and Francois Gagnon. Resilient topology design for wireless backhaul: A deep reinforcement learning approach. *IEEE Wireless Communications Letters*, 11(12):2532–2536, 2022.
- Christian Berger, Philipp Eichhammer, Hans P Reiser, Jörg Domaschka, Franz J Hauck, and Gerhard Habiger. A survey on resilience in the iot: Taxonomy, classification, and discussion of resilience mechanisms. *ACM Computing Surveys (CSUR)*, 54(7):1–39, 2021.
- Abhishek Hazra, Mainak Adhikari, Tarachand Amgoth, and Satish Narayana Srirama. A comprehensive survey on interoperability for iiot: Taxonomy, standards, and future directions. *ACM Comput. Surv.*, 55(1), November 2021.
- Leslie Pack Kaelbling, Michael L Littman, and Andrew W Moore. Reinforcement learning: A survey. *Journal of artificial intelligence research*, 4:237–285, 1996.
- Zhuoran Li, Xing Wang, Ling Pan, Lin Zhu, Zhendong Wang, Junlan Feng, Chao Deng, and Longbo Huang. Network topology optimization via deep reinforcement learning. *IEEE Transactions on Communications*, 71(5):2847–2859, 2023.
- Rahat Masum. Cyber security in smart manufacturing (threats, landscapes challenges). *arXiv preprint arXiv:2304.10180*, 2023.
- Xiangyue Meng, Hazer Inaltekin, and Brian Krongold. Deep reinforcement learning-based topology optimization for self-organized wireless sensor networks. In *2019 IEEE global communications conference (GLOBECOM)*, pages 1–6. IEEE, 2019.
- Carlos Pedroso, Yan Uehara, Michele Nogueira, and Aldri Santos. Atribuições cooperativas de tarefas de sensoriamento baseada em consenso relacional para redes iiot. In *Workshop de Gerência e Operação de Redes e Serviços (WGRS)*, pages 195–208. SBC, 2020.
- Weishan Zhang, Qinghua Lu, Qiuyu Yu, Zhaotong Li, Yue Liu, Sin Kit Lo, Shiping Chen, Xiwei Xu, and Liming Zhu. Blockchain-based federated learning for device failure detection in industrial iot. *IEEE Internet of Things Journal*, 8(7):5926–5937, 2020.
- Tianyu Zhang, Chuanyu Xue, Jiachen Wang, Zelin Yun, Natong Lin, and Song Han. A survey on industrial internet of things (iiot) testbeds for connectivity research, 2024.