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

TIAGO RODRIGO CRUZ

ESTRATÉGIAS PARA USO DE REDES INDUSTRIAIS SEM FIO DO TIPO TSCH EM APLICAÇÕES DE MOBILIDADE

Porto Alegre
2021

TIAGO RODRIGO CRUZ

ESTRATÉGIAS PARA USO DE REDES INDUSTRIAIS SEM FIO DO TIPO TSCH EM APLICAÇÕES DE MOBILIDADE

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

ORIENTADOR: Prof. Dr. Ivan Müller

Porto Alegre
2021

TIAGO RODRIGO CRUZ

ESTRATÉGIAS PARA USO DE REDES INDUSTRIAIS SEM FIO DO TIPO TSCH EM APLICAÇÕES DE MOBILIDADE

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. Edison Pignaton de Freitas, UFRGS
Doutor pela Universidade de Halmstad – Suécia

Prof. Dr. Ivanovitch Medeiros Dantas da Silva, UFRN
Doutor pela Universidade Federal do Rio Grande do Norte – Brasil

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

Coordenador do PPGEE: _____
Prof. Dr. Sérgio Luís Haffner

Porto Alegre, março de 2021.

RESUMO

A utilização de redes sem fio para aplicações industriais surge como uma alternativa para os sistemas cabeados por apresentarem características como flexibilidade de ampliação ou atualização de dispositivos na rede e facilidade de instalação e manutenção. Protocolos de comunicação para redes sem fio industriais, como *Wireless*HART, foram desenvolvidos para atender a requisitos de operação do setor industrial garantindo entrega de mensagens em tempo real, segurança e confiabilidade. O protocolo *Wireless*HART foi desenvolvido para atender aplicações de automação de processos, onde as variáveis do processo são alteradas de forma lenta. Quando inseridos elementos de alta dinamicidade, como a presença de dispositivos móveis ou intermitentes, como nos processos de automação fabril, há um impacto negativo no desempenho destas redes devido à rápida mudança de topologia que não é prevista neste protocolo, e que resultam na redução da taxa de sucesso de transmissões. Dentro deste contexto, este trabalho apresenta a análise dos requisitos e a implementação de dispositivos móveis ou intermitentes e gerenciadores de rede em conformidade com a técnica TSCH (*Time Synchronized Channel Hopping)*, como a empregada no *Wireless*HART. São propostas modificações em procedimentos do protocolo utilizado como base, visando fornecer o suporte a dispositivos móveis que incluem técnicas para agilizar o processo de conexão e desconexão e manter a conectividade do dispositivo enquanto ele se movimenta pela área de cobertura da rede. Os resultados revelam a viabilidade das técnicas propostas, porém, em detrimento de algumas características fundamentais, tais como segurança e baixo consumo de energia. Para mitigar os problemas gerados, são apresentadas propostas a serem implementadas em trabalhos futuros.

Palavras-chave: Redes sem fio industriais, Protocolo WirelessHART, *Handover*, Automação de processos e fabril.

ABSTRACT

The use of wireless networks for industrial applications appears as an alternative for wired systems due to its characteristics such as flexibility to add or remove devices on the network and ease of maintenance and installation. Communication protocols for industrial wireless networks, such as *Wireless*HART, were developed to meet the operating requirements of the industrial sector ensuring real-time communications, security and reliability. The *Wireless*HART protocol was developed to operate in process automation applications, where process variables are changed slowly. When high dynamics elements are inserted in these networks, such as the presence of mobile or intermittent devices, as seen in factory automation processes, there is a negative impact on the performance of these networks due to the fast topology change that is not supported in this protocol, resulting in the reduction of success rate of transmissions. In this context, this work presents the analysis of requirements and the implementation of mobile or intermittent devices and network managers in accordance with the TSCH (Time Synchronized Channel Hopping) technique, which is used in *Wireless*HART. Modifications to the procedures of the protocol used as a basis are proposed, aiming to provide support for mobile devices including techniques to reduce time in processes as connection and disconnection and maintain the connectivity of the device while it moves through the network coverage area. The results show the feasibility of the proposed techniques, however, to the detriment of some fundamental characteristics, such as safety and low energy consumption. In order to mitigate the problems generated, proposals are presented to be implemented in future works.

Keywords: Industrial wireless networks, *Wireless*HART protocol, Handover, Process and factory automation.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ACK	*Acknowledgement*
ANOVA	*Analysis of Variance*
ASN	*Absolut Slot Number*
BER	*Bit Error Rate*
CCA	*Clear Channel Assessment*
CRC	*Cyclic Redundancy Check*
DLPDU	*Data-Link Protocol Data Unit*
DSSS	*Direct Sequence Spread Spectrum*
FDAP	*Field Device Access Point*
FHSS	*Frequency Hopping Spread Spectrum*
ISM	*Industrial Scientific andMedical*
LAN	*Listen Advertise Network*
LANm	*Listen Advertise Network for mobile devices*
LCA	*Listen for Close Advertises*
MIC	*Message Integrity Code*
PV	*Primary Variable*
QoS	*Quality of Service*
RF	Radiofrequência
RSL	*Received Signal Level*
RSSF	Redes de Sensores Sem fio
RSSFI	Redes de Sensores Sem Fio Industrias
RSSI	*Received Signal Strength Indicator*
SNR	*Signal-to-Noise Ratio*
TDMA	*Time Division Multiple Access*
TSCH	*Time Synchronized Channel Hopping*
WH	*Wireless*HART

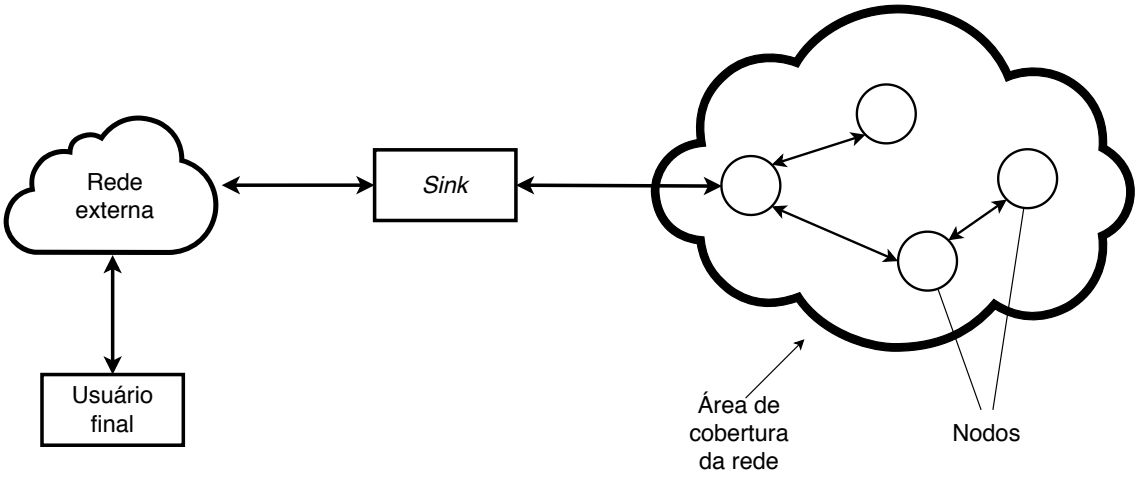
SUMÁRIO

1 INTRODUÇÃO

O estudo de Redes de Sensores Sem Fio (RSSF) tem atraído a atenção de pesquisadores e cientistas nos últimos anos devido a sua potencial aplicação em diversas áreas aliado a suas principais características como capacidade de lidar com falha de nodo, baixo custo de implementação, flexibilidade de ampliação e implementação em ambientes severos ou de difícil acesso. De forma geral pode-se classificar as aplicações em dois grandes grupos: rastreamento e monitoramento remotos. Como exemplos podem-se citar: na área de saúde com o contínuo monitoramento de pacientes e possibilidade de atualização de registros médicos em tempo real; na área industrial com o monitoramento de parâmetros de equipamentos ou rastreamento de dispositivos móveis; na área residencial auxiliando na automação residencial ou detecção de incêndio em edifícios (YANG, 2014); entre outras como na área de meio ambiente, militar, agricultura, segurança e vigilância (RAMSON; MONI, 2017).

Em linhas gerais, pode-se descrever o funcionamento de uma RSSF como uma série de sensores e atuadores, utilizados para monitorar e controlar condições de um determinado ambiente, que se comunicam entre si para transmitir seus dados para um elemento central da rede ou transmitir ações de controle para atuadores. A Figura 1 representa a estrutura típica de uma RSSF e seus principais componentes. A rede é formada por nodos, que podem assumir topologias tanto em estrela como em malha. Estes nodos podem ter funções como sensorear, retransmitir e trocar informações com outras redes. Para atender as funções de sensoreamento e retransmissão, os nodos são compostos por transdutores e rádio transceptores, além de um microcontrolador para processar a variável medida e uma fonte de alimentação. Na Figura 1 também é possível observar o fluxo das comunicações na rede, onde os dados coletados pelos nodos sensores são enviados para o nodo *sink*, que atua como um *gateway* permitindo a comunicação com outras redes para que os dados

Figura 1 – Estrutura de uma RSSF.



Fonte: adaptado de (YANG, 2014)

cheguem ao usuário final. A comunicação é bidirecional, o que permite o controle de atividade de sensores e de atuadores (YANG, 2014).

Em especial, as aplicações industriais apresentam características diferentes nos canais de comunicação sem fio quando comparadas com aplicações em outros ambientes, como por exemplo, o residencial. Isso porque no ambiente industrial há uma significativa presença de ruídos provenientes do processo de produção e também de interferências causadas por estruturas refletivas ou bloqueios no sinal de rádio frequência (RF). Além disso, o ambiente industrial pode apresentar características severas de operação no que se refere a temperatura, umidade, vibrações, dentre outros. Outro fator que pode interferir nas comunicações sem fio é a coexistência, ou seja, duas ou mais redes que compartilham das mesmas frequências para realizar suas comunicações. Parte dos avanços em comunicações sem fio estão relacionados com a caracterização dos canais de RF, já que, uma vez conhecida as características de propagação e interferência de RF é possível projetar ou aprimorar o desenvolvimento de uma RSSF. Segundo (HOWITT *et al.*, 2006), o desenvolvimento de RSSF para aplicações industriais requer a combinação de conhecimentos relacionados com quatro áreas, que são elas:

- Industrial: para providenciar o conhecimento sobre a aplicação;
- Instrumentação: para compreender características de transdutores e demais situações como calibração e deriva;

- Comunicações sem fio: para compreender as características do enlace no meio industrial e escolher a tecnologia mais adequada;

- Redes: para conhecimento das arquiteturas hierárquicas de redes envolvendo diversos dispositivos e integração com diferentes sistemas de comunicação.

Sistemas de automação industriais geralmente são intolerantes à falhas ou atrasos de comunicação em certo grau, e, desta forma é necessário garantir transmissões com altos índices de confiabilidade. Tendo em vista propor soluções confiáveis em comunicação sem fio no ambiente industrial podem-se destacar o surgimento de protocolos como *Wireless*HART (WH), ISA100.11a e WIA-PA. Estes protocolos foram projetados para atender diversos requisitos de operação na indústria, como (GUNGOR; HANCKE, 2009):

- Baixo custo e compacidade: necessário para a implementação em larga escala. Além do custo individual de cada componente também estão inclusos os custos de instalação, manutenção e treinamento para utilização do sistema. Desta forma, características como facilidade de instalação e operação dos equipamentos são importantes para que se tenha redução de custos de operação;

- Interoperabilidade: capacidade de se comunicar com outros sistemas que podem ser utilizados no processo de produção, sejam cabeados ou sem fio;

- Processamento de dados: o processamento local de dados brutos de sensores evita que informações desnecessárias sejam transmitidas pela rede;

- Consumo de energia: o baixo consumo de energia aliado ao consumo eficiente de energia são importantes para a maximização do tempo de vida da rede;

- Auto-organização: este requisito garante que a rede se ajuste em casos de alteração na topologia que podem ser causadas por falhas, mobilidade, novas conexões e desconexões;

- Adaptabilidade: capacidade de lidar com as variações de características dos canais de comunicação que são verificadas com o monitoramento da qualidade do enlace;

- Tolerância à falhas e confiabilidade: mecanismos para garantir a entrega de pacotes ao destino e diferenciação de serviços por critérios de prioridade;

- Segurança: em se tratando de comunicações sem fio em aplicações críticas é necessário impedir o acesso a rede por intrusos, para evitar espionagem e ataques.

1.1 Motivação

Apesar de os protocolos de comunicação apresentarem uma série de especificações para atender aos requisitos de implementação de Redes de Sensores Sem Fio Industrias (RSSFI), existem diversos tópicos nessa área que são explorados pela comunidade científica, onde são propostas melhorias nos procedimentos utilizados e o desenvolvimento de novas técnicas para abranger aplicações não atendidas pelos protocolos. O estudo de RSSFI também contribui para a atualização de especificações de protocolos de comunicação que são feitas regularmente para esclarecimento ou adição de novas funcionalidades.

O protocolo de comunicação utilizado como referência para esse trabalha é o *Wireless*HART (WH). Este protocolo atende aos requisitos industriais para comunicações sem fio seguras, simples e confiáveis. Sua tecnologia de comunicação sem fio foi desenvolvida para operar em baixa potência com baixa taxa de dados, adequadas para monitoramento e controle de processos industriais. Suas aplicações incluem o gerenciamento de plantas industriais e seus equipamentos, geração de alarmes e eventos diversos, aplicáveis primariamente na indústria de processos. O protocolo conta com o suporte de grandes fabricantes no fornecimento de equipamentos compatíveis que caracterizam suas características de flexibilidade, escalabilidade, segurança e interoperabilidade (CHEN; NIXON; MOK, 2010). Aliado a esses fatores, e como facilitador, são utilizado trabalhos prévios e diversas ferramentas adequadas para o desenvolvimento do trabalho, como equipamentos necessários para criar e analisar redes WH reais que incluem: dispositivos de campo, *gateways* e *sniffer* para monitoramento de tráfego da rede e softwares para controle da rede.

O protocolo de comunicação WH, foi desenvolvido essencialmente para aplicações de automação de processos, onde as variáveis do ambiente observado alteram-se de forma lenta. Este é o caso de processos de tancagem, biorreatores e estações de tratamento de efluentes, que trabalham com variáveis como temperatura, pressão ou nível. A presença de alta dinamicidade, que é característica da automação de fábrica, demanda rápidas variações na topologia da rede (física e lógica) que não é uma característica contemplada pelas redes WH, adequada para processos lentos e com nodos fixos. Devido a caracte-

rística de auto-organização do protocolo, algumas condições de operação e manutenção também causam modificações de topologia. A presença de mobilidade é um destes fatores e é classificada em dois grupos: *weak mobility* e *strong mobility* (ALI; SULEMAN; UZMI, 2005). *Weak mobility* é o termo utilizado para representar variações normais que ocorrem durante o funcionamento da rede como conexão e desconexão de nodos ou interrupção no enlace entre dispositivos que podem ser resultado, por exemplo, de falhas no hardware ou bloqueios físicos causados por algum objeto. Já o termo *strong mobility* é utilizado para se referir à movimentação física do nodo, seja por uma movimentação do meio ao qual ele está inserido (ex. água) ou pela movimentação de objetos ou pessoas onde o sensor está fixado. Para este trabalho os termos *weak mobility* e *strong mobility* serão referenciados como baixa mobilidade e alta mobilidade, respectivamente.

O Protocolo WH prevê mudanças na topologia, porém resultantes da presença de baixa mobilidade. Ao enfrentar alguma dessas situações, a rede busca estabelecer novas rotas para o encaminhamento de mensagens que podem levar a mudança da topologia de rede. Por outro lado, se submetermos uma rede WH à variações características de alta mobilidade haverá uma degradação na taxa de sucesso de transmissões (MONTERO *et al.*, 2012). A alta mobilidade está associada a uma frequente mudança de topologia e como resultado tem-se problemas como (DONG; DARGIE, 2012):

- Redução na qualidade de enlaces já estabelecidos, tornando a transmissão de dados mais suscetível a falhas que por sua vez aumenta a taxa de retransmissão de pacotes e o consumo de energia;

- A frequente mudança de topologia acrescenta atrasos na entrega de pacotes devido a necessidade do busca por novas rotas e isso traz como consequência a redução da confiabilidade do sistema.

O estudo da mobilidade em RSSFI permite a compreensão de seus efeitos e a identificação de fatores limitadores ao uso de dispositivos móveis nestas redes. Isso possibilita o desenvolvimento de novos mecanismos de gerenciamento que contribuem para a formação de redes que suportem mobilidade, mantendo-se os requisitos de operação necessários para o ambiente industrial. A utilização de nodos móveis em RSSFI abre espaço para o desenvolvimento de novas aplicações que podem trazer benefícios como aumento de produtividade e também controle sobre saúde e segurança de operadores.

1.2 Objetivos

Sobre o tema de mobilidade em RSSFI, os objetivos deste trabalho são definidos como segue.

1.2.1 Objetivo geral

Oferecer suporte para dispositivos móveis em RSSFI baseadas em TSCH (*Time Synchronized Channel Hopping*), como o protocolo WH, tendo em vista proporcionar um cenário adequado para atender dispositivos que se movimentam dentro do alcance da rede e de dispositivos intermitentes que participam da rede em momentos específicos e por um determinado período de tempo.

1.2.2 Objetivos específicos

- Compreender os procedimentos destas redes e identificar aspectos limitadores à presença de mobilidade;
- Alterar as estratégias padrões de gerenciamento para incluir suporte a alta mobilidade;
- Propor estratégia para redução de tempos de procedimentos;
- Propor melhorias na manutenção da conectividade de dispositivos móveis;
- Sugerir estratégias para aumento da confiabilidade do sistema.

1.3 Contribuições

As principais contribuições deste trabalho são relacionadas ao desenvolvimento de um ambiente adequado adequado que consiga lidar como comportamento de dispositivos móveis em RSSFI. Em resumo algumas contribuições são apresentadas a seguir:

- Desenvolvimento de uma técnica para rápida coleta de dados para que dispositivos possam cumprir suas funções na rede de forma rápida. Isso permite uma comunicação mais adequada entre a rede industrial e dispositivos que possuem restrições de tempo sobre a área de cobertura da rede;

- Desenvolvimento de um mecanismo de *handover* para redes TSCH para que se mantenha a comunicação de dispositivos enquanto eles se movimentam pela rede acelerando a atualização de topologia da rede.;
- Proposta de melhorias como sugestão para processos mais seguros, onde são apresentadas abordagens para propagação de dados de nodos móveis de forma segura pela rede.

O restante do texto está organizado da seguinte forma. Na próxima seção, de fundamentação teórica, são apresentados os principais conceitos utilizados no desenvolvimento deste trabalho. Na seção 3 é apresentada a revisão bibliográfica onde são citados trabalhos que avaliam e propõem técnicas para gerenciamento de mobilidade em RSSFI. A seção 4 refere-se ao desenvolvimento do trabalho onde são apresentados os materiais utilizados juntamente com o detalhamento das técnicas propostas. A seção 5 apresenta os experimentos realizados e os resultados encontrados. Por fim, na seção 6 se encontram as conclusões.

2 FUNDAMENTAÇÃO TEÓRICA

Este trabalho tem como tema a mobilidade de nodos em redes de sensores sem fio industriais (RSSFI) onde são propostas técnicas de agregação e manutenção de dispositivos móveis nestas redes. Neste capítulo são abordados os principais conceitos em torno do tema que incluem tópicos sobre redes industriais e seus procedimentos, a mobilidade e a conectividade de dispositivos móveis.

2.1 Tipos de automação industrial

A escolha de um sistema de automação para uma determinada aplicação está associado a diversos fatores do processo de manufatura. Isso inclui, por exemplo, definir a forma como o produto é manufaturado, métricas de desempenho de produção desejadas, limitações de produção, etc. Na indústria, as aplicações de automação podem ser classificadas como automação de fábrica e automação de processos.

Aplicações típicas de automação de fábrica envolvem a produção/montagem de produtos específicos que empregam uma ou mais máquinas e grande fluxo de materiais e peças. Este tipo de processo apresenta características de controle lógico intensivo e elevadas taxas de transferência de dados.

Já o termo automação de processos é utilizado para descrever sistemas que tipicamente envolvem a transformação de materiais brutos, através de reações químicas, físicas ou térmicas para a produção de um novo produto. A produção pode estar associada a uma ou mais unidades de processo interligadas. Geralmente inclui controles analógicos e os tempos de resposta utilizados são lentos quando comparado com sistemas de automação de fábrica.

2.2 Dispositivos móveis em RSSFI

Atualmente, os principais protocolos de comunicação normatizados para RSSFI como *Wireless*HART, ISA100.11a e WIA-PA (LI *et al.*, 2017) foram projetados essencialmente para atender a redes compostas por nodos estáticos. Apesar de suas diferenças, os protocolos apresentam semelhanças em alguns mecanismos como a utilização de gerenciamento centralizado que contribui no alcance de níveis adequados de confiabilidade necessários em aplicações industriais. Os mecanismos definidos para agregação de dispositivos, descobrimento de vizinhos, agendamento e roteamento de mensagens não são otimizados para atender a redes com dispositivos móveis. Desta forma, há a necessidade do desenvolvimento de técnicas para o gerenciamento de mobilidade na rede. Um dos fatores que influenciam diretamente na manutenção da conectividade de dispositivos móveis é o procedimento de descobrimento de vizinhos que quando adequado reduz a chance de dispositivos perderem conexão e caso aconteça agilizam o processo de reconexão. Em redes *Wireless*HART, por exemplo, esse procedimento é probabilístico e desta forma não garante o tempo para realizar a tarefa de descobrimento, porém este não é um fator crítico já que a rede prevê que os dispositivos ficarão no mesmo local por um grande período de tempo (MONTERO; GOZALVEZ; SEPULCRE, 2017).

O estudo da mobilidade de nodos em redes de comunicação sem fio é essencial para o desenvolvimento de modelos adequados e mecanismos eficientes de estimação de mobilidade. A mobilidade pode ser caracterizada em diversos aspectos e as soluções implementadas podem ser otimizadas para situações específicas. Uma vez que se conhece as características de mobilidade de um sistema é possível, por exemplo, projetar um mecanismo adequado de *handover*.

2.2.1 Tipos de mobilidade

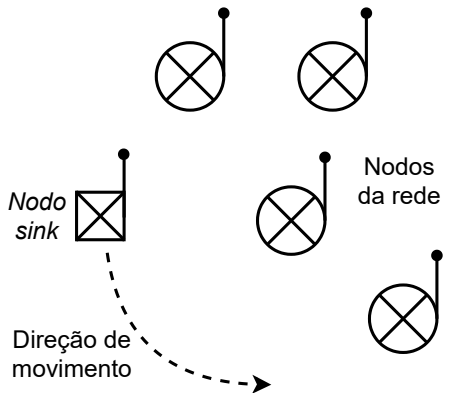
Nas comunicações sem fio, a mobilidade pode aparecer de três formas diferentes (KARL; WILLIG, 2007):

- **Mobilidade de nodo:** Nesse caso são os nodos da rede que se movimentam. É o caso mais comum, porém apresenta grandes desafios de implementação já que resulta em constantes modificações na topologia de rede. Desta forma, a rede deve reconhecer essas mudanças com uma frequência suficiente para manter a conectividade dos dispositivos. Por outro lado é preciso considerar um balanceamento entre

essa frequência de atualização e velocidade do nodo para que se tenha um consumo de energia adequado para manter a funcionalidade da rede. A mobilidade de nodo pode ainda ser dividida em dois grupos: baixa mobilidade e alta mobilidade. Em baixa mobilidade estão os processos que envolvem a entrada e saída de nodos da rede seja por um processo de agregação, desconexão ou falha de comunicação que resulte em modificações usuais na topologia. Já em alta mobilidade se refere a situações onde há a movimentação física do nodo, seja pela movimentação do meio ao qual ele está inserido (ex. água, ar) ou pela movimentação de objetos ou pessoas onde um sensor possa estar fixado.

- **Mobilidade de *sink*:** *Sink* é o nome dado a um equipamento que se movimenta dentro de uma rede coletando informações de nodos fixos conforme exemplo apresentado na Figura 2. Nesse caso a ideia é reduzir o consumo de energia já que se reduz a quantidade de saltos nas comunicações e também evitar gargalos de comunicação em dispositivos próximos a pontos de acesso que podem ser utilizados como rota de comunicação de muitos outros dispositivos. Por outro lado, esse método exige um roteamento eficiente para que não ocorra atrasos ou degradações nos dados das comunicações.

Figura 2 – Nodo *sink* que se movimenta pela rede adquirindo informações de nodos da rede.

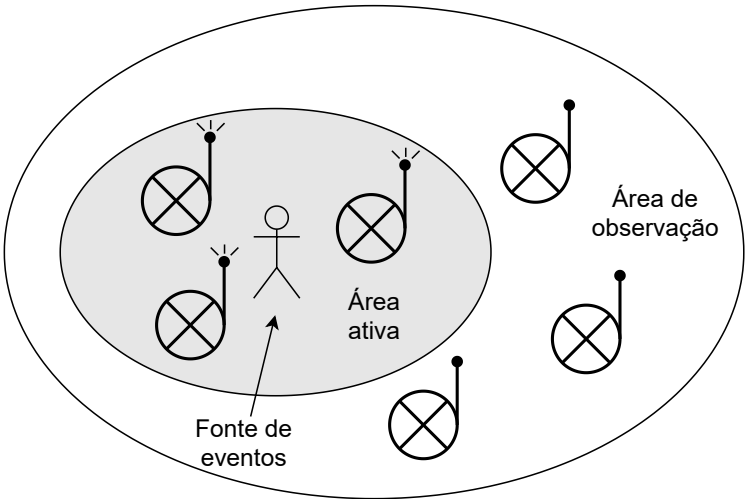


Fonte: do autor

- **Mobilidade de evento:** Em aplicações de detecção de eventos ou de rastreamento, a causa dos eventos ou objeto a ser rastreado pode ser um dispositivo móvel. É importante que a área de observação do evento seja coberta por sensores de forma

suficiente para atender aos requisitos da aplicação. Assim, os sensores permanecem em um estado de baixo consumo de energia até a detecção de um evento onde passam para um estado de atividade ativa para observar o evento e então retornam para o estado anterior. Como apresentado na Figura 3 o sistema apresenta uma área ativa composta pelos sensores, que neste caso, estão rastreando um objeto.

Figura 3 – Rastreamento/detecção de objeto baseado em mobilidade de evento.



Fonte: do autor

2.2.2 Padrões de mobilidade

Os padrões de mobilidade caracterizam a forma como um tipo de mobilidade é realizado. No estudo de RSSFI, três padrões são comumente considerados (DONG; DARGIE, 2012; ZAREEI *et al.*, 2018):

- **Mobilidade de pedestre:** Esse padrão representa as características de movimento de pessoas. Utilizado em aplicações que consideram a utilização de sensores junto a pessoas que caminham em uma determinada área. Esse padrão tem como característica o desvio de obstáculos, limitações em velocidade e pode ou não representar o comportamento de um grupo.

- **Mobilidade veicular:** Descreve o movimento de veículos equipados com sensores. Apresenta velocidades mais elevadas quando comparado com o padrão de pedestre. Pode apresentar característica de determinismo quando utilizada uma rota predefinida ou um plano de movimentos.

- **Mobilidade de meio:** Esse tipo de movimento ocorre por mudanças no meio ao qual o sensor está inserido, por exemplo a água. Apresenta variações em velocidade e também em dimensão.

2.2.3 *Handover*

O sucesso nas comunicações de dispositivos móveis em RSSFI é diretamente dependente da manutenção de enlaces de comunicação. Quando um dispositivo se distancia de seu ponto de conexão (ex. vizinho ou ponto de acesso) ocorre uma degradação no enlace que, dependendo de seu nível, pode resultar em falhas de comunicação devido a fatores como enfraquecimento do nível de sinal e maior suscetibilidade a interferências. O mecanismo, geralmente, empregado para manter a conectividade de dispositivos móveis é o *handover*. O conceito é proveniente das telecomunicações e para uma comparação com o meio industrial utiliza-se pontos de acesso ou dispositivos roteadores no lugar de estações base e dispositivos de campo móveis ao invés de celulares. O procedimento do *handover* busca estabelecer um novo enlace de comunicação para um dispositivo assim que detectado um determinado nível de degradação ou após a perda total do sinal (VAN; AI; LIU, 2017).

O processo de *handover* pode ser descrito em três etapas (BHUVANESWARI, 2011; ZINONOS; VASSILIOU, 2014):

- **Monitoramento:** Durante essa etapa são realizadas medidas para verificar a qualidade dos enlaces de comunicação que variam com a mobilidade dos nodos. A detecção de mobilidade pode ser verificada a partir da avaliação de diversas fontes sendo cada uma com suas vantagens e desvantagens que devem ser levadas em consideração no projeto da aplicação (DONG; DARGIE, 2012). Alguns exemplos são o indicadoor de intensidade de sinal recebido (RSSI - *Received Signal Strength Indicator*), taxa de erro de bit (BER - *Bit Error Rate*), distância, velocidade, potência de transmissão e relação sinal-ruído (SNR - *Signal-to-Noise Ratio*).

- **Decisão:** Após definido o critério de avaliação da qualidade de enlace, é nessa fase que é definida a necessidade ou não do *handover* e também definido o melhor candidato a ser utilizado no processo. O algoritmos empregados nessa etapa podem ser classificados em convencionais e inteligentes (BHUVANESWARI, 2011). Os

métodos convencionais utilizam um valor de limiar que atua como um gatilho sinalizando o sistema da necessidade do *handover*. Junto a essa técnica também é empregado uma margem de histerese para evitar a necessidade de diversos *handovers* causados por pequenas variações no valor de limiar.

Já os métodos inteligentes são assim chamados pois utilizam de inteligência artificial para sinalizar o sistema da necessidade de *handover*. Algumas técnicas empregadas são baseadas em lógica fuzy, redes neurais, reconhecimento de padrões e algoritmos de predição.

- **Execução:** Nessa etapa é feita a transferência do enlace para o nodo escolhido bem como informações de roteamento necessárias para as comunicações.

2.2.3.1 Classificação de handover

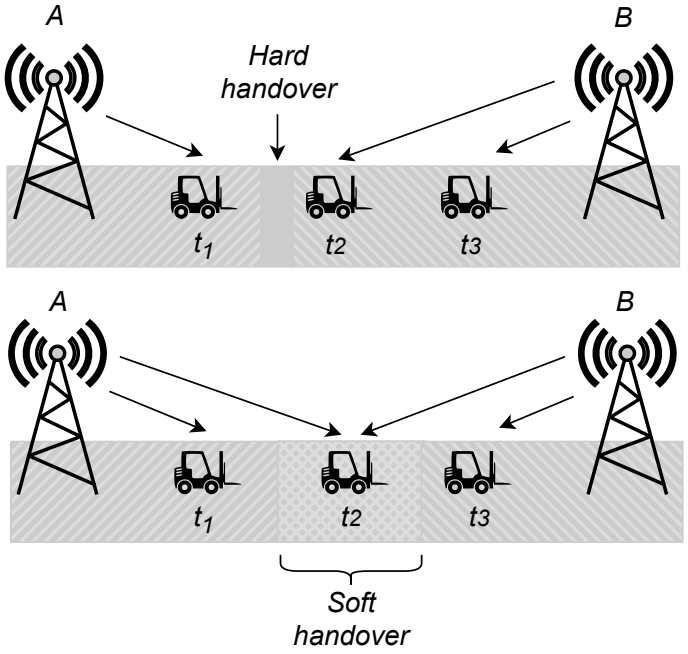
A processo de *handovers* pode ser classificado em diversos critérios que são apresentados a seguir (THAKUR; GANPATI, 2019):

- *Hard* e *soft*

  O termo *hard handover* é utilizado para representar o processo onde uma nova conexão é estabelecida quando detectado que a antiga conexão foi perdida ou removida. Já no *soft handover* uma nova conexão é estabelecida primeiro e então removida a conexão antiga. Ambos os casos são apresentados na Figura 4, que representa um veículo móvel em três momentos distintos (t_1, t_2 e t_3) que se desloca da esquerda para a direita. No instante t_1 em ambos os caso o veículo apresenta conexão com apenas um ponto de conexão. Já no instante t_2, na abordagem de *hard handover* o veículo possui conexão apenas com o ponto B enquanto que no caso de *soft handover* o veículo possui conexão com os pontos A e B, uma vez que a conexão com B foi estabelecida antes da perda da conexão com A. Como pode ser observado no exemplo, o *hard handover* possui sempre conexão com apenas um ponto e no momento em que o dispositivo está entre dois pontos de conexão pode haver o efeito chamado de ping-pong onde podem ocorrer diversas trocas nas conexões gerando maior carga de comunicações na rede. No *hard handover* também há uma faixa onde nenhuma comunicação é realizada devido a execução do processo de *handover* que poder levar a perda de informações já que o dispositivo momentaneamente não pode realizar transmissões. Desta forma o *soft handover* apresenta

vantagens já que elimina o efeito ping-pong e não apresenta pontos de interrupção de comunicação.

Figura 4 – Representação de *handovers* do tipo *hard* e *soft*.



Fonte: do autor

- Horizontal e vertical

  Em *handovers* horizontais o novo ponto de conexão pertence ao mesmo tipo de rede, por exemplo WiFi para WiFi ou WH para WH. Por outro lado, *handovers* verticais uma nova conexão é estabelecida com um nodo de um tipo de rede diferente. A utilização de *handover* vertical deve garantir requisitos de qualidade de serviço (QoS - *Quality of Service*) de todas as redes envolvidas.

- *Downward* e *upward*

  Em *downward handovers* a conexão é mudada de uma rede com maior área de cobertura para uma rede de menor área de cobertura. Já o *upward handover* é o contrário, de uma rede menor para uma maior, por exemplo de uma rede WiFi para uma rede 3G.

2.2.3.2 Requisitos do handover e métricas de desempenho

A implementação de processos de *handover* pode afetar a rede em diversos aspectos, incluindo indicadores de QoS de redes industriais como confiabilidade e disponibilidade.

Desta forma alguns requisitos são desejáveis no projeto desses sistemas para reduzir seus efeitos negativos na rede.

- Mínima latência de *handover*: essa latência é o tempo decorrido desde a requisição até o fim do processo de *handover*. O processo deve ser rápido o suficiente para que sejam minimizadas as degradações ou interrupções no serviço. Quanto maior esse tempo, maior será o atraso nas comunicações da rede contrariando os requisitos de RSSFI.

- Mínimo número de *handovers*: esse requisito influencia na taxa de sucesso do processo que leva em consideração o número de tentativas e o número de *handovers* realizados com sucesso. Em alguns casos o resultado do *handover* pode apresentar um desempenho pior que o anterior o que pode gerar uma nova requisição que é característica do efeito ping-pong. Desta forma é preciso minimizar o número de *handovers* desnecessários.

- Mínima influência na QoS do sistema: o processo de *handover* pode causar sobrecarga na rede, principalmente se não executado de forma precisa tomando decisões corretas. É possível avaliar esse requisito com a verificação da utilização de canais, que apresenta a razão entre os canais sendo utilizados com o número total de canais de comunicação do sistema.

2.3 *Wireless*HART

Optou-se por utilizar como base para o desenvolvimento deste trabalho o padrão *Wireless*HART (WH) por se tratar de um protocolo bem conceituado para aplicações industriais, uma vez que conta com uma série de características que o tornam robusto, seguro e de simples implementação. Porém, as modificações propostas para o desenvolvimento deste trabalho o tornam incompatível com o original, e desta forma as redes formadas para realização de experimentos não são WH pois já não atendem aos critérios estabelecidos nos procedimentos descritos pela norma.

O WH é um protocolo de comunicações sem fio para aplicações em automação de processos. Foi oficialmente apresentado pela HART Communication Foundation

em 2007 como uma atualização à tecnologia HART onde foram adicionadas comunicações sem fio mantendo compatibilidade com os dispositivos HART já existentes assim como comandos e ferramentas. A especificação do WH foi aprovada pela Comissão Eletrotécnica Internacional (IEC - *International Electrotechnical Commission*) como um padrão internacional em 2010.

Trata-se de uma tecnologia de simples implementação devido suas características de auto-organização e auto configuração que ajustam a rede com base em modificações na planta como adição/remoção de dispositivos ou um bloqueio de algum enlace de comunicação. A não utilização de cabos também simplifica a instalação e reduz o custo com materiais de infraestrutura quando comparado com uma rede cabeada. Isso permite o acesso a áreas remotas além do fato de facilitar a implementação de dispositivos em estruturas móveis, como exemplo uma parte móvel de um equipamento.

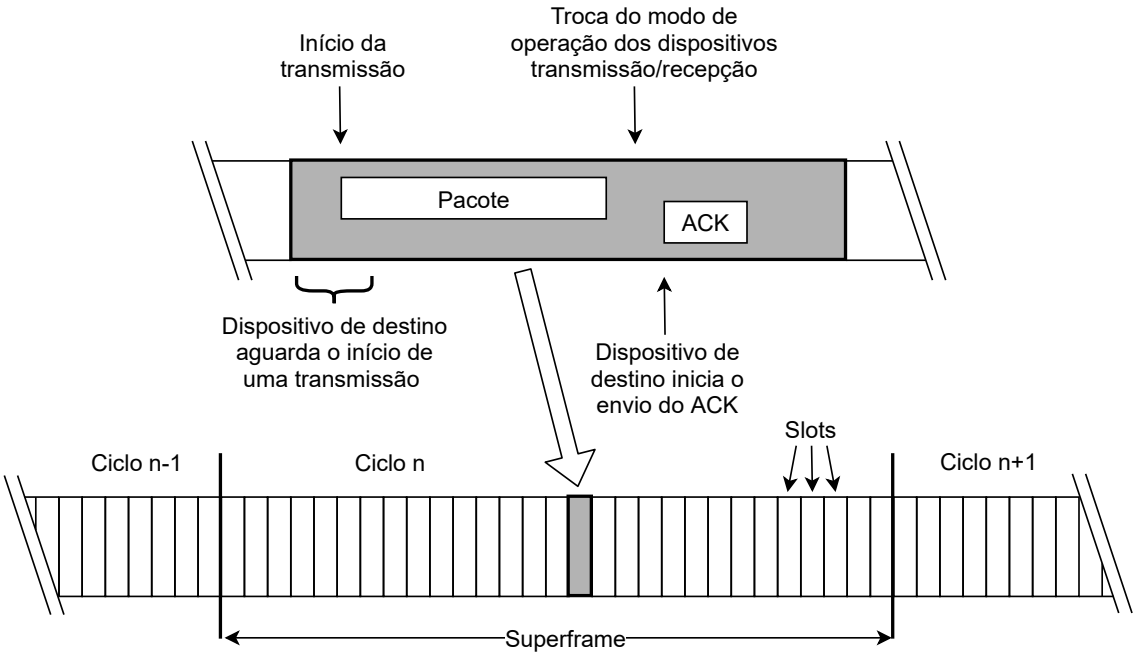
Para garantir robustez de operação perante as condições de operação encontradas no ambiente industrial, o protocolo WH apresenta recursos como técnicas de espalhamento espectral tanto de salto de frequência (FHSS - *Frequency Hopping Spread Spectrum*) como de sequência direta (DSSS - *Direct Sequence Spread Spectrum*). O protocolo IEEE802.15.4, que é utilizado como base para a camada física do WH, divide a banda de frequência de 2.4 GHz em 16 canais não sobrepostos. A banda de frequência de 2.4 GHz é uma das bandas reservadas internacionalmente para o desenvolvimento industrial, científico e médico (ISM - *Industrial Scientific and Medical*) e é livre de licenciamento. A topologia de rede em malha fornece rotas redundantes e pode comportar múltiplos pontos de acesso. A qualidade das rotas é monitorada e quando necessário as rotas são atualizadas. Uma rede WH também pode coexistir com outras redes que operam no mesmo espectro de frequências e para isso o protocolo conta com recursos como verificação de ocupação do canal (CCA - *Clear Channel Assessment*), retransmissão de mensagens e lista de canais proibidos que impede a utilização de canais com constante ocupação registrada.

Se tratando de comunicações sem fio, a rede fica mais suscetível a ataques de espionagem ou sabotagem de processos devido ao alcance das comunicações. O protocolo WH emprega medidas de segurança a todo tempo incluindo algoritmos de encriptação de mensagens, chaves de segurança em diversos níveis e autenticação

de novos dispositivos. Outra proteção é o próprio mecanismo de salto de canais que define o canal somente no momento da transmissão.

O protocolo WH é baseado em Acesso Múltiplo por Divisão de Tempo (TDMA - *Time Division Multiple Access*) que é uma técnica de controle de acesso ao meio que proporciona comunicações determinísticas e sem colisões. As comunicações entre dispositivos são realizadas dentro de slots de tempo fixo de 10 ms. Um conjunto de slots forma um superframe, que ao se repetir continuamente forma o ciclo da rede. Tipicamente, dois dispositivos são associados a um slot, um como origem e outro como destino. A transação feita em um time slot inclui o envio de um *Data-Link Protocol Data Unit* (DLPDU) da origem seguida de uma confirmação (ACK - *Acknowledgement*) enviada pelo destino. Mensagens do tipo *broadcast*, que tem como destino todos os dispositivos, não exigem a resposta do ACK. A representação de um superframe juntamente com seus ciclos e o detalhe de uma comunicação típica em um slot são apresentadas na Figura 5.

Figura 5 – Superframe e slot TDMA.



Fonte: adaptado de (HCF, 2008)

O TDMA permite o agendamento preciso das comunicações que é realizado com base em informações gerais de roteamento da rede bem como demandas de dispositivos de campo ou aplicações. É através do agendamento de comunicações que

dispositivos sabem quando e qual é o serviço que deve ser realizado, que pode ser aguardar a chegada de um pacote da rede ou propagar um pacote na rede.

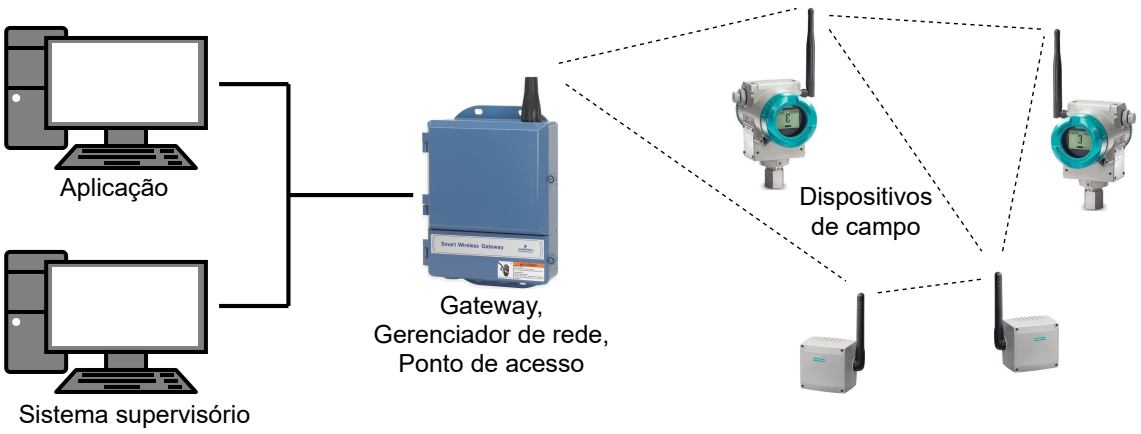
2.3.1 Componentes de uma rede WH

Os elementos básicos de uma rede WH incluem:

- Dispositivos de campo: elementos conectados na planta de automação com funções de sensoreamento e atuação de campo. Os equipamentos podem apresentar a tecnologia WH já integrada ou também através de adaptadores WH para equipamentos cabeados compatíveis. Todos esses dispositivos devem ser capazes de rotear pacotes na rede.
- Gateway: permite a comunicação entre dispositivos de campo com aplicações ou outras redes de comunicação existentes na planta.
- Gerenciador de rede: responsável pela configuração da rede, agendamento de comunicações entre dispositivos, gerenciamento de tabelas de roteamento e monitoramento da rede. Este gerenciador pode ser integrado ao Gateway, a um *host* de aplicação ou a um controlador de processos de automação.

Na Figura 6 é apresentada a arquitetura típica de uma rede WH e como seus elementos principais são distribuídos. Neste caso, um único equipamento, chamado de gateway, contém o gerenciador de rede, o gateway e o ponto de acesso.

Figura 6 – Arquitetura típica de uma rede WH.



Fonte: do autor

2.3.2 Processo de agregação (*Join*)

O processo de agregação é utilizado por novos dispositivos para obter acesso a rede. Em linhas gerais, pode-se resumir esse processo pelos seguintes passos:

- Anúncio periódico da rede feito por dispositivos que já fazem parte da rede. O pacote de anúncio de rede contém as informações que o novo dispositivo precisa para iniciar sua comunicação com a rede;
- Monitoramento, por parte do novo dispositivo, para localizar e sincronizar-se com a rede;
- Estabelecer um canal seguro de comunicação com o gerenciador de rede;
- Verificar a autenticidade do novo dispositivo;
- Provisionar o novo dispositivo para sua integração total com a rede.

A seguir o processo de agregação de novos dispositivos é apresentado com mais detalhes juntamente com um diagrama de sequência representando o processo na Figura 7.

1. **Provisionamento inicial do dispositivo:** Antes de tentar contato com a rede o dispositivo deve ser provisionado com uma chave de acesso e um identificador de rede. A chave de acesso atua como uma senha para garantir acesso a rede e o identificador de rede é utilizado para localizar a rede correta, já que é possível que mais de uma rede WH esteja em operação na mesma área. Em dispositivos comerciais esses parâmetros são configurados utilizando uma ferramenta de manutenção padrão HART através da porta de manutenção do equipamento. Uma vez concluído o provisionamento inicial, o dispositivo deve ser configurado para o modo de agregação, seja de forma automática ou em um desejado momento através da porta de manutenção. É nesse modo que o novo dispositivo passa a escutar comunicações da rede e coletar informações de dispositivos já conectados.
2. **Divulgação da rede:** O ponto de acesso juntamente com dispositivos já conectados à rede são responsáveis pela transmissão periódica de pacotes de anúncio de rede. Esses pacotes contém toda a informação que novos dispositivos precisam para tentar se conectar com a rede. Os pacotes são enviados

no primeiro link disponível, que não seja compartilhado, após a contagem do temporizador associado a essa tarefa. As informações contidas nesses pacotes são:

- Número de slot absoluto (ASN - *Absolut Slot Number*): Uma estampa temporal que representa o número de slots decorridos desde a criação da rede.
- *Join control*: indica a capacidade de aceitação do dispositivo que está anunciando de receber novos dispositivos. Quanto menor esse valor, melhor.
- Mapa de canais: Indica os canais disponíveis para comunicação. O mapa de canais juntamente com o ASN e o *offset* de canal são utilizados para determinar o canal no momento de cada comunicação.
- Links de agregação: Lista todos os links reservados para a agregação do dispositivo que está anunciando a rede. Os novos dispositivos são limitados a se comunicar por esses links até que sejam provisionados pelo gerenciador de rede com seus links normais.

3. **Sincronização:** Se tratando de uma rede determinística baseada em TDMA é necessário que o novo dispositivo sincronize-se com o tempo da rede antes de iniciar suas transmissões. O dispositivo escuta o primeiro canal por um determinado período de tempo e troca para o próximo canal. No momento em que é encontrado uma transmissão com o mesmo identificador de rede é realizado uma tentativa de sincronização. Além da sincronização são realizadas novos testes com outros pacotes da rede para confirmá-la. Caso rejeitada, o escaneamento é retomado. O escaneamento é realizado dessa forma durante o período de busca ativa e se a rede não for identificada a busca passa para o estado passivo onde o mesmo procedimento é realizado, porém com menor frequência e menor consumo de energia.
4. **Requisição de agregação:** Uma vez sincronizado com a rede o novo dispositivo envia uma requisição de agregação como resposta a um pacote de anúncio. O novo dispositivo escolhe um dispositivo pelo qual a requisição será enviada com base em métricas como nível de sinal e *join control* que são dados que foram coletados de vizinhos na etapa de busca anterior. O dispositivo esco-

lhido para encaminhar comunicações entre o novo dispositivo e o gerenciador de rede durante o processo de agregação é chamado de *proxy*. Rotas que utilizam *proxy* são utilizadas por dispositivos que ainda não foram integrados à rede pelo gerenciador. Isso inclui dispositivos que estão em processo de agregação ou em quarentena. Mensagens que são encaminhadas via rota *proxy* apresentam bytes de controle juntamente com referências de endereço para que a mensagem chegue ao destino final.

Os comandos enviados na requisição de agregação são:

- Comando 0 (*Read Unique Identifier*): Apresenta informações de identificação do dispositivo.
- Comando 20 (*Read Long Tag*): Informa o nome do dispositivo.
- Comando 787 (*Report Neighbor Signal Levels*): Informa os vizinhos descobertos que ainda não possuem um enlace.

Após o envio da requisição o temporizador do serviço de retransmissão é iniciado. Se o tempo for atingido e não for recebido uma confirmação do envio uma nova requisição é enviada pelo próximo pacote de anúncio disponível e o contador de retransmissões é decrementado. O processo é encerrado junto com uma mensagem de erro se o número máximo de retransmissões for atingido. A requisição é enviada em links definidos para o serviço de agregação, porém esses links são do tipo compartilhados e podem ser disputados se mais de um dispositivo estiver requisitando acesso a rede ao mesmo tempo, o que resulta em colisão. Para evitar novas colisões o serviço de retransmissão também conta com um sistema de atrasos, definido de forma aleatória, para enviar uma nova tentativa de requisição. Outro fator que pode resultar na necessidade de uma retransmissão é a falha de comunicação devido a perda de conectividade com o *proxy*.

Um novo dispositivo na rede é agregado através dos links propagados pelo anúncio enviado por outro dispositivo já na rede, e esses links são utilizados apenas para agregação. Transcorridos os estados da máquina de estados de agregação, o dispositivo passa a comunicar-se com os demais através de novos links. Nos dispositivos pelo qual o novo entrou na rede, restam os links de anúncio utilizados anteriormente, os quais ficam novamente ociosos, até que

outro dispositivo é agregado através dele. A Tabela 1 apresenta um típico escalonamento de links de agregação, atribuídos a dois dispositivos considerando superframes de 1024 slots. O dispositivo D2 foi agregado à rede através de outro que já estava agregado (D1), utilizando uma rota *proxy*. Neste exemplo, a cada dispositivo foram alocados dois links de tipo *join* sendo um de transmissão e outro de recepção. Estas informações sobre os links de agregação são propagadas pela rede nos pacotes de anúncio e assim o novo dispositivo sabe exatamente o momento para enviar sua requisição.

Tabela 1 – Escalonamento de links de agregação.

Dispositivo	Opção	Slot	*Offset* de canal	Superframe
D1	Transmissão	149	0	1
	Recepção	726	0	0
D2	Transmissão	166	2	1
	Recepção	513	0	0

5. **Resposta de requisição** A requisição é encaminhada pela rede até que chega ao *gateway*, que identifica que a mensagem é de um dispositivo desconhecido solicita a criação de uma sessão de agregação. Através dessa sessão o gerenciador de rede estabelece um canal de comunicação seguro com o novo dispositivo e permite que a requisição seja avaliada no processo de autenticação. Uma vez autenticado, a primeira resposta é construída e enviada para o dispositivo através de um dispositivo *proxy*, definido dessa vez pelo gerenciador. Esta resposta é referenciada na Figura 7 como "resposta_1". Os seguintes comando são enviados em formato de requisição:

   – Comando 961 (*Write Network Key*): Configura a chave de rede no dispositivo.

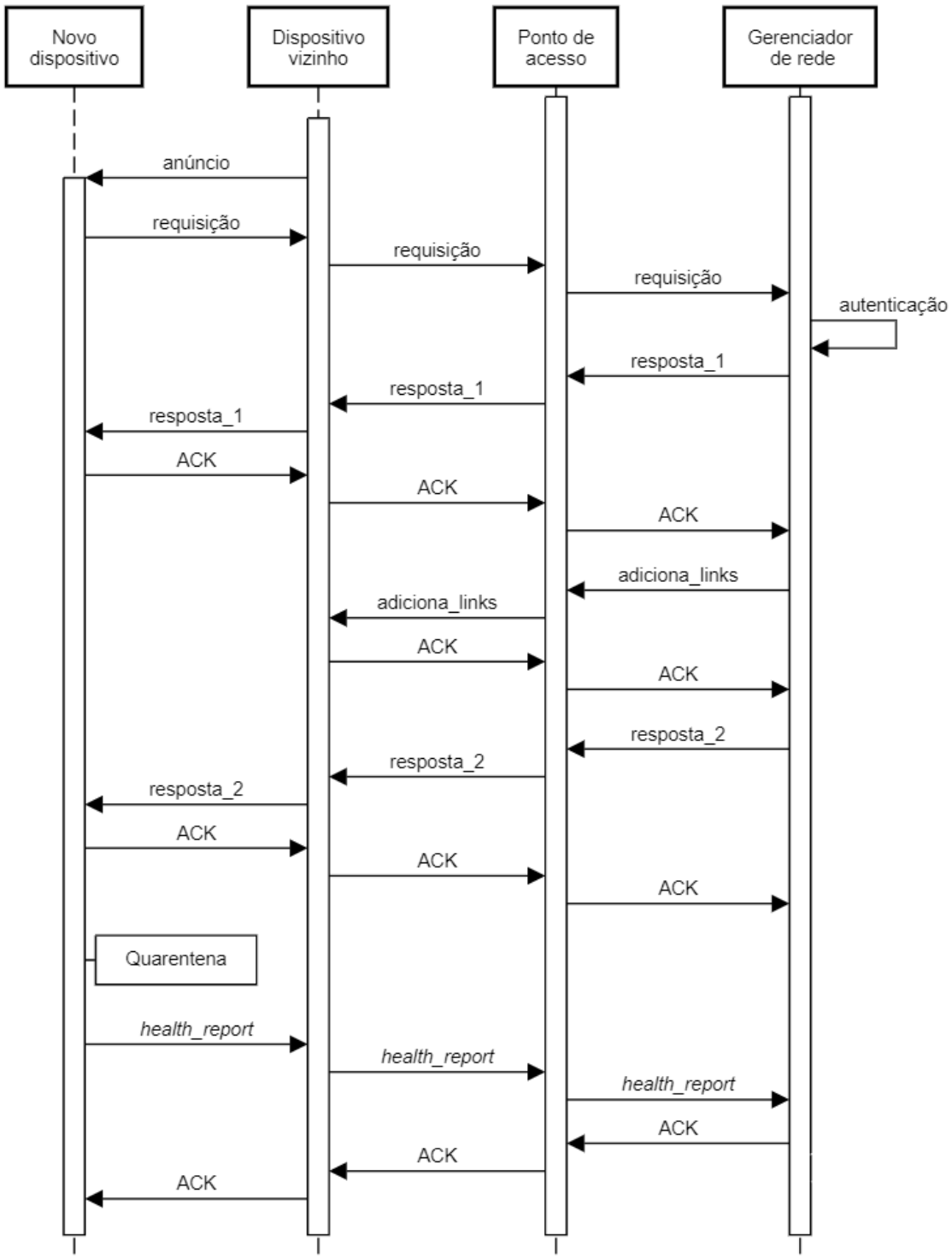
   – Comando 962 (*Write Device Nickname Adress*): Define um apelido para o dispositivo. Esse é um nome de menor tamanho utilizado como identificação do dispositivo.

   – Comando 963 (*Write Session*): Estabelece uma sessão com o dispositivo

para poder gerenciá-lo.

6. **Integração total com a rede:** Após a confirmação do recebimento dos comandos da etapa anterior, o gerenciador envia novos comandos de configurações que incluem: transferir as comunicações dos links de agregação para links normais; definir fontes de tempo para o dispositivo; e atualização da tabela de vizinhos. Estes comandos são apresentados de forma reduzida por apenas um comando referenciado como "resposta_2" na Figura 7. A partir desse ponto o dispositivo já é considerado conectado e passa para o estado de quarentena. Nesse estado o dispositivo possui comunicação apenas com o gerenciador de rede mas já opera normalmente e inicia o serviço de *health report*, onde o dispositivo informa periodicamente ao gerenciador informações estatísticas (nível de sinal entre outras) de seus vizinhos. Essa informação é utilizada para ajustar a rede conforme necessário. O dispositivo deixa o estado de quarentena quando uma sessão com o *gateway* é criada. A decisão de quando criar a sessão é definida pelo gerenciador de rede. Desta forma, aplicações externas podem acessar a dados dos dispositivos de campo. Além de uma sessão com o *gateway* os dispositivos de campo necessitam requisitar banda necessária para prover o serviço de publicação.

Figura 7 – Diagrama de sequência do processo de agregação



Fonte: adaptado de (HCF, 2009)

3 REVISÃO BIBLIOGRÁFICA

Os protocolos para comunicações sem fio industriais são desenvolvidos para superar os desafios na propagação de rádio frequências no ambiente industrial e garantir níveis adequados de qualidade de serviço. Como estes protocolos foram desenvolvidos para atender aplicações de automação de processos, e portanto, para redes com dispositivos estáticos, as técnicas de gerenciamento não são otimizadas para atender dispositivos móveis. Desta forma, a inserção de mobilidade nestas redes exige a criação de novas técnicas de gerenciamento que incluem, por exemplo, alterações ou criação de novos procedimentos como agregação/desconexão/reconexão de dispositivos, agendamento de comunicações e descobrimento de vizinhos. Neste contexto são encontrados trabalhos na literatura científica que propõem técnicas de gerenciamento de mobilidade para RSSFI. A seguir são apresentados trabalhos relacionados ao tema desta dissertação que trazem como foco o desenvolvimento de técnicas para controle de topologia na presença de dispositivos móveis bem como técnicas para redução de tempo de processos considerados lentos.

Em (MONTERO *et al.*, 2012) é apresentado um estudo sobre o impacto da presença de mobilidade no desempenho de redes de sensores sem fio industriais (RSSFI) em protocolos com característica de gerenciamento centralizado, que é o caso do *Wireless*HART utilizado no estudo. O experimento realizado utiliza de nodos fixos que formam uma rede e um dispositivo móvel que deseja se conectar à essa rede. Esse dispositivo realiza uma trajetória retilínea com velocidade constante. Diferentes topologias de rede foram avaliadas tendo em vista verificar o impacto do aumento do número de nodos fixos bem como a relação do desempenho com o número de saltos entre o dispositivo móvel e o gerenciador de rede. O modelo apresentado considera situações onde o dispositivo perde a comunicação e realiza uma nova tentativa de conexão e também o caso onde a rede consegue estabelecer um novo enlace de comunicação antes de interromper o atual, ou seja, realiza

o processo de *handover*. A métrica empregada é a utilização do canal que pode ser usada por um nodo para transmitir dados, e é definida como a razão entre o máximo número de slots que o gerenciador pode alocar para um nodo transmitir mensagens de dados e o número total de slots do superframe. Inicialmente os resultados mostram que a utilização do canal aumenta quando se aumenta a duração do dispositivo móvel sobre a cobertura da rede, onde observa-se um desempenho melhor para os caso de *handover* comparados aos casos de reconexão. Utilizou-se como comparação um dispositivo fixo representando a máxima utilização do canal e, neste caso, uma topologia simples com apenas um salto entre o dispositivo fixo e o gerenciador de rede. Analisando o desempenho para 90 s de tempo do dispositivo móvel sobre a cobertura da rede, tem-se aproximadamente 40 % da utilização máxima do canal de comunicação para o caso de reconexão e 60 % para o caso de *handover*. Estes valores tendem ao máximo desempenho quando elevado o tempo sobre a cobertura de rede para mais de 15 min. O experimento também verifica a influência do tamanho do superframe no desempenho da rede. Os resultados mostram que sobre baixa mobilidade na rede maior é o desempenho quando utilizado um grande superframe, visto que menos slots são utilizados para gerenciamento e portanto sobram mais slots a serem alocados para transmissão de dados. Por outro lado, quando a rede está sobre alta mobilidade o desempenho é maior para superframes menores. Isso ocorre devido ao fato de que um maior número de reconexões é realizado e consequentemente um maior número de slots de gerenciamento é necessário para atender a essa demanda. Os resultados mostram ainda que o desempenho da rede está diretamente relacionado com a velocidade do dispositivo móvel e com o alcance das comunicações. A maximização de desempenho considerando estes fatores ocorre para superframes com tamanho muito abaixo dos 6400 slots definidos pela norma. Outra dependência do desempenho é o número de saltos entre o dispositivo que quer se conectar a rede e o gerenciador de rede. Quanto maior o número de saltos, menor é o desempenho. Isso foi verificado fixando-se os valores de velocidade do dispositivo e alcance de rede e variando-se as topologias para incrementar o número de dispositivos fixos no caminho até o gerenciador de rede. Os resultados apresentados nesse trabalho, mostram que os mecanismos presentes no protocolo WH não são adequados para gerenciar de forma eficiente a mobilidade de nodos na rede.

No trabalho de revisão bibliográfica sobre RSSFI apresentado em (ZAND *et al.*, 2012), os autores descrevem sobre as tecnologias comumente utilizadas para o geren-

ciamento RSSFI, bem como suas vantagens e desvantagens de operação em aplicações industrias que podem demandar de requisitos como confiabilidade e atender sistemas de tempo real. Um dos tópicos apresentados pelos autores como problema de pesquisa é relacionado ao gerenciamento centralizado. Esta é uma técnica utilizada pelos principais protocolos de comunicação para RSSFI onde há um elemento central responsável por tarefas como agendamento de comunicações e gerenciamento de rotas. Apesar desta técnica apresentar uma maior facilidade de implementação, ela pode apresentar baixo desempenho no que se trata a tempo de reação, uma vez que todas atualizações na rede precisam passar pelo elemento central. Em situações em que a rede apresenta alta densidade de nodos as latências de comunicação aumentam devido ao grande número de saltos no encaminhamento de mensagens e acabam inviabilizando sua utilização em situações de dinamicidade elevada que necessitam de decisões rápidas. Como resultado, podem-se encontrar maiores taxas de perda de pacotes que consequentemente geram respostas tardias e maior consumo de energia para retransmissões.

Em (MÜLLER *et al.*, 2013) é proposta uma técnica de descentralização de gerenciamento para a rápida coleta de dados de dispositivos intermitentes. O trabalho apresenta o desenvolvimento de um dispositivo de campo especial, chamado de FDAP (*Field Device - Access Point*), com um coprocessador incorporado. Este dispositivo apresenta características de gerenciamento locais para lidar com dispositivos que tenham comportamento de acesso intermitente à rede. Quando um dispositivo deseja acessar a rede, uma sessão é criada com o FDAP que gerencia localmente o processo de agregação. A proposta inclui a criação de comandos especiais e também modificações na pilha de protocolos dos dispositivos que acessam a rede pelo FDAP, isso mantendo características de confiabilidade e segurança do protocolo utilizado como base, o WH. A comunicação com o dispositivo é realizada através do reuso de slots de anúncio o que evita colisões. Uma vez que o gerenciamento da agregação de dispositivos é realizada localmente elimina-se o atrasa encontrado no processo padrão devido ao encaminhamentos de mensagem pela rede. Desta forma, reduz-se o tempo necessário para realizar a tarefa de agregação e o dispositivo pode executar sua função na rede de forma mais rápida.

Uma forma bem conhecida de manter dispositivos móveis conectados à uma rede sem fio é a técnica de *handover*. Essa técnica busca estabelecer uma nova conexão para um dispositivo assim que detectado uma degradação na qualidade de um link de comunicação

ou após a perda desse enlace. O processo é composto por três etapas: monitoramento, que verifica a qualidade dos links de comunicação; decisão, que verifica se há a necessidade de realizar o *handover*; e execução, que quando necessário identifica um novo caminho e estabelece uma conexão por ele. O algoritmo mais comum para realizar o *handover* é baseado em um limiar (*threshold*) e exige estudos prévios para a determinação de um valor ideal para a métrica utilizada. Além disso, pode também ser implementado um sistema de histerese para evitar o efeito de flutuação na medida. Em (ZINONOS; VASSILIOU, 2014) essa técnica é apresentada utilizando o indicador de intensidade do sinal recebido (RSSI - Received Signal Strength Indicator) como métrica juntamente com uma proposta que utiliza a perda do link (*link loss*) como métrica. O método proposto utiliza o envio de pacotes para calcular a perda medindo-se as confirmações (*acknowledgments*). O experimento realizado utiliza um simulador com treze dispositivos fixos e um dispositivo móvel que segue um trajetória aleatória e envia um pacote de dados a cada três segundos. Foram realizadas cem repetições, com período de duração de duzentos segundos para cada técnica onde foram variados os parâmetros de *link loss* e da margem da histerese. Para avaliação de desempenho foram utilizadas métricas como perda de pacotes fim-a-fim, número de decisões de *handover*, taxa de sucesso de *handover* e consumo de potência. Os resultados apontam diversas relações entre as variáveis avaliadas. Como exemplo podem-se citar: a determinação de um limiar com menor perda de pacotes com o custo de aumento no número de decisões de *handover* e um consequentemente aumento no consumo de energia; a redução na margem de histerese, para o método proposto, resulta em um maior número de decisões de *handover* o que aumenta o *overhead* da rede já que se trata de uma técnica baseada em eventos. Os autores também avaliaram as duas situações em conjunto e que por sinal apresentaram os melhores resultados no que se refere ao desempenho geral e após a decisão de *handover*, visto que nem toda decisão gera com sucesso um *handover* e em alguns casos essa nova comunicação pode ainda ser pior que a anterior.

Já em (MA *et al.*, 2017) é apresenta uma técnica para aprimorar decisões de *handover*. Ao invés de utilizar métricas individuais, o sistema utiliza teoria de lógica fuzzy para integrar três métricas e obter um resultado mais preciso. As métricas avaliadas são: o estado de movimento do dispositivo, que é avaliado com base na variação do valor de RSSI de mensagens recebidas; a condição do canal, que é avaliada pela relação sinal-ruído (SNR);

e a taxa de entrega de pacotes, que pode ser definido avaliando-se o número total de mensagens transmitidas e o número de transmissões com sucesso, ou seja, que confirmaram o recebimento com um ACK. O mecanismo também inclui a utilização de conexões temporárias e registro rápido de dispositivos. Os experimentos realizados incluem testes simulados e também em ambiente industrial real cujo sistema monitorava parâmetros de máquinas de solda. Os resultados apresentam comparações com soluções que utilizam o protocolo WH e *handover* com RSSI como métrica de avaliação. O sistema também garante taxas de entrega de pacotes em média de 98.5 % em ambiente industrial.

Em (MONTERO; GOZALVEZ; SEPULCRE, 2017) é proposta uma técnica que modifica o protocolo de descobrimento de vizinhos do protocolo WH, sobre o qual o trabalho foi desenvolvido, tendo em vista prover suporte para que dispositivos móveis permaneçam conectados à rede enquanto eles se movem. O processo de descobrimento de vizinhos é executado por dispositivos já conectados à rede para atualizar suas tabelas de vizinhos e periodicamente enviar essas informações ao gerenciador de rede que atualiza as tabelas de roteamento. No protocolo WH esse procedimento é realizado através do envio e recepção de mensagens de *keep alive*. Esse procedimento é probabilístico e utiliza links compartilhados específicos para essa aplicação. Um dispositivo envia o *keep alive* após um período aleatório enquanto todos os outros permanecem em modo de recepção, caso um dispositivo receba um *keep alive* de um dispositivo ainda não identificado, ele armazena em sua tabela de vizinhos e notifica o gerenciador de rede. Os autores propõem a atualização de uma técnica (LAN - *Listen Advertise Network*) que utiliza o mecanismo de anúncio da rede (*advertisements*) para realização do processo de descobrimento de rede. Desta forma, tem-se um sistema determinístico já que cada dispositivo possui links dedicados no superframe de gerenciamento para a tarefa de anúncio, enquanto que os links para *keep alive* são compartilhados, utilizados de forma aleatória pelos dispositivos e em menor número no superframe de gerenciamento. O sistema requer que enquanto um dispositivo envia seu anúncio todos os outros estejam em modo de recepção, independente de sua posição na rede que pode nem mesmo escutar quem está transmitindo. Dentro desse contexto os autores propõem a técnica LCA (*Listen for Close Advertises*) onde cada dispositiva tenta escutar apenas anúncios de um a dois saltos de distância. Desta forma tem-se uma melhor utilização de recursos da rede e uma consequente redução no consumo de energia uma vez que é reduzido o tempo em que o dispositivo precisa estar em modo de recepção. Os

autores ainda apresentam outra técnica, chamada LANm (Listen Advertise Network for mobile devices), que explora as diferentes necessidades de dispositivos móveis e estáticos. O sistema padrão de descobrimento de rede do WH é empregado para os dispositivos caracterizados como estáticos e a técnica LAN para dispositivos móveis. Dentre as métricas utilizadas para avaliação de resultados, podem-se citar a probabilidade de descobrimento, a probabilidade de um dispositivo móvel se manter conectado enquanto ele se move, número de bytes consumidos por superframe pelo processo de descobrimento e consumo de energia. Os cenários avaliados apresentam diferentes topologias onde o dispositivo móvel segue trajetórias retilíneas e aleatórias. Os resultados mostram que as técnicas propostas são capazes de detectar vizinhos até 25 vezes mais rápido quando comparado com o procedimento padrão do WH. O custo disso é o aumento no consumo médio de energia da rede causado pela inclusão dos dispositivos móveis.

Em (WEI *et al.*, 2018) é apresentado uma técnica para acelerar o processo de descobrimento de vizinhos que determina com antecedência quais os potenciais novos vizinhos. Neste caso é utilizado um algoritmo que agenda uma tarefa que recomenda vizinhos através do compartilhamento de informações sobre vizinhos. Há também um segunda etapa que, dentre os vizinhos recomendados, identifica quais podem realmente contribuir para reduzir o tempo de descobrimento. Um dos fatores que podem influenciar nesse aspecto é, por exemplo, a distância entre os dispositivos. A validação do trabalho é feita através de simulação, onde os nodos são distribuídos aleatoriamente em um plano bidimensional com número de nodos e velocidade variadas. Os resultados apresentam comparações com outras técnicas e em geral apresenta melhores resultados. Pode-se citar também algumas limitações como uma redução no desempenho quando a densidade de nodos na rede é baixa e a relação entre a densidade de nodos com o tamanho do slot necessário para lidar com a informação dos vizinhos, uma vez que um maior número de colisões está associado a um maior tamanho de slot.

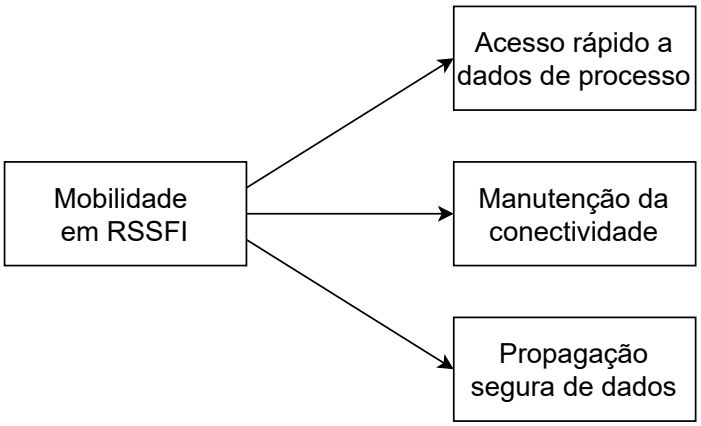
A presença de alta dinamicidade em RSSFI devido à mobilidade dos nodos acabam se tornando objeto de estudo visto que os protocolos padrões para estas comunicações não preveem a utilização de nodos móveis, que dentro do ambiente industrial podem ser representados por veículos autônomos, dispositivos vestíveis, máquinas e equipamentos móveis, entre outros. Os trabalhos apresentados anteriormente visam mostrar os efeitos práticos deste problema de pesquisa e propor soluções com base em métricas de desem-

penho desejadas em cada caso. Este trabalho apresenta técnicas que buscam atender dispositivos considerados especiais devido a sua característica de inserir dinamicidade na rede. Isso inclui dispositivos intermitentes, ou seja, que desejam participar da rede em momentos específicos e de forma rápida e também de dispositivos que se movem fisicamente sobre a área de cobertura da rede. Para ambos os casos o tempo é utilizado como métrica de avaliação, onde deseja-se um menor tempo para um dispositivo intermitente cumprir sua função na rede e um menor tempo para um dispositivo móvel encontrar uma nova rota de comunicação durante o processo de *handover*.

4 DESENVOLVIMENTO

Tendo em vista a falta de suporte à mobilidade apresentada pelos atuais protocolos para comunicação sem fio em ambientes industriais, este trabalho propõe o desenvolvimento de técnicas focadas em estabelecer um ambiente adequado para esses dispositivos e desta forma expandir as aplicações em RSSFI. Isso possibilita, por exemplo, a comunicação da rede industrial com dispositivos móveis ou de característica intermitente, que não estão sempre operando sobre a área de cobertura da rede. De forma geral, a Figura 8 apresenta as estratégias de gerenciamento propostas para o tema de mobilidade em RSSFI, que são detalhadas neste capítulo.

Figura 8 – Visão geral das propostas apresentadas neste capítulo.



Fonte: do autor

As técnicas propostas buscam atender a dois momentos distintos de operação de dispositivos móveis, um associado a sua agregação na rede e outro referente a manutenção da conectividade com a rede. Inicialmente, uma técnica é proposta para acelerar o acesso a dados de dispositivos móveis, e para isso é preciso modificar o processo de agregação de novos dispositivos. No padrão WH, este processo é lento devido devido aos diver-

sos procedimentos empregados, que visam garantir robustez e segurança. Há uma série de requisitos que devem ser verificados e configurações a serem realizadas para que este processo ocorra de forma a cumprir os requisitos de operação da rede. Isso envolve a troca de diversas mensagens na rede que podem também estar associadas a diversos saltos para que a mensagem chegue ao destino devido à topologia da rede. Já para o segundo caso, é empregada uma técnica conhecida como *handover*, onde o dispositivo precisa alterar seu enlace de dados para manter sua conectividade com a rede. Neste caso foi avaliado um cenário onde os dispositivos já se encontram conectados com a rede e estão em operação. Também são propostas estratégias de gerenciamento para o caso de *handover* durante o processo de agregação de dispositivos. Por fim, são sugeridas modificações para a propagação segura de dados dentre outras considerações sobre segurança e consumo de energia.

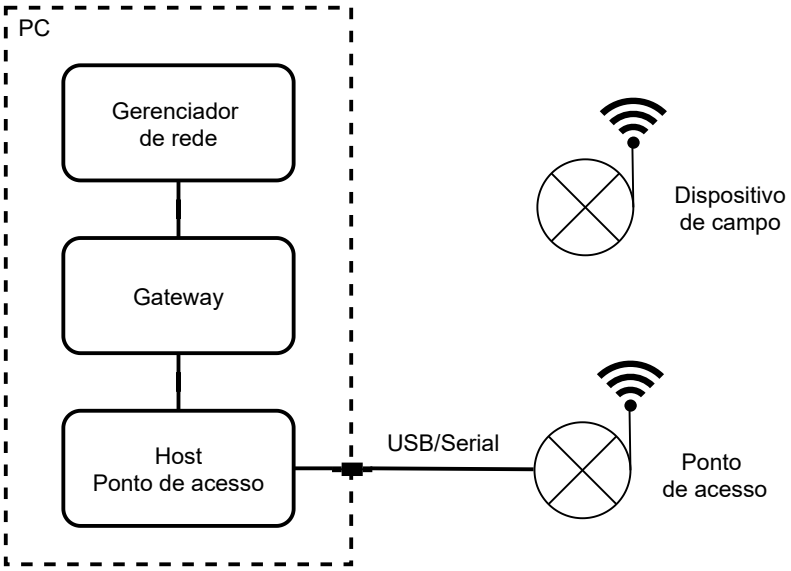
4.1 Materiais

Os experimentos realizados neste trabalho são práticos e utilizam de uma estrutura para criar e manter redes WH. Como elemento principal tem-se um *gateway*, desenvolvido em (CAINELLI *et al.*, 2020), que possibilita a criação de redes compatíveis com o protocolo WH e que devido sua característica de customização permite a implementação de modificações nos processos padrões. O *gateway* é, na verdade, composto por três aplicações: o gerenciador de rede, o *gateway* e o *host* do ponto de acesso. Essas aplicações rodam em um computador com sistema operacional Linux e se conectam conforme apresentado na Figura 9.

Todos dispositivos de campo e o ponto de acesso utilizam do mesmo hardware, que foi desenvolvido em (MÜLLER *et al.*, 2010). Desta forma, utilizando-se diferentes firmwares, define-se o dispositivo como fixo, móvel ou ponto de acesso. O equipamento conta com um transceptor de rádio frequência padrão IEEE 802.15.4 que opera na banda de frequência 2,4 GHz (NXP, 2013). Na Figura 10 é apresentado o rádio utilizado que é compatível com o padrão WH.

Os experimentos realizados também incluem a utilização de um coprocessador para gerenciamento local de dispositivos, que é uma aplicação desenvolvida em (MÜLLER, 2012), que apresenta como principal característica a capacidade de enviar comandos HART para dispositivos compatíveis com o protocolo. Esta ferramente é executada em

Figura 9 – Estrutura do gerenciador de rede.



Fonte: do autor

Figura 10 – Rádio compatível com o padrão WH.

Fonte: (MÜLLER *et al.*, 2010)

um computador e se comunica com o dispositivo por meio de uma porta de manutenção RS-485. O coprocessador tem implementados os principais comandos HART que podem ser controlados pelo usuário através de uma interface gráfica. Isso permite extrair informações e modificar parâmetros da rede de forma descentralizada.

4.2 Métodos

Os métodos propostos buscam estabelecer modificações nos procedimentos padrões executados em redes WH para que seja possível prover suporte a dispositivos móveis, tendo em vista duas situações que representam grande parte das aplicações envolvendo mobilidade de nodos em RSSFI. São elas: dispositivos com atividade intermitente na rede, ou seja, permanecem sobre o alcance da rede por um determinado tempo e, dentro desse tempo, precisam executar sua função na rede; e dispositivos que se conectam à rede e se movem dentro da área de cobertura da rede.

O primeiro caso, de dispositivos intermites, será abordado como uma técnica de coleta rápida de dados, já o segundo caso como *handover*.

4.2.1 Coleta rápida de dados

A situação onde dispositivos móveis apresentam atividade intermitente na rede exige que seu processo de agregação seja rápido devido sua possível restrição de tempo sobre a área de cobertura da rede. Como forma de simular a atuação de um dispositivo na rede, determinou-se como função do dispositivo a execução do serviço de publicação, onde o dispositivo compartilha informações com a rede. Para utilizar o serviço de publicação, o dispositivo é configurado para operar no modo *burst*, onde envia dados periodicamente através de comandos em formato de resposta sem a necessidade de uma requisição. A definição de quais dados são enviados e em que intervalo de tampo, são configuradas por uma série de comandos que podem ser executados com a rede em operação ou previamente ao processo de agregação, onde nesta última opção o dispositivo passa a executar o serviço de publicação de forma automática imediatamente após concluir o processo de agregação. O dado utilizado neste trabalho para o serviço de publicação é a variável primária (PV - *Primary Variable*), que é enviada para o gateway ficando disponível para que aplicações externas possam acessá-la.

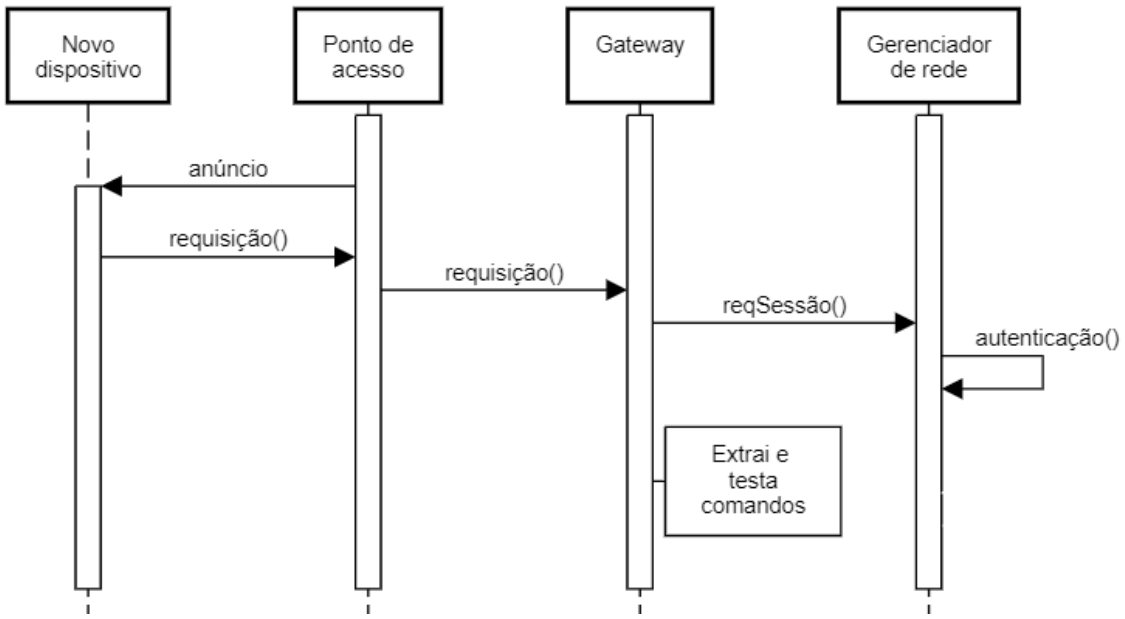
No processo padrão, o serviço de publicação só pode ser executado após o término do processo de agregação onde o dispositivo é definido como conectado e uma sessão com o *gateway* é criada. Em mais detalhes esse processo padrão é apresentado na subseção 2.3.2. Visto que toda vez que o dispositivo é ativado e deseja publicar sua variável no *gateway* é necessário realizar um novo processo de agregação, desta forma propõe-se uma técnica que armazena a variável no *gateway* de forma mais rápida que o processo convencional.

Nesse novo cenário o dispositivo não será considerado pela rede como um dispositivo conectado, apenas utilizará o processo de agregação como meio de publicação de sua variável. O método proposto utiliza o mesmo provisionamento inicial e o tempo de sincronização do dispositivo com a rede. Então, após definir um dispositivo como *proxy*, uma requisição de agregação modificada é enviada para o gerenciador de rede. A fim de apresentar o comportamento desejado, o firmware desses dispositivos móveis foi alterado para gerar uma requisição de agregação com comandos diferentes. A mensagem é encaminhada pela rede até que chegue ao *gateway*. Nesse momento, seguindo o procedimento padrão, o *gateway* identifica que se trata de uma mensagem de um novo dispositivo e solicita uma sessão de agregação para o dispositivo para estabelecer uma comunicação segura com o gerenciador de rede. Então, o gerenciador de rede executa procedimentos de segurança para verificar se o novo dispositivo está apto a participar da rede e se confirmado, o comando de escrita de sessão é enviado ao novo dispositivo que por sua vez deve confirmar o recebimento da mensagem por meio do envio da resposta. Uma vez que a sessão de agregação é criada com sucesso, o *gateway* pode encaminhar a requisição de agregação para o gerenciador de rede. Por questões de segurança, o pacote contendo a requisição de agregação é encaminha pela rede de forma encriptada, e é nesse momento, após a criação da sessão de agregação, que a mensagem é decifrada e seu conteúdo pode ser acessado. Nessa etapa foi adicionada uma estrutura de decisão, no *gateway*, para verificar se a requisição enviada é proveniente de um dispositivo padrão ou de um dispositivo móvel cujo firmware foi modificado. Na Figura 11, o processo para coleta rápida de dados é apresentado de forma simplificada em um diagrama de sequências.

O dispositivo modificado gera uma requisição de agregação diferente onde o comando 787, que indica o nível de sinal de vizinhos, foi removido. Esse comando é importante para o gerenciador de rede, mas na técnica proposta a mensagem não chega até ele, o que torna esse comando dispensável. Em seu lugar foi adicionado o comando 1, em formato de resposta, que lê a variável primária do dispositivo. Essa é uma das quatro variáveis dinâmicas disponíveis para utilização no protocolo.

Com base no tipo de requisição, o *gateway* segue de maneira distinta. Para o caso de uma requisição padrão o algoritmo segue o protocolo padrão WH, conforme apresentado anteriormente na sessão 2.3.2. Já para o método proposto, quando se trata de um dispositivo móvel de característica intermitente, o conteúdo da requisição é extraído e a variável

Figura 11 – Diagrama de sequências da técnica proposta para coleta rápida de dados.



Fonte: do autor

primária é armazenada em um *buffer* no *gateway*.

4.2.2 *Handover* na etapa de operação

A utilização de dispositivos móveis em RSSFI exige que os mecanismos de gerenciamento da rede sejam adequados para atender às necessidades de operação destes elementos. A forma de movimento pode apresentar características distintas de velocidade e trajeto dependendo da aplicação em questão. Desta forma, soluções genéricas podem ser otimizadas para um determinado caso se as características de operação forem bem conhecidas e assim, modelar o sistema de forma adequada.

De forma geral, as técnicas de *handover* são empregadas em redes com nodos móveis para estabelecer um novo enlace de comunicação para um dispositivo assim que verificado um determinado nível de degradação no enlace atual. O processo de descobrimento de vizinhos está diretamente associado ao desempenho do *handover*, uma vez que representa o tempo necessário para encontrar uma nova alternativa para a comunicação.

No protocolo de comunicação WH, o processo de descobrimento de vizinhos é realizado através do envio de mensagens periódicas chamadas de *health report*. Estas mensagem são enviadas por dispositivos que já fazem parte da rede com destino ao gerenciador de rede informando dados estatísticos sobre vizinhos. As estatísticas sobre outros disposi-

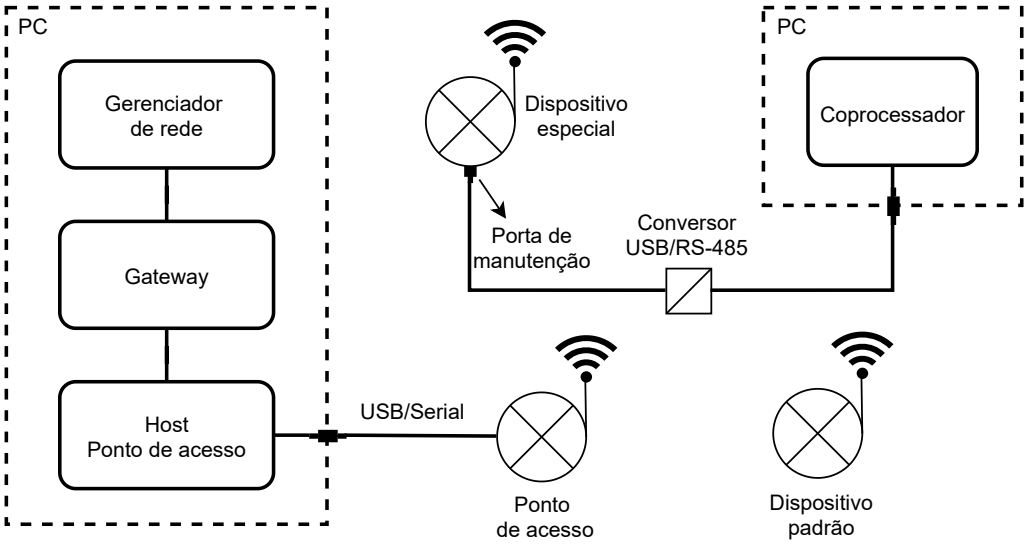
tivos são obtidas pela análise de mensagens transmitidas pela rede. Assim, o gerenciador de rede pode atuar para otimizar a configuração da rede e, por exemplo, estabelecer novas rotas de comunicação. O serviço de descobrimento de vizinhos é iniciado no momento em que o dispositivo atinge o estado de quarentena do processo de agregação. A primeira mensagem de *health report* é gerada após a identificação de pelo menos três vizinhos ou como consequência do fim da contagem do temporizador associado a esta função. Uma vez sinalizada a necessidade do envio de um *health report*, um agendamento é feito para enviá-lo no próximo link de descobrimento disponível. Uma mensagem de *health report* é composta por três comandos em formato de resposta, que são eles: comando 780 (*Report Neighbor Health List*) no qual são informadas as estatísticas de comunicações (envios/falhas/recepções) e de média de nível de sinal recebido (RSL - *Received Signal Level*) sobre vizinhos já conectados, ou seja, que apresentam enlace de comunicação entre si; comando 787 (*Report Neighbor Signal Level*) que indica estatísticas somente sobre RSL de vizinhos não conectados; e o comando 779 (*Report Device Health*) que contém estatísticas de comunicações do dispositivo de origem.

É através do serviço de descobrimento de vizinhos que o gerenciador de rede avalia as condições da rede e toma decisões para melhorar o desempenho da rede. Em uma situação ideal, para atender à dinamicidade de uma rede com nodos móveis, o serviço de descobrimento de vizinhos deve ser capaz de notificar ao gerenciador de rede as variações nas estatísticas adquiridas geradas pelo movimento físico do nodo. Porém, em RSSFI convencionais como o WH, quando um dispositivo é afastado de seu ponto de conexão a uma distância em que há a perda da conectividade e passa a gerar falhas de comunicação, o gerenciador de rede interpreta inicialmente esta situação como uma possível falha temporária e age de maneira a contorná-la e reestabelecer a conexão perdida. Só no momento em que os dispositivos que eram vizinhos notificarem ao gerenciador que o dispositivo já não está mais presente em suas tabelas de vizinhos, através do *health report*, é que o gerenciador deduz a desconexão e remove toda sua configuração da rede. E para participar novamente da rede este dispositivo precisa passar por todo processo de agregação como se fosse a primeira vez.

Dentro deste contexto, propõe-se uma técnica de *hard handover* para tratar a presença de dispositivos móveis e acelerar o processo de atualização de topologia. A situação utilizada como base para o experimento apresenta uma rede já formada com nodos fixos

e um dispositivo móvel especial que apresenta características próprias de gerenciamento que são controladas por um processo local, que neste caso foi emulado por uma aplicação externa ligada a sua porta de manutenção. Esta estrutura é apresentada na Figura 12.

Figura 12 – Estrutura de rede utilizada na técnica de *handover*.



Fonte: do autor

A abordagem utilizada visa avaliar a qualidade dos enlaces de comunicação de vizinhos e quando necessário tomar a decisão de realizar o *handover* para que o dispositivo estabeleça uma nova conexão. Optou-se por utilizar a métrica de RSL, que representa a potência do sinal recebido (medido em dBm), como parâmetro de decisão visto que é uma variável de fácil acesso e que apresenta uma relação entre o nível de sinal e o movimento físico de um nodo. Esta não é uma relação direta, visto que não só a distância de um nodo influencia no valor médio de RSL apresentado. O valor de RSL pode apresentar muitas oscilações devido as características de operação do ambiente industrial, e por isso o protocolo emprega um filtro digital do tipo IIR conforme apresentado em (1):

$$RSL_{Médio} = RSL_{Anterior} - \left(\frac{RSL_{Anterior}}{RSL_{Damp}}\right) + \left(\frac{RSL_{Medido}}{RSL_{Damp}}\right) \quad (1)$$

Onde RSL_{Medido} é o valor de RSL do pacote atual, $RSL_{Anterior}$ é o valor médio anterior e RSL_{Damp} é uma constante que representa o fator de amortecimento. Esta constante deve ser uma potência de 2, o padrão é 64 e pode ser definida pelo usuário para para ajustar a resposta do filtro.

Criou-se um novo *script* no coprocessador que faz uma avaliação periódica dos valores

de RSL de vizinhos conectados através do comando 780 (*Report Neighbor Health List*) que dentre as informações coletadas sobre as comunicações, este comando apresenta a média de RSL desde a última requisição. Através da avaliação periódica do RSL e um valor de gatilho para decisão do *handover* é possível gerenciar de forma mais rápida o processo de busca por uma nova conexão quando comparado com o processo padrão de descobrimento de vizinhos. Neste casou definiu-se o valor de gatilho como -75 dBm que é o valor de sensibilidade mínima do rádio de acordo com o padrão IEEE 802.15.4. Quando verificada a redução no valor de RSL a um nível que represente a necessidade de um novo enlace, o coprocessador envia um comando de desconexão para o dispositivo (comando 960 - *Disconnect Device*). Este comando força a saída do dispositivo removendo suas configurações da rede e reinicializando seu estado de agregação para o estado inicial de forma que o dispositivo já possa buscar uma nova conexão. Como se trata de um *hard handover* considera-se um período de tempo em que o dispositivo perde a conexão com a rede, que neste caso é o tempo necessário para realizar um novo processo de agregação. O procedimento proposto é apresentado na Figura 13 como uma máquina de estados finita implementada no coprocessador.

Figura 13 – Representação por máquina de estados finita do processo realizado pelo co-processador para gerenciamento do *handover*.

Fonte: do autor

4.2.3 *Handover* na etapa de agregação

Embora a técnica para uso de dispositivos móveis baseada em *hard handover* seja factível, algumas lacunas não são preenchidas por ela. Sendo assim, sugere-se a investigação de outras técnicas a fim de minimizar tempos de processo. Nesta subseção, uma proposta de *soft handover* é apresentada para a etapa de agregação de dispositivos. Embora não tenha sido implementada, a proposta é modelada para análise de viabilidade e desenvolvimento em trabalho futuro.

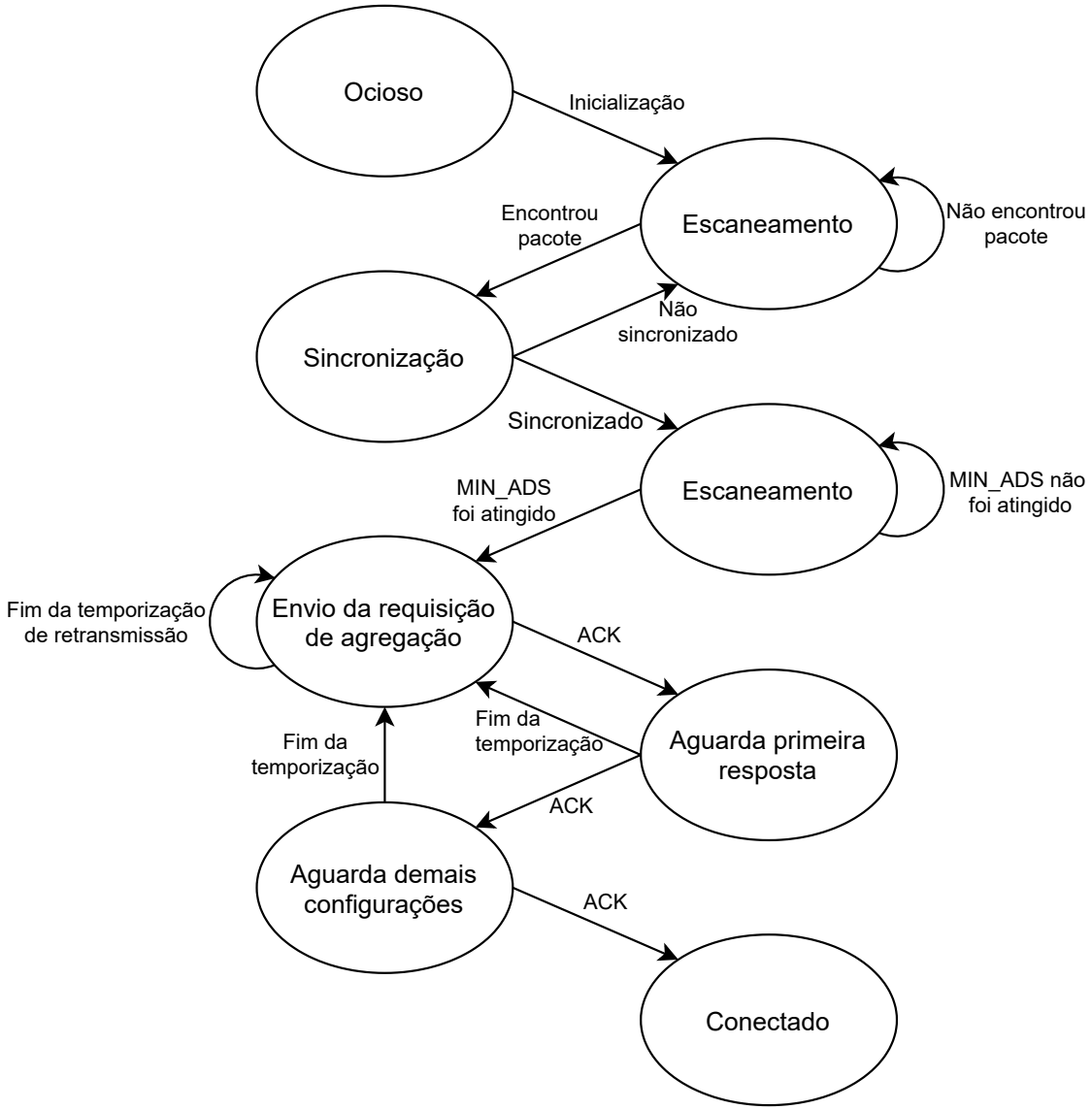
Como apresentado na subseção 2.3.2, o processo de agregação de um dispositivo de campo à rede segue um modelo claramente definido na norma do protocolo WH. O modelo é implementado como uma máquina de estados no dispositivo padrão, conforme a Figura 14. Nesta representação é possível observar com mais detalhes o processo realizado antes do envio de uma requisição de agregação, onde o dispositivos apresenta dois estados de escaneamento. Nestes estados, o dispositivo realiza uma busca por comunicações da rede que é feita de forma sequencial nos canais de comunicação. No primeiro estado de escaneamento, o dispositivo utiliza as comunicações encontradas para realizar e confirmar a sincronização com o tempo da rede. Uma vez confirmada a sincronização, o dispositivo passa novamente para um estado de escaneamento onde busca por anúncios da rede. Quando atingido o valor mínimo de anúncios encontrados (definido na Figura 12 como MIN_ADS), o dispositivo escolhe o melhor candidato anunciante que é pelo qual será enviada a requisição de agregação no próximo estado.

A fim de propiciar o *soft handover* e manter mais de uma conexão ativa durante a etapa de agregação, duas abordagens são sugeridas, uma incluindo modificações na camada de enlace, rede e aplicação do protocolo para que o dispositivo móvel possa lidar com possíveis reconexões durante o processo de agregação e outra no gerenciador de rede, para que provisione o dispositivo móvel com informações suficientes para que este possa se conectar com mais de um dispositivo na rede. Ainda, uma combinação das duas abordagens também é possível.

4.2.3.1 Alterações no firmware do dispositivo móvel

Para entendimento da proposta, o processo convencional de agregação de um dispositivo é mostrado na Figura 14, na forma de máquina de estados finita. O modelo para *soft handover* baseado na alteração do comportamento do processo de agregação de um

Figura 14 – Representação por máquina de estados finita do processo de agregação padrão realizado pelo dispositivo de campo.

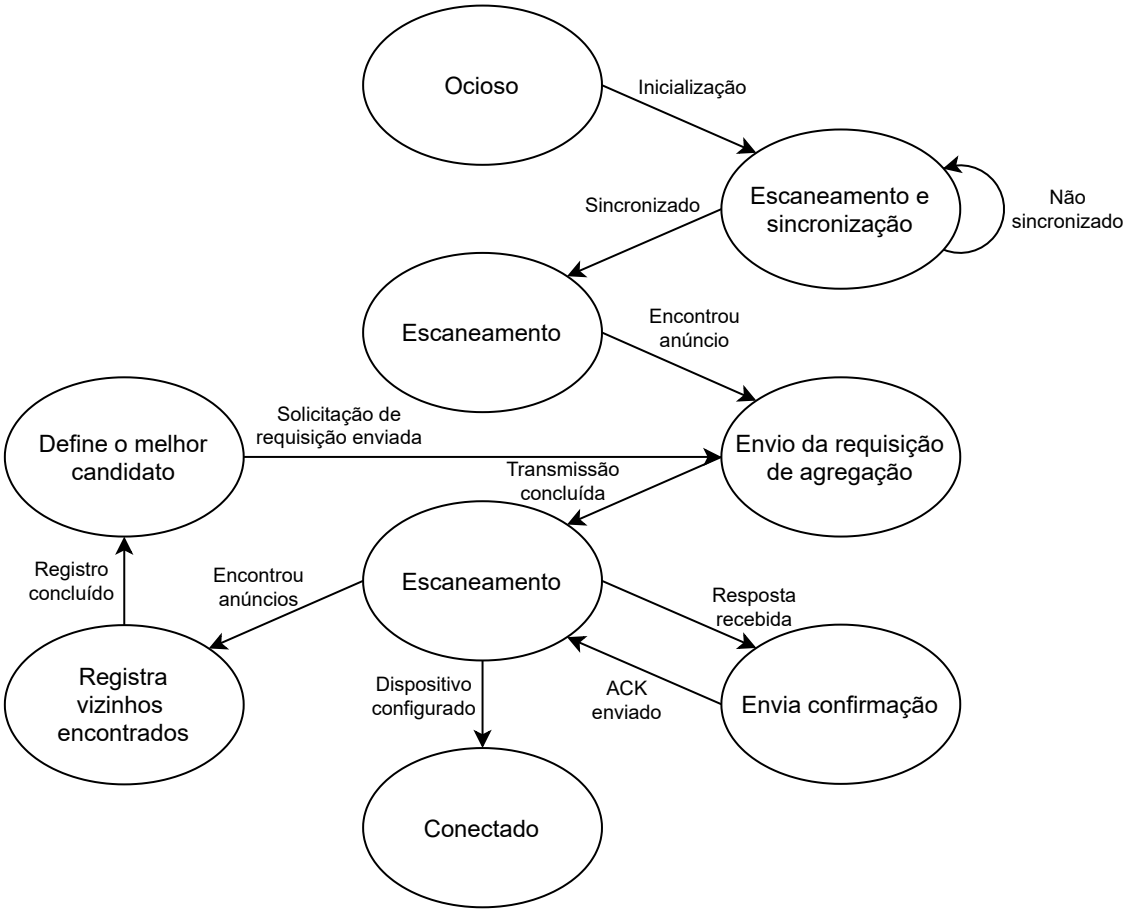


Fonte: do autor

dispositivo é apresentado na Figura 15.

Inicialmente o processo ocorre de forma semelhante ao padrão, onde o dispositivo realiza a tarefa de sincronização por meio do escaneamento dos canais em busca de comunicações da rede. Ao passar para o segundo estado de escaneamento, o dispositivo busca por um anúncio e quando o encontra já passa para o próximo estado para enviar sua requisição de agregação. Neste caso, opta-se por responder ao primeiro anúncio mesmo que este não seja o melhor candidato visto que se quer uma resposta rápida e eventualmente melhores candidatos também receberão requisições na sequência.

Figura 15 – Representação por máquina de estados finita do processo de agregação modificado para o dispositivo de campo.



Fonte: do autor

A abordagem considerada altera a máquina de estados do processo de agregação para que o escaneamento de vizinho continue ativo. Na medida em que o processo evolui, o dispositivo decide através de uma tarefa de aplicação, se envia pedido de requisição para ingresso na rede novamente, seja para o mesmo vizinho para o qual enviou anteriormente, seja para outro, escolhido da sua tabela de vizinhos, levando-se em consideração o RSL percebido. Nesta abordagem o dispositivo passa para um novo estado de escaneamento, após o envio da requisição de agregação que pode ser observado na Figura 15, onde o dispositivo aguarda as respostas do gerenciador de rede mas também continua na busca por anúncios da rede. Periodicamente, os vizinhos percebidos são registrados e uma nova requisição é enviada para o melhor candidato de sua tabela.

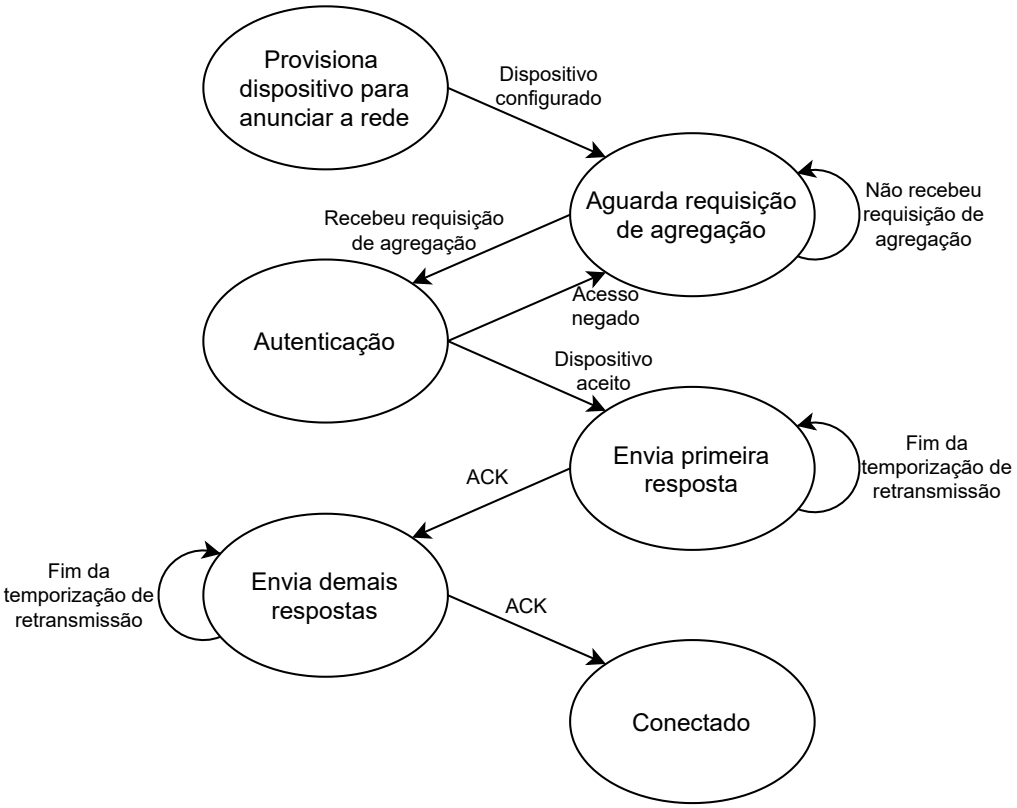
Uma vez proposto o modelo, o firmware do dispositivo deve ser alterado profundamente, uma vez que há um processo concorrente importante, onde o pedido de requisição

é enviado periodicamente para um vizinho paralelamente (ou pelo menos, anteriormente) ao escaneamento de novos vizinhos.

4.2.3.2 Alterações no gerenciador de rede

Para entendimento da proposta, o processo convencional de agregação de um dispositivo feito pelo gerenciador de rede é mostrado na Figura 16, na forma de máquina de estados finita. O modelo para *soft handover* baseado no comportamento do gerenciamento de rede é proposto como uma alteração do algoritmo de inclusão de novos dispositivos na rede, conforme o modelo apresentado na Figura 17.

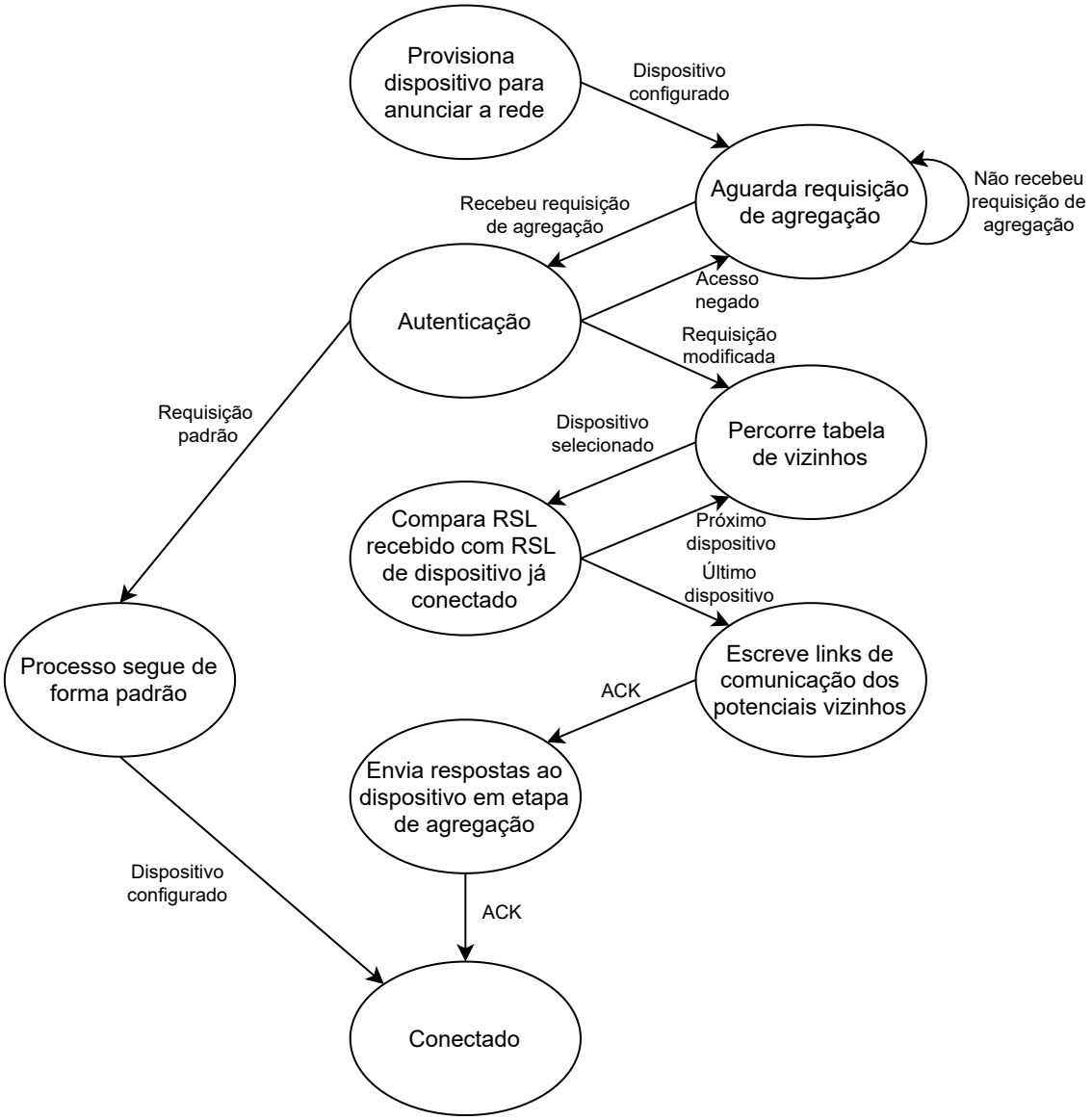
Figura 16 – Representação por máquina de estados finita do processo de agregação padrão realizado pelo gerenciador de rede.



Fonte: do autor

Inicialmente, o processo é alterado pela verificação da resposta não convencional dos comandos 0, 20 e 1, enviados pelo dispositivo móvel. A partir deste momento, o gerenciador tem seu comportamento alterado, objetivando o envio de mais links para prover acesso contínuo ao dispositivo móvel. Em concordância com o conceito *soft handover*, o dispositivo móvel disporá de mais links para tentar manter-se na rede, e fará isso no-

Figura 17 – Representação por máquina de estados finita do processo de agregação modificado para o gerenciador de rede.



Fonte: do autor

vamente em nível de aplicação, avaliando a potência dos sinais dos vizinhos na medida em se move pela rede. A diferença em relação à proposta anterior, está na recepção prévia dos links para comunicação com os vizinhos, enviada pelo gerenciador modificado. Como dificuldade adicional, salienta-se a possibilidade de que os links enviados sejam de vizinhos que já não estão mais no alcance do dispositivo móvel.

4.3 Considerações sobre segurança

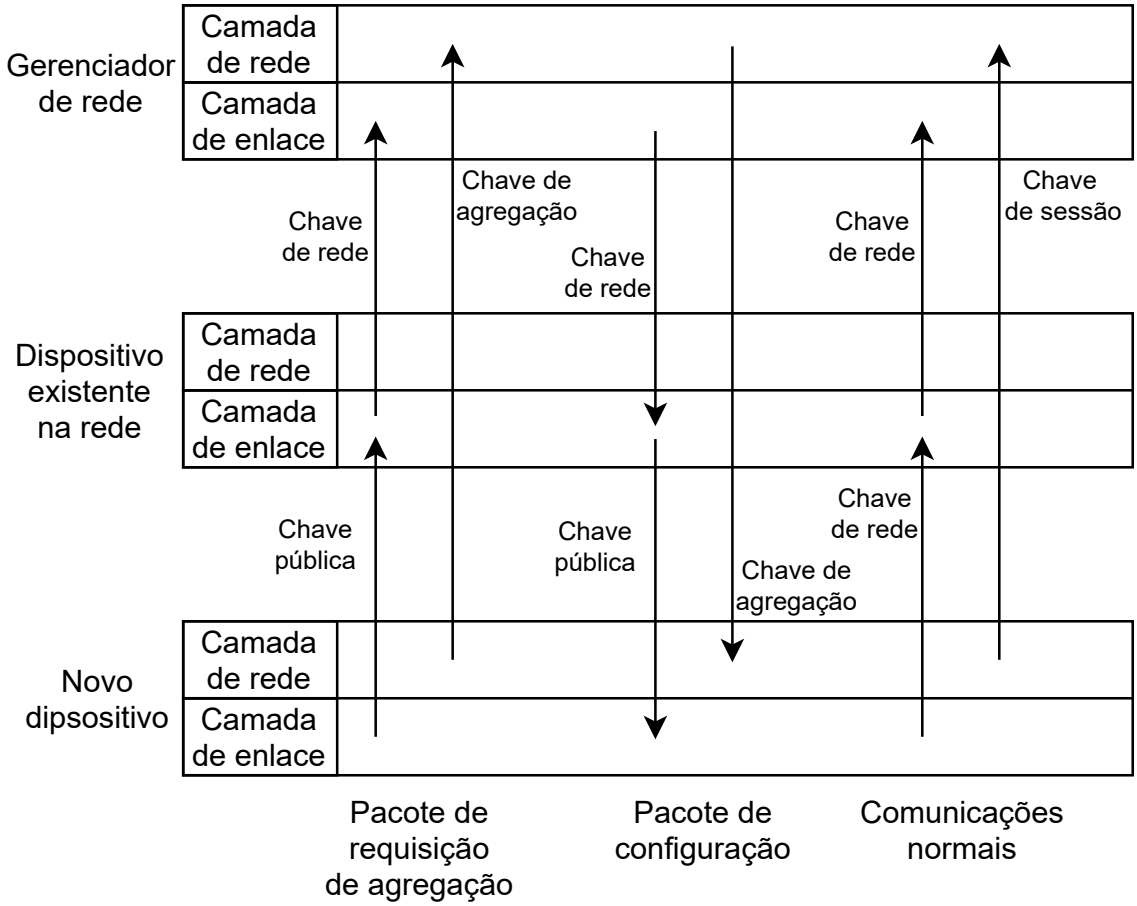
O protocolo utilizado como base para este trabalho, o WH, é um sistema seguro e apresenta serviços de segurança nas camadas de enlace e de rede. Na camada de enlace a integridade dos dados é verificada a cada evento de comunicação em nível de enlace, ou seja, ponto-a-ponto. O processo combina um método de verificação cíclica de redundância (CRC - *Cyclic Redundancy Check*) e um código de integridade de mensagem (MIC - *Message Integrity Code*). O CRC é empregado sobre todo DLPDU e o MIC é uma variável resultante do algoritmo de encriptação que dentre os parâmetros de entrada inclui uma chave de segurança de 128 bits, que neste caso é a chave de rede, e o *nonce* que é um número construído para ser único para o pacote atual já que depende do valor de ASN e do endereço do dispositivo de origem. O *nonce* é utilizado para garantir que comunicações não sejam reusadas em ataques de repetição. Caso o dispositivo esteja em processo de agregação e ainda não tenha uma chave de rede, uma chave bem conhecida é utilizada em seu lugar. Esta chave também é utilizada em pacotes de anúncio e tem valor igual para todos dispositivos da rede. A chave bem conhecida é pública e tem valor hexadecimal de 7777 772E 6861 7274 636F 6D6D 2E6F 7267. Na camada de enlace os dados do pacote não são encriptados, apenas é feita a autenticação da mensagem através da geração e comparação do MIC.

Já na camada de rede são utilizadas diversas chaves de segurança e também a encriptação de dados para prover confidencialidade e integridade de conexões fim-a-fim. O cabeçalho do pacote da camada de rede não é encriptado para permitir que dispositivos intermediários possam encaminhar a mensagem pela rede. Um dos parâmetros utilizados na encriptação do conteúdo do pacote é chave de sessão, que é única para cada conexão fim-a-fim entre dois dispositivos da rede. Caso o dispositivo se encontre em processo de agregação e ainda não tenha uma sessão com o gerenciador de rede, a chave de agregação é utilizada neste caso.

A representação de utilização de chaves de segurança nas camadas de enlace e de rede são apresentadas na Figura 18. Quando o dispositivo se encontra em processo de agregação, a chave pública para gerar o MIC na camada de enlace e utiliza a chave de agregação para gerar o MIC na camada de rede e encriptar o conteúdo da requisição de agregação. Após a autenticação do dispositivo o gerenciador de rede gera uma chave de sessão e estabelece uma comunicação segura com o dispositivo. Então, o dispositivo

passa a utilizar a chave de rede para autenticação na camada de enlace e a chave de sessão recebida para autenticação e encriptação na camada de rede.

Figura 18 – Uso das chaves de segurança em comunicações.



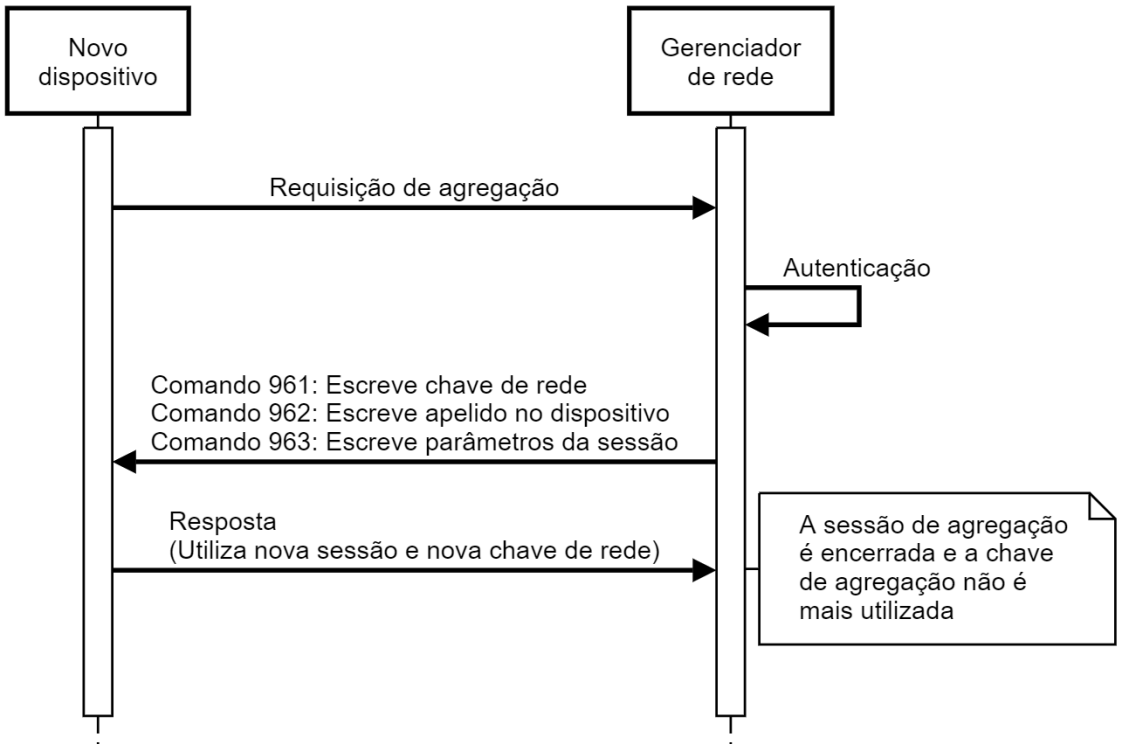
Fonte: adaptado de (CHEN; NIXON; MOK, 2010)

Ambas as chaves de rede e de sessão são trocadas logo no início do processo de agregação após a autenticação do dispositivo, conforme a Figura 19 demonstra. Isso necessário, uma vez que a chave de rede inicial é uma chave bem conhecida, de domínio público e a chave de sessão inicial é na verdade a chave de agregação. A chave de agregação é programada no gerenciador de rede e no dispositivo a ser adicionado na rede.

As modificações aqui propostas visam a rápida agregação e desagregação dos dispositivos móveis e intermitentes, numa rede baseada no protocolo WH. Isto implica necessariamente em uma redução drástica no número de mensagens trocadas entre o gerenciador e o dispositivo móvel, seja em enlace direto, via ponto de acesso, ou via *proxy*. Do ponto de vista de segurança algumas características são comprometidas da seguinte forma:

- O enlace ponto-a-ponto, uma vez capturado pode ser “quebrado” em força bruta,

Figura 19 – Chaves de segurança recebidas nas comunicações iniciais.



Fonte: do autor

uma vez que a chave criptográfica utilizada é pública, restando a descoberta do *nonce* adequado, que está relacionado ao ASN. Uma vez capturara de decifrada, novas mensagens poderão ser criadas, e estas serão válidas, a menos do conhecimento do dispositivo invasor sobre os *slots* válidos para recepção de mensagens.

- A confidencialidade do enlace fim-a-fim será comprometida apenas se a chave de agregação for descoberta, e, uma vez que não há propagação da mesma pela rede, apenas se esta for descoberta de forma de forma direta, a segurança estará comprometida. Como forma direta de descoberta entende-se pelo acesso ao software de configuração do gerenciador de rede, ou pelo acesso ao software de configuração dos dispositivos de campo.

Como medidas preventivas de diminuição da segurança prevista no protocolo original, sugerem-se as seguintes modificações no processo de agregação e desagregação dos dispositivos móveis ou intermitentes:

- Envio da nova chave de rede para o dispositivo móvel/intermitente, que passa a propagar a variável de processo com a nova chave. Neste processo, explicitado

pelo diagrama de sequências da Figura 20, o dispositivo móvel entra em modo "pré agregado" e, na ocasião de troca de par, envia duas requisições de agregação, uma utilizando a chave rede bem conhecida e outra com a chave de rede modificada, previamente recebida pelo gerenciador. Desta forma, o dispositivo *proxy* poderá encaminhar os dados de processo do móvel, uma vez que consegue autenticar com a chave bem conhecida, mas, ao receber a mesma mensagem autenticada com a chave de rede trocada, também a reconhece, uma vez que a chave de rede é a mesma para todos os dispositivos da rede. Ainda, será necessária a modificação da máquina de estados do dispositivo *proxy*, que ao receber uma segunda requisição do dispositivo móvel, com o MIC encriptado com a nova chave de rede, deverá sinalizar o gerenciador que está encaminhando uma mensagem de um dispositivo móvel seguro.

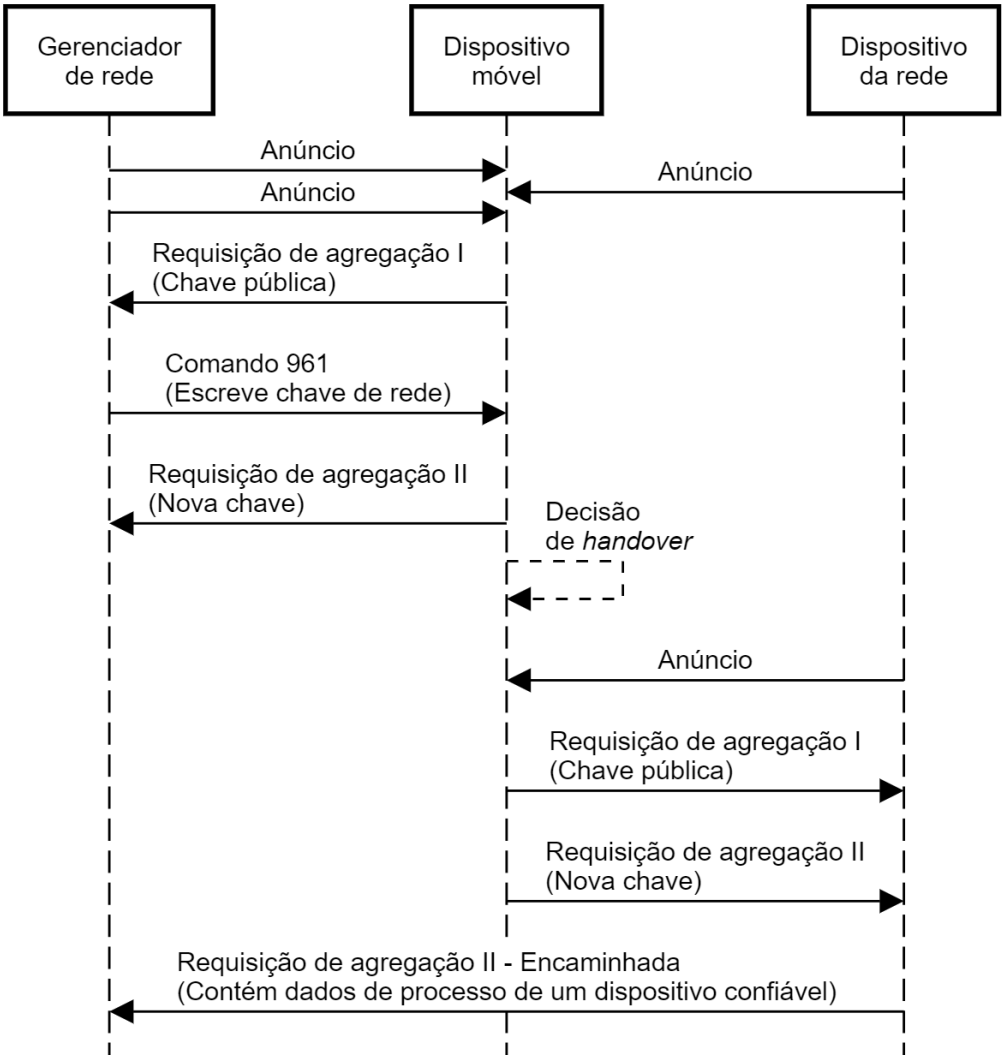
No caso do processo de agregação ocorrer diretamente por um dispositivo *proxy*, o mesmo deverá seguir o protocolo da Figura 21, onde o dispositivo *proxy* gera por conta própria o envio do comando 961 para a troca da chave de rede, uma vez que já possui a mesma. Neste caso, cabe questionar a quebra do nível de segurança ocasionado pela descentralização do gerenciamento, uma vez que dispositivos da rede que não o gerenciador poderão enviar dados relacionados à segurança da rede.

- Outra possibilidade sugerida é o envio de anúncios encriptados com uma chave de agregação diferente a da chave comumente utilizada, no caso, uma chave específica para dispositivos móveis, conforme apresentado na Figura 22. Como desvantagem, o tempo para agregação seria aumentado, uma vez que as mensagens encriptadas com cada uma das chaves seria alternada. Ainda, o escalonamento provido pelo anúncio ao dispositivo móvel poderia ser diferente do provido a um dispositivo fixo.

- Em nível de gerenciamento ainda mais alto, as mensagens enviadas pelo dispositivo móvel aos seus pares, que se modificam ao longo do trajeto, poderiam ser "autenticadas" pelo comportamento dos enlaces, que poderia ser repetitivo no caso de um AGV ou de uma máquina rotativa.

Outras estratégias podem ser elaboradas, porém, deve-se considerar a robustez em nível físico e de enlace, uma vez que os saltos entre os 15 canais de comunicação do WH já

Figura 20 – Proposta de modificação para propagação de dados de forma segura.



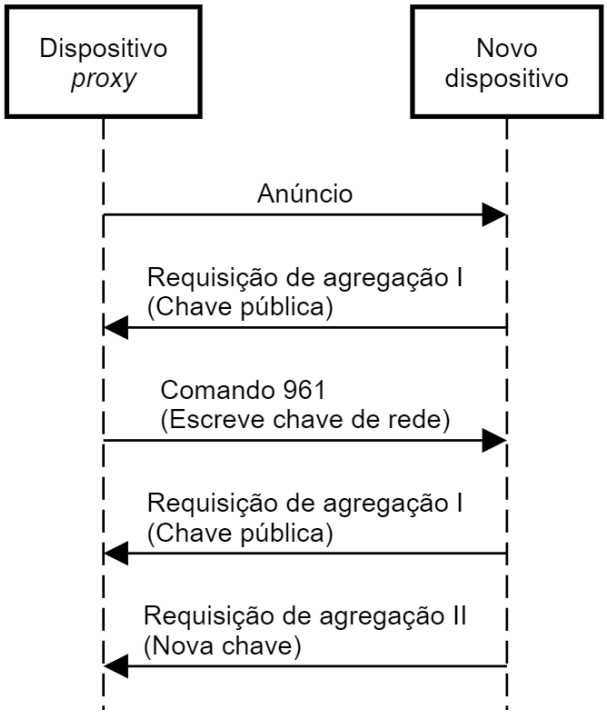
Fonte: do autor

propiciam certo grau de segurança. Os saltos são conhecidos apenas por dispositivos que podem decifrar o pacote de anúncio, devidamente encriptado com a chave de segurança.

4.4 Considerações sobre consumo de energia

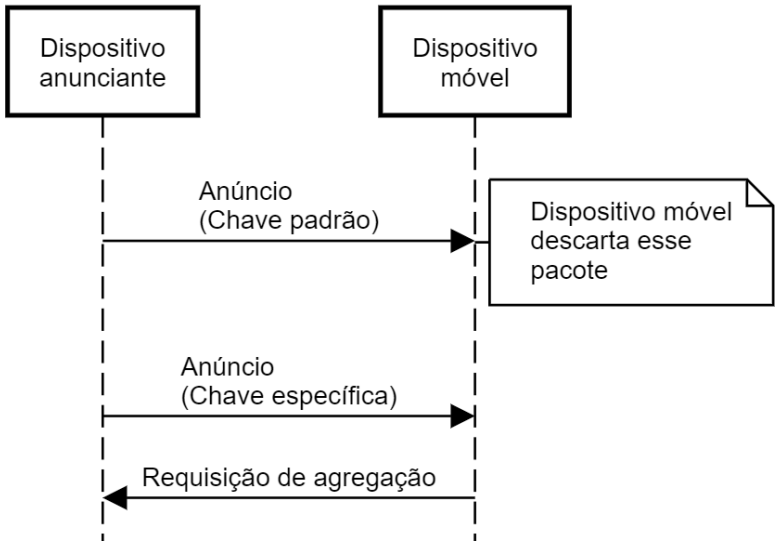
Outra característica do protocolo que é comprometida pelas mudanças aqui propostas é o baixo consumo de energia, requisito fundamental para sistemas baseados em RSSFI. Pelo fato de conectar, desconectar e reconectar na rede, além de passar por longos períodos em modo recepção, a corrente elétrica média demandada pelo transceptor é maior em comparação com transceptores de RSSFI convencionais. Conforme mencionado anteriormente, o transceptor utilizado neste trabalho é derivado de trabalhos anteriores (MÜLLER

Figura 21 – Proposta de modificação para agregação por *proxy*.



Fonte: do autor

Figura 22 – Proposta de modificação na divulgação da rede.



Fonte: do autor

et al., 2010) e estudos subsequentes foram realizados a fim de se obter um modelo do consumo de energia do mesmo. Os resultados deste estudo prévio apresentam o modelo de consumo do transceptor em função dos eventos de comunicação correntes (*sleep*, ocioso,

transmitindo, recebendo e detectando energia do canal RF) (MÜLLER *et al.*, 2016). O modelo revela, como esperado, que a diferença entre estados operacionais do transceptor implica em quantidades de energia demandada muito maiores que no estado *sleep*, conforme a Tabela 2. A fim de comparar o consumo médio de energia, é possível avaliar duas aplicações distintas, uma relativa ao processo de agregação de um dispositivo convencional e outra, de um dispositivo móvel em operação *hard handover*. Para tanto, os algoritmos de predição de consumo de energia devem ser carregados na pilha do protocolo para a realização da coleta dos dados, conforme proposto no trabalho anterior. Esta atividade é considerada como possível trabalho futuro.

Tabela 2 – Consumo registrado em uma comunicação de transmissão com confirmação do dispositivo de destino (ACK)

Estado	Consumo [mW]
Transmissão	191,4
Recepção	92,4
Ocioso	13,2
Detecção de energia	85,8
Sleep	0,495

Mas, com o intuito de antever os possíveis resultados bem como as possíveis soluções, apresentam-se aqui as considerações sobre o consumo de energia em função das aplicações anteriormente mencionadas, que utilizam dispositivos móveis.

- AGV (*Automated Guided Vehicle*): neste caso, o dispositivo móvel poderá ser alimentado pelo próprio AGV, o que reduz a necessidade de baixo consumo por parte do transceptor. O consumo de energia demandado pelos motores elétricos do AGV é muito superior ao demandado pelo transceptor, de modo que é considerado desprezível;

- Dispositivo intermitente fixo gerador de alarmes: um equipamento deste tipo, como um chuveiro em uma planta química, quando usado deve gerar um alarme a ser transmitido pelo sistema de comunicação, uma vez que o seu uso deve ser acompanhado de algum procedimento de resgate ou assistência ao operador. Por tratar-

se de um dispositivo fixo, instalado em local apropriado, amplamente divulgado, o mesmo poderá ser alimentado por rede elétrica. Ainda, por tratar-se de equipamento utilizado de forma esporádica, o mesmo poderá ser mantido em estado *sleep*, ativado pelo evento de uso;

- Dispositivo intermitente móvel gerador de alarmes: podem ser identificadores de operadores em plantas, dispositivos vestíveis que realizam coleta de dados fisiológicos e as emitem quando tem oportunidade de comunicação, equipamentos de rastreamento de ativos, todos com característica intermitente, não determinística ou periódica de comunicação. Neste caso, o baixo consumo de energia é imperativo, uma vez que são equipamentos móveis, com possibilidade de recarga de energia limitada.

5 RESULTADOS

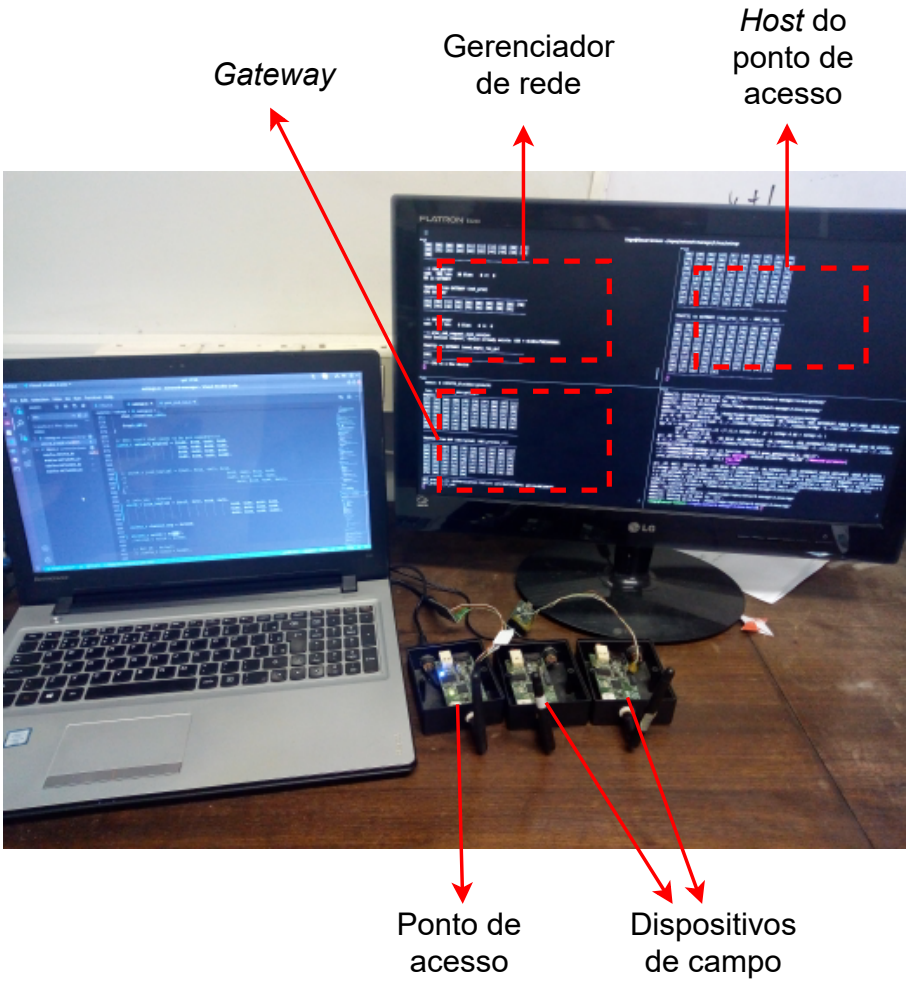
Neste capítulo são apresentados os resultados dos experimentos realizados juntamente com o detalhamento de seus projetos. As técnicas implementadas de coleta rápida de dados e *handover* foram desenvolvidas a partir de modificações realizadas em procedimentos de formação e manutenção de redes WH, porém estas modificações tornam a rede incompatível com padrão já que afetam requisitos como segurança e confiabilidade, além de demandarem modificações no comportamento do gerenciador de rede, não previstas na norma do protocolo.

5.1 Experimento 1 - Coleta rápida de dados

Tendo em vista avaliar o desempenho da técnica proposta, foi projetado e executado um experimento em redes reais para permitir o ingresso e envio de dados de dispositivos de forma rápida. O objetivo do experimento é verificar se há uma diferença significativa no tempo de publicação de uma variável dinâmica de dispositivos de campo quando comparados o método padrão com o método proposto de coleta rápida de dados. A bancada experimental utilizada inclui os seguintes equipamentos: três rádios, onde dois deles atuam como dispositivos de campo sendo um com o firmware padrão e outro com o firmware modificado para a técnica proposta e o terceiro rádio atuando como ponto de acesso; um computador para executar as aplicações do *gateway* (gerenciador de rede, *gateway* e o *host* do ponto de acesso); e um conversor USB-Serial para conectar o ponto de acesso físico ao seu *host* no computador. Estes equipamentos são apresentados na Figura 23.

Para identificar o tamanho amostral do experimento e evitar erros de amostragem, realizou-se um experimento preliminar para verificar valores médios de tempos e suas va-

Figura 23 – Bancada experimental.



Fonte: do autor

riações. O software estatístico Minitab conta com uma funcionalidade de assistência para cálculo do tamanho amostral, onde é preciso inserir informações sobre a variabilidade dos dados que inclui o desvio padrão e a diferença entre médias que se quer detectar. É preciso inserir também uma informação de potência estatística, que representa a probabilidade de o teste detectar uma diferença significativa quando ela realmente existe. As informações de variabilidade estão diretamente relacionadas com o tamanho amostral e por isso sua estimativa deve ser adequada. A determinação destes valores pode depender de conhecimento prévio, de estudos já realizados ou como neste caso, que apresenta uma proposta nova, através de um experimento preliminar.

Assim, considerando os valores definidos na Tabela 3, chegou-se a um tamanho amostral de 20. Ou seja, foram coletadas 20 amostras para cada caso avaliado (técnica padrão e técnica proposta).

Tabela 3 – Parâmetros para o cálculo do tamanho amostral.

Parâmetro	**Valor**
Número de níveis	2
Diferença entre médias [s]	4,5
Potência estatística	0,9
Desvio padrão [s]	4,2

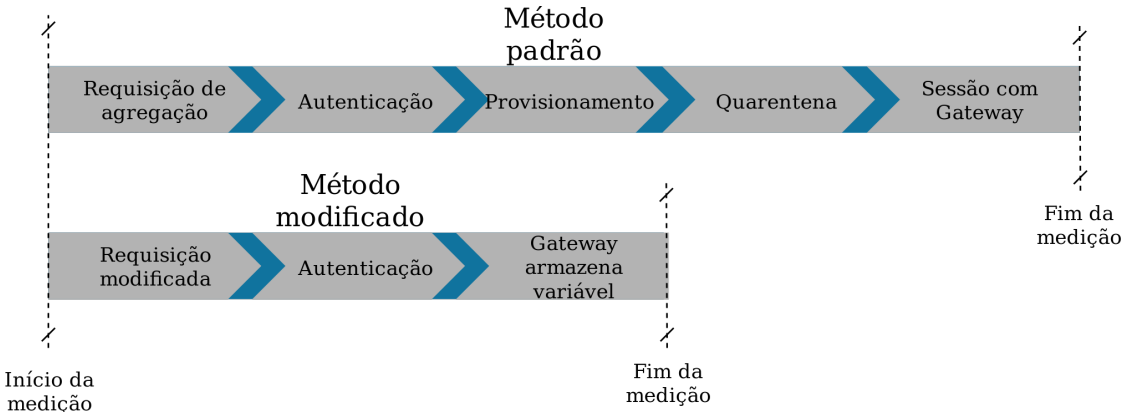
O experimento foi realizado seguindo instruções de metodologia experimental (MONTGOMERY, 2012), onde os seguintes passos foram executados para cada amostra:

- Sortear uma amostra. A amostra define qual técnica (padrão ou modificada) será usada na rede;
- Criar a rede e aguardar o início do serviço de divulgação da rede;
- Ativar o dispositivo escolhido e aguardar a publicação de sua variável dinâmica;
- Coletar o tempo de execução do processo.

A variável de resposta do experimento em questão é o tempo e as medidas foram coletadas utilizando estampas temporais, com precisão de milissegundos, nos registros de atividade do *gateway*. O período de tempo avaliado em cada caso inicia no mesmo instante, quando o dispositivo responde a um anúncio da rede enviando a requisição de agregação. Desta forma, o período de sincronização não é levado em consideração. O tempo dessa etapa inicial, entre a ativação do dispositivo e a sincronização, é variável e inclusive não é possível garantir que a sincronização será realizada. Já o fim da medição avaliada em cada caso é diferente, conforme apresentado na Figura 24. Em ambos os casos, foi avaliado o momento em que a variável dinâmica é disponibilizada no *gateway*. Para o método padrão isso ocorre após a criação da sessão com o *gateway*, já na técnica proposta, o fim da medição ocorre após a autenticação do dispositivo quando a sessão de agregação é criada, permitindo acesso aos dados que são armazenados no *gateway*.

Todas as amostras foram coletadas no mesmo dia. Os dispositivos foram posicionados próximos ao ponto de acesso sem nenhuma interferência física entre eles. Como fator

Figura 24 – Período de tempo avaliado em cada caso.



Fonte: do autor

não controlável, pode-se citar a coexistência com redes Wi-Fi presentes no local do experimento, além de sinais provenientes de outros protocolos de comunicação que utilizam a banda de 2,4 GHz. Para a análise dos dados foi utilizada assistência computacional do software estatístico Minitab onde foi realizada uma análise de variância (ANOVA - *Analysis of Variance*) com um nível de significância $\alpha = 0,05$ cujo resultado é apresentado na Tabela 4.

Tabela 4 – Análise de variância.

Fontes de variação	**Graus de liberdade**	**Soma dos quadrados**	**Média quadrática**	**Valor de F**	**Valor de P**
Técnica	1	635,387	635,387	23173,790	0,000
Erro	38	1,042	0,027	-	-
Total	39	636,429	-	-	-

Dado que o valor de P é menor que o nível de significância (α) é possível concluir com 95 % de confiança que a técnica afeta significativamente a variável de resposta (tempo). Os resultados médios para cada técnica são apresentados na Tabela 5. Os resultados revelam que a técnica proposta leva aproximadamente oito segundos a menos no tempo para publicar sua variável dinâmica no *gateway* quando comparado com a técnica padrão.

Tabela 5 – Resultados do experimento 1.

Técnica	**Tempo médio [s]**	**Desvio padrão [s]**
Padrão	9,998	0,224
Proposta	2,027	0,068

5.2 Experimento 2 - *Hard handover*

Os equipamentos utilizados neste experimento são os mesmos apresentados anteriormente na Figura 23 com adição de outro computador para executar a aplicação do coprocessador que é ligado ao dispositivo especial em sua porta de manutenção. Este experimento tem como objetivo avaliar qual o tempo necessário entre o dispositivo receber um comando de desconexão e enviar uma nova requisição de acesso para a rede. Este período representa o tempo que o dispositivo não se comunica com a rede e sua minimização representa melhor desempenho para a rede. Os dados foram coletados através de estampas temporais, mas desta vez em um terminal de depuração do dispositivo. Para isso, foram realizadas modificações no firmware do dispositivo para que o mesmo sinalize os eventos de interesse em sua porta de comunicação serial.

Para a coleta de cada amostra foram realizados os seguintes passos:

- Inicializar a rede;
- Conectar um nodo, que passa também a propagar anúncios;
- Conectar o nodo especial;
- Desconectar do nodo especial (pelo comando 960);
- Aguardar nova requisição de acesso a rede;
- Coletar o tempo.

Há muitas variáveis que influenciam no tempo necessário para a primeira etapa do processo de agregação até o envio da requisição de agregação, como a taxa de anúncios, o número de dispositivos conectados e também características definidas internamente no dispositivo. O ponto de acesso foi configurado para propagar anúncios a cada 500 ms,

mas ainda assim é preciso considerar que está é uma tarefa de baixa prioridade além do tempo necessário para seu agendamento. Para a configuração utilizada, tem-se um link de agregação configurado para um superframe de 127 slots. Neste experimento testou-se também o impacto de uma variável interna que define o número de anúncios que o dispositivo precisa receber antes de enviar a requisição, aqui essa variável é representada por MIN_ADS. Por padrão esta variável tem valor três o que permite por exemplo, que diante dos anúncios recebidos o dispositivo tenha opções para escolher a mais adequada e também notificar o gerenciador de rede sobre vizinhos identificados. Os testes também incluem a variável MIN_ADS com valor um, visto que para um dispositivo móvel especial a informação coletada de outros dispositivos não é relevante, uma vez que o dispositivo móvel não irá se comportar na rede como um roteador de pacotes.

Para ambos os casos testados, foram recolhidas 20 amostras e as médias dos resultados são apresentadas na Tabela 6.

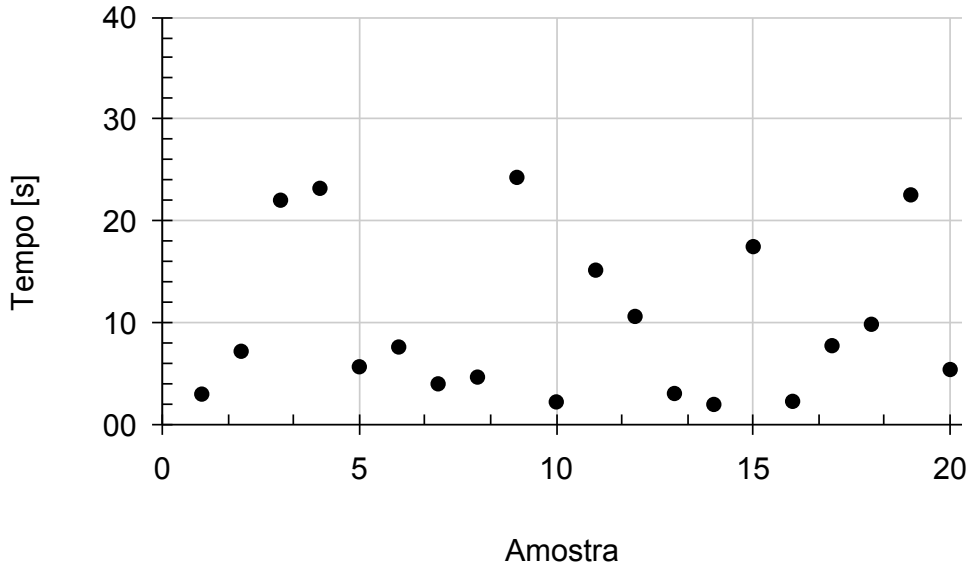
Tabela 6 – Resultados do experimento 2.

MIN_ADS	**Tempo médio [s]**	**Desvio padrão [s]**
1	10,000	7,840
3	32,778	1,741

Analisando-se os valores médios nota-se que, de fato, a variável MIN_ADS é responsável por representar grande parte do tempo avaliado. Considerando que este é um dispositivo móvel e que precise realizar a tarefa de forma mais rápida possível, a opção de MIN_ADS = 1 seria a mais adequada. Os dados coletados também mostram uma grande diferença no desvio padrão, esta variação nos dados é mais perceptível quando avaliamos os gráficos de dispersão de cada caso, que são apresentados nas figuras 25 e 26.

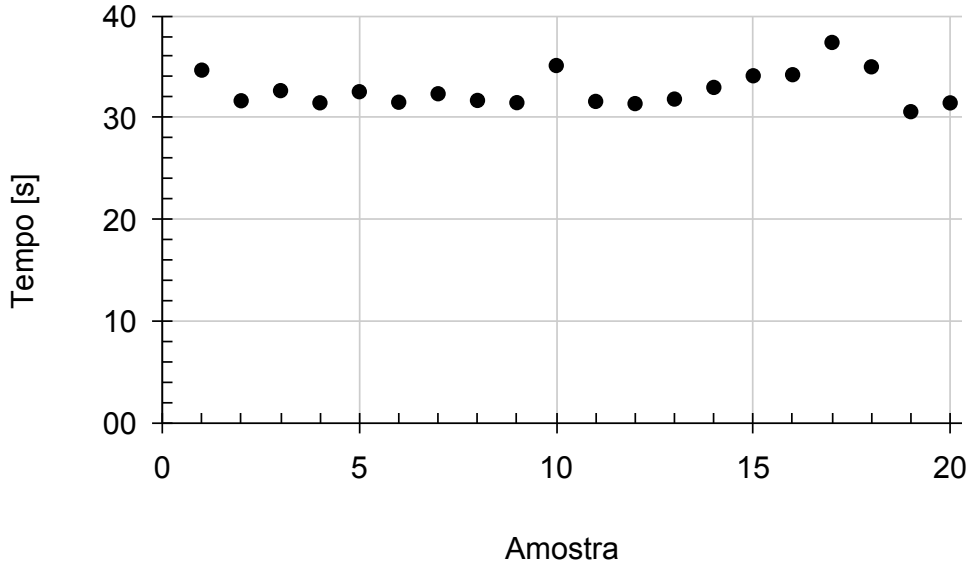
Com o gráfico apresentado na Figura 25 nota-se uma grande variação em torno do valor médio que é um reflexo da característica probabilística do processo de busca por anúncios. Esta tarefa é realizada de forma sequencial pelos canais de comunicação (do canal 11 ao 25), onde o dispositivo escuta o canal por um período de tempo em busca de comunicações e troca para o próximo se nada for encontrado. Como o dispositivo está ingressando na rede, ele não tem informações sobre a forma como os dispositivos

Figura 25 – Gráfico de dispersão para MIN_ADS = 1.



Fonte: do autor

Figura 26 – Gráfico de dispersão para MIN_ADS = 3.



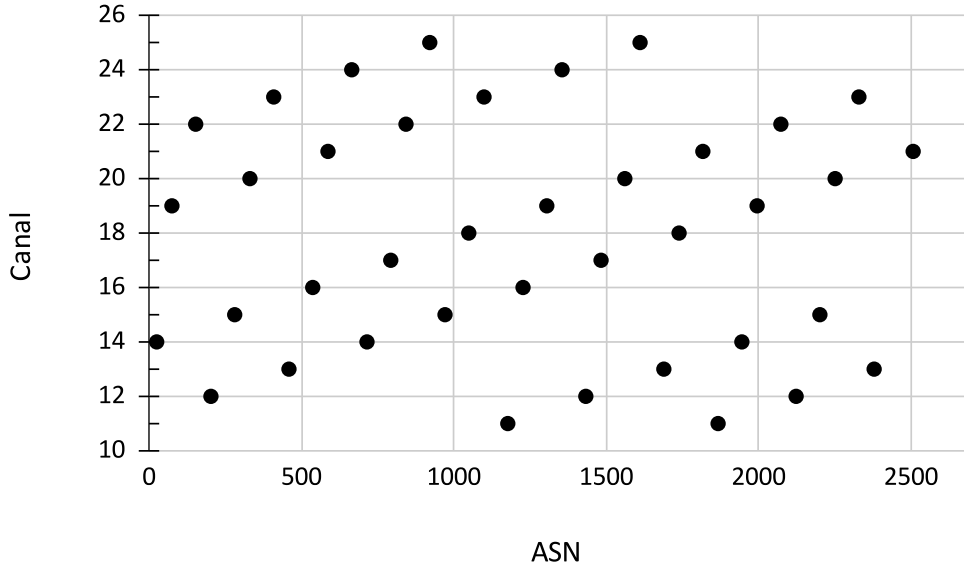
Fonte: do autor

anunciantes estão enviando suas mensagens na rede. Por uma questão de segurança o canal de comunicação só é definido no momento da comunicação e depende de fatores como lista de canais disponíveis, tempo atual da rede e o *offset* de canal que é uma variável

definida na criação dos links pelo gerenciador de rede.

Como exemplo, apresenta-se a forma como o ponto de acesso utilizado realiza a divulgação da rede através da propagação de pacotes de anúncio. Toda vez que o temporizador responsável pela tarefa de divulgação sinalizar o fim da contagem, um pacote de anúncio é gerado e enviado no primeiro link de transmissão disponível que não seja compartilhado. De forma geral, todas as outras comunicações da rede tem prioridade no agendamento de links. Neste caso o dispositivo apresenta dois links de transmissão não compartilhados em seu superframe, que tem tamanho 127 slots, sendo um no slot 20 e outro no 70. Assim, o dispositivo tem capacidade de enviar dois pacotes de anúncio por superframe. O canal escolhido para a comunicação depende das seguintes variáveis: ASN, *offset* do canal e mapa de canais. A Figura 27 apresenta as primeiras possibilidades de envio de pacotes de anúncio considerando um ASN inicial de valor zero. Desta forma, a partir das informações utilizadas no ponto de acesso, é possível garantir que todos os canais de comunicação estão disponíveis para utilização.

Figura 27 – Representação dos possíveis canais de comunicação para envio de pacotes de anúncio disponíveis no ponto de acesso.



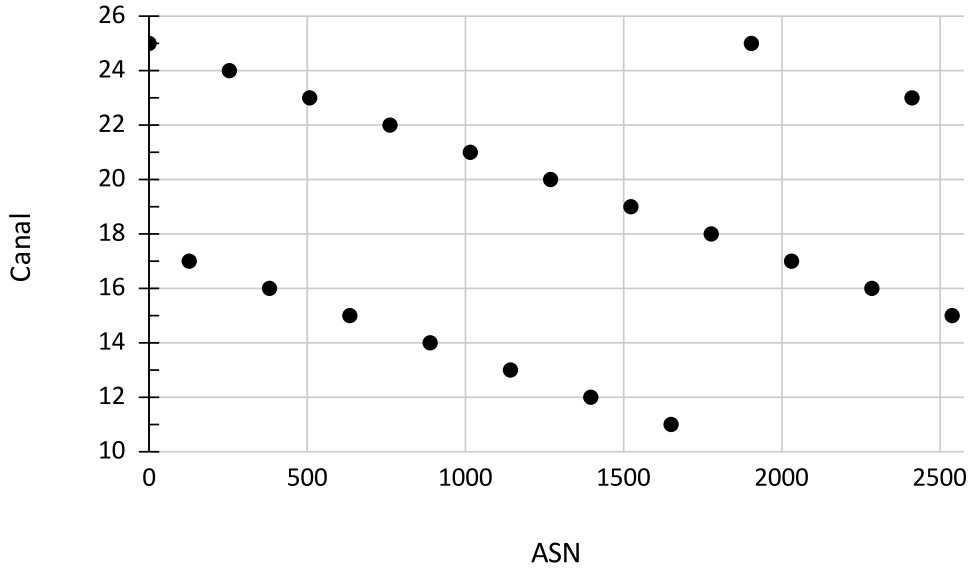
Fonte: do autor

Como o ponto de acesso foi configurado para enviar pacotes de anúncio com um intervalo de 500 ms e cada superframe possui 127 slots com tempo fixo de 10 ms cada, tem-se uma utilização dentro da capacidade de transmissão do dispositivo, já que se tem

uma transmissão de anúncio a aproximadamente cada quatro repetições do superframe.

Com o auxílio do *sniffer*, coletou-se amostras de anúncios propagados pelo ponto de acesso que são apresentadas na Figura 28. Neste caso, nota-se a influência da definição do intervalo de propagação de anúncios, que está em 500 ms, e também verifica-se a diversidade de canais. Vale salientar que neste experimento apenas o ponto de acesso faz parte da rede e nenhuma outra comunicação de maior prioridade que o anúncio está sendo transmitida.

Figura 28 – Canais utilizados na propagação de anúncios.



Fonte: do autor

6 CONCLUSÕES

As aplicações de RSSF abrangem diversas áreas incluindo o setor industrial onde são empregadas principalmente para uso em controle e monitoramento de processos. Estas redes apresentam uma alternativa para os sistemas cabeados trazendo vantagens como facilidade de instalação, facilidade em realizar modificações na rede (adição ou reorganização de nodos) e redução de custo. Atualmente, os principais protocolos de comunicação destinados para RSSFI apresentam em seus projetos diversas características para superar desafios de implementação como consumo eficiente de energia, interferências, segurança e gerenciamento de dados. Devido à grande aplicabilidade destas redes, encontram-se estudos em diversos domínios que buscam avaliar desempenhos, propor melhorias ou novos procedimentos.

Este trabalho apresenta um estudo que trás como tema a presença de mobilidade de nodos em RSSFI. Esta característica aumenta a dinamicidade da rede e exige mecanismos de gerenciamento adequados para manter estes nodos funcionais e evitar problemas como: aumento na taxa de perda de pacotes que podem ocorrer devido à degradação na qualidade dos enlaces de comunicação; elevação de atrasos em comunicações decorrentes da frequente necessidade de busca por novas rotas; ou também o aumento no consumo de energia que acaba sendo um reflexo do processo como um todo devido a retransmissões e novas comunicações. Protocolos como o WH, que foi utilizado como base de estudo neste trabalho, apresentam apenas suporte para situações de baixa mobilidade que alteram a topologia de rede mas em uma baixa frequência como o caso da inserção de um novo dispositivo ou a perda da capacidade de transmissão devido a uma interferência ou falha no dispositivo. Já para aplicações onde os nodos da rede apresentam alta mobilidade, tem-se uma frequente mudança de topologia de rede a qual não se tem suporte no protocolo WH. A alta mobilidade está relacionada a movimentação física do nodo pela

área de cobertura da rede, seja por ação do meio ao qual ele está inserido ou ainda por movimentação própria ou da pessoa ou equipamento que ele possa estar fixado.

As técnicas propostas neste trabalho atuam em dois momentos distintos de operação de dispositivos móveis. Um focado na etapa de agregação de dispositivos, voltado para dispositivos que participam da rede de forma intermitente e que precisam realizar suas funções na rede de forma rápida e outro momento focado na manutenção da conectividade de dispositivos que se movem sobre a área de cobertura da rede.

Inicialmente propôs-se uma técnica para coleta rápida de dados cujo objetivo é tornar disponível uma variável dinâmica de um dispositivo no *gateway* de forma mais rápida que o processo padrão. Esta técnica busca atender a dispositivos que apresentam restrições de tempo sobre o alcance da rede. O método proposto aplica modificações tanto na forma como o dispositivo faz a sua requisição de agregação quanto no *gateway* que deve ser capaz também de identificar este pedido especial. A modificação inicia após a sincronização do dispositivo com a rede que é o momento de envio da requisição de acesso. Junto a esta mensagem já é enviada uma variável dinâmica que, após uma verificação de segurança de acesso realizada pelo gerenciador de rede, é armazenada no *gateway* que é por onde redes externas tenham acesso a informações da RSSFI. Uma vez que as modificações alteram o protocolo padrão, tem-se uma consequente alteração na segurança. A mensagem que contém a variável dinâmica que era antes encriptada com uma chave secreta, agora utiliza a chave de agregação que representa um nível inicial de segurança. Neste caso projetou-se um experimento para avaliar os resultados comparando o método proposto com o padrão WH. Os resultados do experimento mostram que a técnica proposta é em média cinco vezes mais rápida que o procedimento padrão. Esta diferença poderia ser ainda maior visto que o período final de medição do método padrão não considera a etapa já do serviço de publicação onde é preciso alocar recursos de comunicação para então efetivamente enviar a variável. Enquanto que no método proposto são utilizados os links de agregação para este propósito.

Outra abordagem apresentada neste trabalho trata da manutenção de conectividade em dispositivos que se movem pela área de cobertura da rede. Neste caso propõe-se modificações no gerenciamento de dispositivos onde o próprio dispositivo tem a capacidade de monitorar as suas conexões e de tomar decisões, caracterizando-se assim como uma técnica de *handover*. Para isso, utilizou-se de uma ferramenta externa, chamada de

coprocessador, conectada a um dispositivo para realizar o gerenciamento local. O método utilizado inclui o monitoramento da qualidade de enlace com dispositivos vizinhos através de um *script* de programação que envia comandos periódicos para o dispositivo e compara as respostas em um controle por histerese que é responsável pela decisão de encontrar ou não uma nova rota para o dispositivo. Desta forma, quebra-se a principal barreira que impede a utilização de dispositivos móveis em rede WH que é o serviço de descobrimento de vizinhos que não é adequado para situações de alta amobilidade devido aos mecanismos utilizados e grandes latências associadas ao processo, que em um primeiro momento tratam a mudança no posicionamento do dispositivo com uma falha de comunicação. Realizou-se um experimento que visa avaliar o tempo em uma das etapas do processo e também analisar uma variável que pode afetar neste tempo de forma direta. Os dados coletados mostram os valores médios encontrados mas também revelam uma grande aleatoriedade na etapa de sincronização e busca por anúncios do processo de agregação que é resultado do mecanismo probabilístico implementado.

Para atingir os objetivos desejados, tanto o dispositivo decampo quanto o gerenciador de rede WH foram largamente modificados para adequar a demanda do dispositivo móvel, de tal forma a incompatibilizar com o padrão WH. Ainda,é necessário o uso de processos paralelos ao funcionamento convencional do dispositivo de campo, na forma de gerenciador de rede descentralizado. Os resultados obtidos revelaram a viabilidade da proposta, tendo como pontos positivos a possibilidade de atender aplicações industriais de alta dinamicidade, tais como o uso de nodos acoplados em AGV (Automated Guided Vehicles), sensores vestíveis para monitoramento de sinais fisiológicos de operadores da planta ou nodos intermitentes geradores de alarmes em situações de alto risco. Como pontos negativos, são percebidos comprometimentos em segurança e consumo de energia, que não atendem mais os requisitos da rede WH original, utilizada como ferramenta para implementação deste trabalho.

O estudo realizado neste trabalho permitiu compreender em detalhes a forma como procedimentos padrões em RSSFI são executados uma vez que os materiais utilizados permitem acesso aos seus códigos fonte. Desta forma, através de análise do comportamento da rede e de suas técnicas de gerenciamento foi possível encontrar os principais fatores que afetam de forma negativa no desempenho da rede quando adicionados dispositivos móveis, e atuar de forma a propor soluções mais adequadas para estas aplicações.

Ambas as técnicas apresentadas não resolvem de forma completa os problemas resultantes da presença de alta mobilidade em RSSFI, mas já fornecem soluções iniciais cujos resultados apresentam evolução para um suporte adequado à mobilidade.

Como trabalhos futuros, podem-se citar a modificação das delimitações utilizadas no trabalho atual bem como o estudo de fatores limitadores encontrados com objetivo de ampliar a abrangência das aplicações em busca de uma solução ideal. Isso inclui, por exemplo:

- Ampliar a densidade de nodos nas redes de teste. Desta forma é possível avaliar também a interação com nodos vizinhos em um cenário de maior ocupação de recursos de comunicação.

- Diferenciar dispositivos móveis de estáticos para que se possa otimizar o desempenho em cada caso, visto que suas características de operação apresentam muitas diferenças.

- Explorar o serviço de publicação e sua relação com novos dispositivos em etapa de sincronização e busca nos canais de comunicação. Como relatado, esta etapa da agregação apresenta um período de execução aleatório e que influencia de forma direta no tempo de agregação.

- Modelar o sistema para que se tenha definições claras de aplicações e formas de operação e movimento que podem ser abrangidas pelas técnicas propostas.

REFERÊNCIAS

ALI, M.; SULEMAN, T.; UZMI, Z. A. MMAC: a mobility-adaptive, collision-free mac protocol for wireless sensor networks. *In*: INTERNATIONAL PERFORMANCE, COMPUTING, AND COMMUNICATIONS CONFERENCE, 2005, Phoenix, USA. **Proceedings [...]** IEEE, 2005. p. 401–407.

BHUVANESWARI, A. Survey on handoff techniques. **Journal of Global Research in Computer Science**, [S.l.], v. 2, n. 6, p. 140–144, June 2011.

CAINELLI, G. *et al.* Development of a Network Manager Compatible with WirelessHART Standard. *In*: CONGRESSO BRASILEIRO DE AUTOMÁTICA, 2020. **Anais [...]** SBA, 2020. v. 2, n. 1.

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

DONG, Q.; DARGIE, W. A survey on mobility and mobility-aware MAC protocols in wireless sensor networks. **IEEE Communications Surveys & Tutorials**, [S.l.], v. 15, n. 1, p. 88–100, Feb. 2012.

GUNGOR, V. C.; HANCKE, G. P. Industrial wireless sensor networks: challenges, design principles, and technical approaches. **IEEE Transactions on Industrial Electronics**, [S.l.], v. 56, n. 10, p. 4258–4265, Oct. 2009.

HCF. **TDMA Data Link Layer Specification**. Austin, USA: HART Communication Foundation, 2008. n. HCF_SPEC-075.

HCF. **Network Management Specification**. Austin, USA: HART Communication Foundation, 2009. n. HCF_SPEC-085.

HOWITT, I. *et al.* Wireless industrial sensor networks: framework for QoS assessment and QoS management. **ISA Transactions**, [S.l.], v. 45, n. 3, p. 347–359, Jan. 2006.

KARL, H.; WILLIG, A. **Protocols and architectures for wireless sensor networks**. England: John Wiley & Sons, 2007. 497 p.

LI, X. *et al.* A review of industrial wireless networks in the context of industry 4.0. **Wireless Networks**, [S.l.], v. 23, n. 1, p. 23–41, Nov. 2017.

MA, J. *et al.* A reliable handoff mechanism for mobile industrial wireless sensor networks. **Sensors**, [S.l.], v. 17, n. 8, p. 1797, Aug. 2017.

MONTERO, S.; GOZALVEZ, J.; SEPULCRE, M. Neighbor discovery for industrial wireless sensor networks with mobile nodes. **Computer Communications**, [S.l.], v. 111, p. 41–55, Oct. 2017.

MONTERO, S. *et al.* Impact of mobility on the management and performance of WirelessHART industrial communications. *In*: INTERNATIONAL CONFERENCE ON EMERGING TECHNOLOGIES & FACTORY AUTOMATION, 2012, Krakow, Poland. **Proceedings [...]** IEEE, 2012. p. 1–4.

MONTGOMERY, D. C. **Design and analysis of experiments**. 8th. ed. [S.l.]: John Wiley & Sons, 2012. 730 p.

MÜLLER, I. **Gerenciamento descentralizado de redes sem fio industriais segundo o padrão WirelessHART**. 2012. 105 p. Tese (Doutorado em engenharia) — Programa de Pós-Graduação em Engenharia Mecânica e Materiais, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2012.

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

MÜLLER, I. *et al.* WirelessHART fast collect: a decentralized approach for intermittent field devices. *In*: INTERNATIONAL CONFERENCE ON INDUSTRIAL INFORMATICS, 2013, Bochum, Germany. **Proceedings [...]** IEEE, 2013. p. 254–259.

MÜLLER, I. *et al.* Energy consumption estimation for TDMA-based industrial wireless sensor networks. *In*: INTERNATIONAL CONFERENCE ON INDUSTRIAL INFORMATICS, 2016, Poitiers, France. **Proceedings [...]** IEEE, 2016. p. 625–630.

NXP. **MC1322x datasheet**. Disponível em: <https://www.nxp.com/docs/en/data-sheet/MC1322x.pdf>. Acessado: 31 jan. 2020.

RAMSON, S. J.; MONI, D. J. Applications of wireless sensor networks—A survey. *In*: INTERNATIONAL CONFERENCE ON INNOVATIONS IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND MEDIA TECHNOLOGY, 2017, Coimbatore, India. **Proceedings [...]** IEEE, 2017. p. 325–329.

THAKUR, P.; GANPATI, A. Survey on handover techniques in VANET. **International Journal of Computer Sciences and Engineering**, [S.l.], v. 7, n. 6, p. 236–250, June 2019.

VAN, D. D.; AI, Q.; LIU, Q. Vertical handover algorithm for WBANs in ubiquitous healthcare with quality of service guarantees. **Information**, [S.l.], v. 8, n. 1, p. 34, Mar. 2017.

WEI, L. *et al.* A fast neighbor discovery algorithm in WSNs. **Sensors**, [S.l.], v. 18, n. 10, p. 3319, Oct. 2018.

YANG, S.-H. **Wireless Sensor Networks**. London: Springer, 2014. 293 p.

ZAND, P. *et al.* Wireless industrial monitoring and control networks: the journey so far and the road ahead. **Journal of Sensor and Actuator Networks**, [S.l.], v. 1, n. 2, p. 123–152, Aug. 2012.

ZAREEI, M. *et al.* Mobility-aware medium access control protocols for wireless sensor networks: a survey. **Journal of Network and Computer Applications**, [S.l.], v. 104, p. 21–37, Feb. 2018.

ZINONOS, Z.; VASSILIOU, V. Handoff algorithms for industrial mobile wireless sensor networks. *In*: INTERNATIONAL CONFERENCE ON NEW TECHNOLOGIES, MOBILITY AND SECURITY, 2014, Dubai, United Arab Emirates. **Proceedings [...]** IEEE, 2014. p. 1–6.