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

ALEXANDRE DE ANDRADE LORENÇATO

ANALISADOR DE REDES WIRELESSHART

Porto Alegre
2013

ALEXANDRE DE ANDRADE LORENÇATO

ANALISADOR DE REDES WIRELESSHART

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. Carlos Eduardo Pereira

Porto Alegre
2013

ALEXANDRE DE ANDRADE LORENÇATO

ANALISADOR DE REDES WIRELESSHART

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. Carlos Eduardo Pereira, UFRGS
Doutor pela Universität Stuttgart, Alemanha

Banca Examinadora:

Prof. Dr. Leandro Buss Becker, UFSC
Doutor pela Universidade Federal do Rio Grande do Sul, Brasil

Prof. Dr. João César Netto, UFRGS
Doutor pela Universite Catholique de Louvain, Bélgica

Prof. Dr. Valner João Brusamarello, UFRGS
Doutor pela Universidade Federal de Santa Catarina, Brasil

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

Porto Alegre, Junho de 2013.

AGRADECIMENTOS

Ao professor Carlos Eduardo Pereira, pela oportunidade de trabalho, disponibilidade e auxílio nos momentos de maior dificuldade do trabalho.

Aos colegas de laboratório Jean Michel Winter, Ivan Müller, Gustavo Kunzel e ao professor João César Netto, pela troca de informações e dicas de implementação nas atividades desenvolvidas no mestrado.

À direção da CP Eletrônica, hoje adquirida pelo grupo Schneider-Electric, pela liberação de horário de estudo que proporcionaram a utilização dos equipamentos disponibilizados pelo Laboratório de Sistemas de Controle, Automação e Robótica (LASCAR).

Aos meus amigos e familiares que me apoiaram e incentivaram durante esta jornada.

Faço um agradecimento especial aos meus pais Pedro e Alice, ao meu filho Mateus e minha esposa Carolina pela atenção, carinho e incentivo incondicional para a conclusão de mais essa etapa.

RESUMO

A segurança da informação, a diversidade de rotas entre os dispositivos da rede, o acesso ao meio de modo determinístico e isento de colisões e a mudança de canal frequente tornam a comunicação no protocolo *Wireless*HART robusta e confiável para utilização em meio industrial. Entretanto, para adoção crescente dessa tecnologia, é necessário que os fabricantes de sensores e atuadores industriais desenvolvam dispositivos *Wireless*HART. Disto surge a necessidade de criação de ferramentas capazes de auxiliar o desenvolvimento e depuração destes novos dispositivos de rede. O Analisador de rede *Wireless*HART é, sem dúvida, uma delas. Diversas abordagens são propostas para a análise de redes *Wireless*HART. Entretanto, em todas elas a utilização de um microcomputador como elemento do sistema inviabiliza sua utilização em campo. A presença de cabos, armazenamento local dos dados e exigência de baterias são alguns dos aspectos relevantes que devem ser levados em consideração quando o sistema precisa ser utilizado em campo. O presente trabalho propõe alternativas aos sistemas de análise de redes atuais apresentando duas propostas conceitualmente diferentes mas que cumprem os requisitos básicos para sua utilização em campo. Uma destas abordagens, baseada na proposta de integração entre um dispositivo de campo e o método inovador de captura de mensagens utilizando apenas um transceptor, é implementado como prova do conceito.

Palavras-chave: Redes sem fio, WirelessHART, IEEE 802.15.4, analisador de redes.

ABSTRACT

*Wireless*HART is a robust and reliable protocol for industrial environment usage because of its secure mechanism, the ability of programming several communication routes between network devices, and deterministic, free of collisions channel hopping medium access controller. However, in order to increase the adoption of this technology, it is necessary to increase the amount of *Wireless*HART manufacturers to develop industrial sensors and actuators devices. This leads to the necessity of create tools that will assist the development and debugging of new network compliant devices. The *Wireless*HART network analyzer is undoubtedly one of these tools. Various approaches are being proposed for the analysis of *Wireless*HART networks. However, all of them make use of a microcomputer as an element of the whole system and this difficults their use in real field applications. The presence of wires, lack of local data storage and other aspects such as batteries limitations must be considered when the users intend to use analysis systems in field. This work proposes alternatives to current analysis networks systems by presenting two conceptually different proposals that meet the basic requirements for the use in the field. One of them is based on the proposed integration between a field device and an innovative method of capturing messages using only one transceiver, which is implemented as proof of concept.

Keywords: *Wireless*HART, Industrial wireless sensor network, IEEE 802.15.4, wireless network analyzer.

SUMÁRIO

LISTA DE ILUSTRAÇÕES 8

LISTA DE TABELAS 10

LISTA DE ABREVIATURAS 11

1 INTRODUÇÃO 12
1.1 Objetivos 15
1.2 Organização da dissertação 15

2 FUNDAMENTAÇÃO TEÓRICA 17
2.1 O Padrão IEEE 802.15.4 17
2.2 O Protocolo *Wireless*HART 22
2.2.1 Camada física 25
2.2.2 Camada de enlace de dados 26
2.2.3 Camada de rede 30
2.2.4 Camada de transporte 32
2.2.5 Camada de aplicação 33
2.3 O Protocolo HART-IP 34
2.4 Síntese do capítulo 36

3 ANÁLISE DO ESTADO DA ARTE 37
3.1 Revisão bibliográfica 37
3.1.1 Wi-Analys 37
3.1.2 Analisador de 16 canais 39
3.1.3 Analisador IEEE 802.15.4 monocanal 41
3.1.4 Z-Monitor 42
3.1.5 Analisador WH distribuído 44
3.2 Análise comparativa dos trabalhos mais relevantes 45
3.3 Síntese do capítulo 48

4 O ANALISADOR DE REDES *WIRELESS*HART 50
4.1 Desafios e limitações na análise de redes *Wireless*HART 50
4.2 Arquitetura do analisador de rede proposto 52
4.3 Unidade coletora de dados 56
4.3.1 Coletor de dados monocanal 58
4.3.2 Coletor de dados multicanal 61
4.4 Unidade analisadora de dados 64
4.5 Análise comparativa entre as abordagens propostas 66

4.6 Síntese do capítulo 67

5 IMPLEMENTAÇÃO E RESULTADOS 69
5.1 Implementação do coletor monocanal 69
5.1.1 Hardware da unidade coletora de dados monocanal 70
5.1.2 O Firmware da unidade coletora de dados monocanal 71
5.1.3 O Gerenciador da unidade coletora de dados monocanal 78
5.2 Implementação do coletor de dados multicanal 82
5.3 Resultados experimentais 89
5.4 Síntese do capítulo 99

6 CONCLUSÕES E TRABALHOS FUTUROS 100

REFERÊNCIAS 104

LISTA DE ILUSTRAÇÕES

Figura 1: Topologia estrela e ponto a ponto (IEEE, 2006) 19
Figura 2: PPDU definido pelo padrão 802.15.4 (IEEE, 2006) 21
Figura 3: Rede *Wireless*HART típica (CHEN; NIXON; MOK, 2010) 23
Figura 4: Modelo OSI do protocolo *Wireless*HART (CHEN; NIXON; MOK, 2010) 25
Figura 5: *Timeslot Wireless*HART (HCF SPEC-075 Rev. 1.1) 27
Figura 6: *Superframe Wireless*HART (HCF SPEC-075 Rev. 1.1) 28
Figura 7: Saltos de frequência no protocolo *Wireless*HART (HCF SPEC-075 Rev. 1.1) 29
Figura 8: DLPDU do protocolo *Wireless*HART (HCF SPEC-075 Rev. 1.1) . . . 30
Figura 9: NPDU do protocolo *Wireless*HART (HCF SPEC-085 Rev. 1.2) . . . 32
Figura 10: TPDU do protocolo *Wireless*HART (HCF SPEC-085 Rev. 1.2) 33
Figura 11: Dispositivos HART-IP (HCF SPEC-085 Rev. 2.0) 35
Figura 12: Analisador de redes *Wireless*HART Wi-Analys 38
Figura 13: Analisador proposto por (KRATZIG et al., 2009) 40
Figura 14: Analisador proposto por (MRAZ et al., 2011) 41
Figura 15: Analisador proposto por (KOUBAA et al., 2011) 43
Figura 16: Analisador proposto por (FERRARI et al., 2009) 44
Figura 17: *Probes* coletoras proposta por (FERRARI et al., 2009) 45
Figura 18: Entidades elementares em um analisador de redes 53
Figura 19: Etapas propostas na coleta de dados 54
Figura 20: Rede com múltiplas unidades coletoras 55
Figura 21: Coletor de dados monocanal integrado a uma rede *Wireless*HART . . 59
Figura 22: Elementos do coletor de dados multicanal 63
Figura 23: Etapas do processo de análise proposto por (KUNZEL, 2012) 66
Figura 24: Hardware do namimote (MULLER et al., 2012) 70
Figura 25: Tarefas concorrentes do *firmware* da unidade coletora 72
Figura 26: Pontos de captura de mensagens *Wireless*HART 73
Figura 27: Fluxogramas do produtor e consumidor implementado 77
Figura 28: Gateway *Wireless*HART 1420A 79
Figura 29: Fluxograma implementado do gerenciador da unidade coletora monocanal 80
Figura 30: Sequência de comandos executados pelo gerenciador da unidade coletora monocanal 83
Figura 31: Projeto de hardware do rádio coletor 85
Figura 32: Diagrama de blocos da placa base do coletor multicanal 85
Figura 33: Placas da unidade coletora de dados multicanal 88

Figura 34: Equipamentos utilizados nos ensaios 90
Figura 35: Detecção de dispositivos na rede e vizinhos da unidade coletora . . . 91
Figura 36: Leitura de *superframes* e *links* na vizinhança da unidade coletora . . . 92
Figura 37: Leitura de *superframes*, *links* e processos de manutenção da unidade coletora 93
Figura 38: Resultado do ensaio de ajuste temporal 94
Figura 39: Estrutura do arquivo de integração 96
Figura 40: Rede formada durante o ensaio 97
Figura 41: Informações dos dispositivos obtidos através da ferramenta de análise 98
Figura 42: Estrutura dos *superframes* obtidos pela ferramenta de análise 98

LISTA DE TABELAS

Tabela 1: PHYs definidas no padrão IEEE 802.15.4 20
Tabela 2: Canais utilizados no protocolo *Wireless*HART 26
Tabela 3: Comparação entre os trabalhos analisados 48
Tabela 4: Ajuste temporal entre dispositivos de campo e o ponto de acesso . . . 95

LISTA DE ABREVIATURAS

ACK	*Acknowledgment*
ASN	*Absolute Slot Number*
CSMA-CA	*Carrier Sense Multiple Access with Collision Avoidance*
FFD	*Full-Function Device*
FPGA	*Field-Programmable Gate Array*
GPS	*Global Positioning System*
HCF	*HART Communication Foundation*
IEEE	*Institute of Electrical and Electronics Engineers*
ISM	*Industrial, Scientifical e Medical*
ITU-T	*International Telecommunication Union-Telecommunication Standardization Sector*
LR-WPAN	*Low-Rate Wireless Personal Area Network*
MAC	*Medium Access Control*
MIC	*Message Integrity Code*
NPDU	*Network Protocol Data Unit*
PAN	*Personal Area Network*
PHY	*Physical Layer*
RFD	*Reduced-Dunction Device*
TDMA	*Time Division Multiple Access*
TPDU	*Transport Layer Packet*
TTL	*Time to Live*
WPAN	*Wireless Personal Area Network*
WH	*Wireless*HART

1 INTRODUÇÃO

Aspectos como facilidade de manutenção, rapidez na detecção de falhas, escalabilidade da solução e custos operacionais associadas à implementação e sua posterior manutenção são frequentemente levados em consideração na escolha de novos sistemas de automação para a indústria.

Nos sistemas tradicionais, onde a interligação entre sensores, atuadores e controladores é feita por par trançado, o custo da instalação de novos dispositivos aumenta consideravelmente quando as distâncias aumentam. A utilização de cabos também não é recomendada em ambientes com alta umidade, presença de campos magnéticos fortes, de difícil acesso aos sensores e/ou atuadores, com vibrações intensas ou que dependam de mobilidade dos dispositivos. Nestes casos, o uso de soluções sem fio se torna mais atrativa do que as soluções cabeadas existentes (LOW; WIN; ER, 2005).

As redes de sensores sem fio são sistemas em que cada nó sensor pertencente a rede utiliza rádio frequência para se comunicar com sua vizinhança, detectar mudanças no meio ao qual estão inseridas e transmitir as informações coletadas aos demais sensores da rede. Devido à natureza colaborativa destas redes, a topologia da rede vai sendo automaticamente formada através do conhecimento da vizinhança de cada um dos nós sensores. A partir da percepção do entorno, estes sensores também são capazes de perceber modificações no meio e superar eventuais falhas mantendo a rede funcional (AKYILDIZ et al., 2002).

A perda de dados causada pela falha de algum nó sensor pode ser considerada normal para a maioria dos sistemas de rede. Contudo, em aplicações industriais, tais falhas são

inaceitáveis. Dispositivos sem fio para utilização em ambientes industriais devem ser projetados para funcionamento sem interrupção por diversos anos, especialmente quando utilizados em processos automatizados contínuos (GUTIERREZ et al., 2010).

Neste contexto, a utilização de redes de sensores sem fio em aplicações industriais deve prever mecanismos para garantir confiabilidade na comunicação dos dados e robustez para manutenção da rede ativa mesmo quando implementada em ambientes fabris onde são significativos os efeitos da reflexão/absorção dos sinais de rádio frequência, das interferências causadas por outras redes sem fio e ou ainda pelo ruído gerado pelos equipamentos industriais (LOW; WIN; ER, 2005), (GUNGOR; HANCKE, 2009).

Com o objetivo de atender esta nova demanda, muitos protocolos de comunicação industrial tem sido desenvolvidos. As especificações dos protocolos ISA100.11a, ZigBee PRO e *Wireless*HART(WH) são apenas alguns exemplos nesse sentido (RADMAND et al., 2010). Apesar das diferenças conceituais na implementação destes protocolos de comunicação, o padrão IEEE 802.15.4 tem sido utilizado constantemente como base destas novas propostas para uso industrial.

O padrão IEEE 802.15.4 é um protocolo de comunicação sem fio que compreende uma faixa muito específica de dispositivos de comunicação. Sua padronização foi voltada para redes com baixa taxa de transferência de dados, curto alcance, baixa complexidade de hardware e consumo de energia limitado. Entretanto, por não garantir o cumprimento de requisitos temporários severos exigidos pelos processos fabris, seu uso não pode ser diretamente empregado em aplicações industriais (YOO et al., 2010).

O protocolo de comunicação WH surgiu para eliminar esta restrição. Desenvolvido sobre a camada física do padrão IEEE 802.15.4, ele redefiniu o mecanismo de acesso ao meio tornando-o determinístico. Especificou mecanismos de retransmissão de mensagens e utilizou saltos de frequência a cada comunicação. A diversidade de rotas foi prevista através da utilização de uma rede em malha. A segurança da informação também foi coberta no padrão permitindo autenticação, integridade e criptografia utilizando algoritmos estabelecidos.

Com o surgimento deste novo protocolo de comunicação, tornou-se necessário o de-

senvolvimento de ferramentas auxiliares capazes de permitir aos desenvolvedores a implementação e validação do protocolo. Deste modo, a HART Communication Foundation (HCF) criou um conjunto de ferramentas visando realizar ensaios e testes automatizados nos diferentes processos especificados na norma. Assim, se um dispositivo fosse aprovado nos ensaios de certificação, ele estaria em conformidade com a especificação do protocolo garantindo comunicação com equipamento de diversos fabricantes. Uma destas ferramentas utilizadas no processo de certificação é o analisador de redes oficial da HCF chamado de Wi-Analys (HAN et al., 2009).

Um analisador em uma rede sem fio é o equipamento responsável por sintonizar as frequências predefinidas pela camada física, interpretar os sinais captados pela antena, convertê-los para dados digitais e encaminhar tais fluxos de dados para alguma ferramenta auxiliar de análise. Nessa concepção, o analisador de redes basicamente funciona como um conversor de meio entre o ar e a interface de comunicação com o microcomputador. Do ponto de vista do analisador de redes, nenhum processamento é feito nos dados recebidos e a ferramenta de análise dos dados é um software sendo executado em um microcomputador que tem a responsabilidade de interpretar, validar e apresentar os dados capturados.

O foco de um analisador de redes formado a partir desta estrutura é auxiliar o desenvolvedor nas etapas iniciais do projeto onde aspectos como temporizações, a formação das estruturas de dados, as informações presentes dentro das mensagens trocadas entre os dispositivos de rede e a resposta dos comandos são avaliados. Esta parte do desenvolvimento ocorre em ambiente laboratorial e aspectos como mobilidade e armazenamento local das informações não são levadas em consideração no projeto da ferramenta de análise do redes.

Entretanto, quando a avaliação da rede sem fio precisa ser feita em campo, a presença de um microcomputador e a necessidade de fios interligando os equipamentos causam restrições quanto a mobilidade do ponto em que é feita a captura dos dados. Além disso, o consumo excessivo de baterias dos sistemas baseados em microcomputador também limita a autonomia do equipamento.

Assim sendo, torna-se fundamental o desenvolvimento de ferramentas capazes de realizar as etapas de coleta de dados e posterior análise do protocolo para situações reais em campo. Nestes ambientes, a possibilidade de armazenamento local dos dados para posterior análise e a previsão de alimentação por fontes alternativas à concessionária de energia elétrica são características desejáveis no projeto do sistema.

1.1 Objetivos

Os objetivos a serem alcançados por esse trabalho são:

a) Realizar um estudo das ferramentas de análise de rede baseadas no padrão IEEE 802.15.4 e no protocolo WH identificando nas ferramentas estudadas características importantes para a análise de redes WH;

b) Propor a estrutura de uma ferramenta móvel capaz de se associar a uma rede WH e que tenha a habilidade de armazenar os dados coletados em campo para posterior análise em ambiente laboratorial;

c) Implementar essa ferramenta, baseada na abordagem monocanal, desenvolvendo seu *firmware* e *software* auxiliar a partir de um *hardware* previamente concebido;

d) Projetar o *hardware* específico de uma estrutura coletora de dados multicanal;

e) E, por fim, integrar o processo de coleta de dados em campo com alguma ferramenta de análise de dados já desenvolvida.

1.2 Organização da dissertação

Esta dissertação está organizada da seguinte forma: no capítulo 2 é discutido a camada física do padrão IEEE 802.15.4 e o protocolo WH enumerando seus aspectos mais importantes. No capítulo 3 são analisados alguns trabalhos mais relevantes relacionados à análise de rede sem fio. No capítulo 4 é apresentada a proposta a ser desenvolvida nesse trabalho. O capítulo 5 mostra os resultados experimentais obtidos. Finalizando o trabalho,

o capítulo 6 discute os objetivos atingidos propondo melhorias e expondo as limitações observadas durante o desenvolvimento.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo tem por objetivo apresentar alguns conceitos fundamentais necessários para o entendimento deste trabalho. Inicialmente, o padrão IEEE 802.15.4, que é utilizado como base do protocolo WH, é descrito. Em seguida, uma breve explicação do protocolo de comunicação WH, que é o foco do analisador de redes descrito nesse trabalho, é apresentado. Finalizando o capítulo, é feita uma introdução do protocolo HART-IP utilizado para obter, externamente à redes sem fio, dados dos dispositivos de campo.

2.1 O Padrão IEEE 802.15.4

Em Dezembro de 2000, o IEEE-SA New Standards Committee oficialmente sancionou a criação de um novo projeto para iniciar o desenvolvimento de um novo padrão chamado IEEE 802.15.4 - Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPAN). A meta do grupo de trabalho do IEEE 802.15.4 era definir um padrão de comunicação por rádio frequência para ser utilizado em dispositivos de baixa complexidade, baixo custo de produção e manutenção, baixo consumo de energia e baixa transferência de dados. A palavra chave durante o processo de desenvolvimento era simplicidade (GUTIERREZ et al., 2010). Os resultados obtidos neste trabalho foram aprovados em Maio de 2003 e publicados em Outubro do mesmo ano. Entretanto, os trabalhos nesta área não cessaram. Dois novos grupos foram criados para dar continuidade ao desenvolvimento do padrão.

O primeiro deles, chamado de IEEE 802.15.4a, teve por responsabilidade adicionar uma camada física alternativa ao padrão IEEE 802.15.4-2003. O interesse por trás desse

desenvolvimento era incluir a capacidade de localização e aumento na taxa de dados mantendo baixo o consumo de energia (KARAPISTOLI et al., 2010).

O segundo grupo de trabalho, chamado de 802.15.4b, teve o propósito de melhorar as especificações do padrão IEEE 802.15.4-2003. Este grupo estava focado em resolver ambiguidades, reduzindo complexidades desnecessárias, aumentar a flexibilidade no uso das chaves de segurança e fazer extensões ao padrão já definido. Deste grupo partiu a revisão atual da especificação IEEE 802.15.4-2006 que foi aprovada em Junho de 2006 e publicada em Setembro do mesmo ano.

A especificação IEEE 802.15.4-2006 (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, 2006) foi desenvolvida para ser compatível com a revisão anterior. Em outras palavras, dispositivos em conformidade com o padrão 802.15.4-2006 deviam ser capazes de se associar e se comunicar com uma rede composta por dispositivos em conformidade com o padrão IEEE 802.15.4-2003.

A norma definiu que os participantes de uma rede padrão 802.15.4 poderiam ser divididos em dois tipos:

a) *FULL-FUNCTION DEVICE* (FFD) é um dispositivo completo. Possui todas as funções necessárias às tarefas de roteamento e inicialização da rede;

b) *REDUCED-FUNCTION DEVICE* (RFD): que é um dispositivo com recursos limitados. Apresenta apenas funções básicas de ingresso e comunicação na rede.

Um dispositivo FFD, ao ser inicializado, procura uma rede para participar. Caso não encontre uma rede, ele tem todas as funções necessárias para criar a rede. Ou seja, os dispositivos FFD tem o poder de se tornar o coordenador PAN da rede. Dispositivos FFD tem também capacidade de atuar como nós roteadores de rede trocando mensagens com outros dispositivos FFD e RFD. Em contrapartida, os dispositivos RFD poderiam apenas se comunicar com os dispositivos FFD. Não há possibilidade de comunicação entre dispositivos RFDs. Isto os torna mais simples do ponto de vista de implementação e permite que tenham requisitos mais limitados do ponto de vista de memória e processamento.

O coordenador PAN é o elemento principal de uma rede 802.15.4. Esta entidade é responsável pela inicialização da rede e gerenciamento das associação dos nós subsequentes.

Após o primeiro dispositivo FFD assumir o papel de coordenador PAN, a rede está pronta para aceitar novos membros. Uma rede em conformidade com o padrão 802.15.4 somente existe se houver um único coordenador PAN por rede.

As topologias de rede que podem ser formadas são representadas na Figura 1. Duas topologias foram previstas: topologia em estrela e topologia ponto a ponto. Na topologia em estrela, o coordenador PAN inicializa a rede, gerencia a associação de novos membros e realiza o roteamento da rede como um todo. Todos os outros dispositivos devem obrigatoriamente ter comunicação direta com o coordenador PAN.

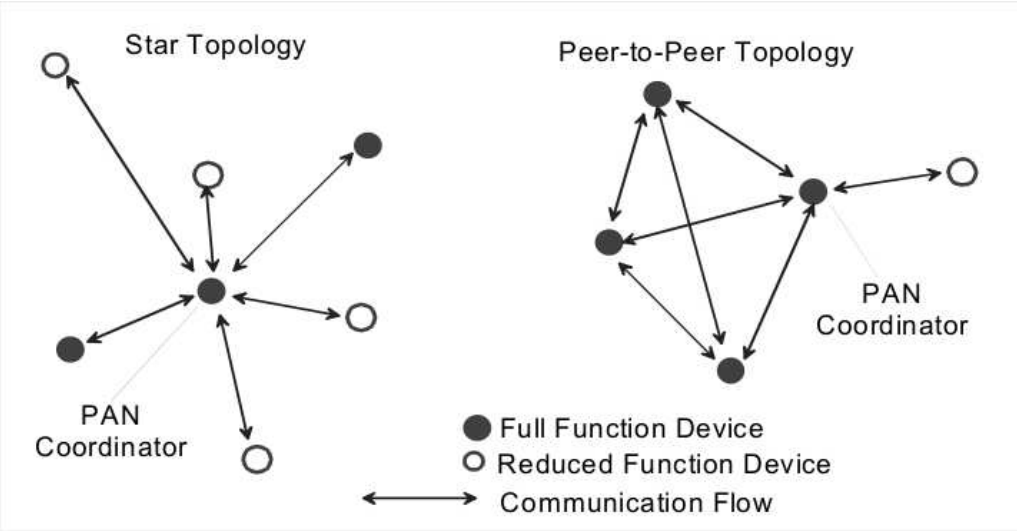


Figura 1: Topologia estrela e ponto a ponto (IEEE, 2006)

Em ambos os casos, o coordenador PAN exerce as funções de inicialização e administração da rede. Entretanto, na topologia ponto a ponto, os dispositivos de rede podem se comunicar entre si sem a utilização de recursos do coordenador PAN. A topologia de rede ponto a ponto também permite formação de redes mais complexas como a topologia em malha. Esta topologia é muito comum em redes de sensores sem fio para aplicações industriais.

Apesar do padrão IEEE 802.15.4 citar mecanismos de associação e criação da rede, topologias possíveis de serem construídas e a definição de algumas entidades de rede capazes de realizar roteamento, o modo como essas funcionalidades devem ser implementadas não está descrito na norma. A arquitetura definida para o padrão IEEE 802.15.4 consiste exclusivamente da definição da camada física (PHY) e da subcamada de acesso

ao meio (MAC).

A camada física define 3 faixas de frequências, livres de licença na banda *Industrial, Scientifical e Medical*(ISM), para comunicação: 868 MHz (Europa), 915 MHz (América do Norte) e 2450 MHz (uso global). A associação destas frequências, com diferentes técnicas de modulação, formam as PHYs especificadas na norma IEEE 802.15.4. O resumo, com as características de cada uma delas, pode ser visto na tabela 1.

Tabela 1: PHYs definidas no padrão IEEE 802.15.4

PHY (MHz)	Frequências (MHz)	Modulação	Taxa (kbit/s)
868	868-868.6	BSPK	20
915	902-928	BSPK	40
868 (opcional)	868-868.6	ASK	250
915 (opcional)	902-928	ASK	250
868 (opcional)	868-868.6	O-QPSK	100
915 (opcional)	902-928	O-QPSK	250
2450	2400-2483.5	O-QPSK	250

Fonte: (IEEE, 2006)

Dentre as PHY apresentadas, A PHY 2450 MHz é a que tem sido mais frequentemente utilizada em redes sem fio. ISA100.11a, WH e ZigBee são alguns exemplos de protocolos de comunicação sem fio que a utilizam em suas especificações.

A PHY 2450 MHz foi definida com dezesseis canais, numerados de 11 a 26, utilizando técnica de espalhamento espectral *direct sequence spread spectrum* (DSSS). O último canal definido no espectro, o canal 26, não possui abrangência global, portanto não é frequentemente utilizado. A taxa máxima de transferência de dados para esta PHY é de 250 kbit/s em um único canal.

A estrutura do *PHY protocol data unit* (PPDU) pode ser vista na Figura 2. Cada PPDU consiste basicamente dos seguintes componentes: um cabeçalho de sincronização, identificado como SHR, o cabeçalho da camada física, identificado como PHR e os dados da camada superior representado por *PHY payload*.

A sincronização entre transmissor da mensagem e o receptor é realizado pelo cabeçalho de sincronização. Seu tamanho é dependente da PHY e, para o caso específico da PHY 2450 MHz, compreeende um total de 4 bytes de preâmbulo e 1 byte de delimitação de início de frame.

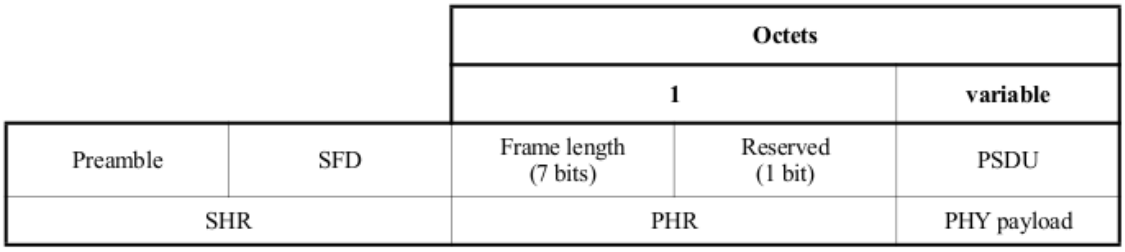


Figura 2: PPDU definido pelo padrão 802.15.4 (IEEE, 2006)

O cabeçalho da camada física é composto por apenas um byte que define o tamanho da parte de dados da mensagem. Este campo, definido com apenas 7 bits de comprimento, limitou o tamanho máximo da parte de dados ao valor de 127 bytes. Desta forma, o tamanho máximo da PPDU não pode exceder 133 bytes por pacote transmitido.

Acima da camada física, encontra-se a camada de enlace de dados. Um de seus componentes é a subcamada MAC que define regras para o uso do canal físico de rádio no envio de mensagens entre os nós da rede. Nela também são definidas estruturas de controle para o mecanismo de retransmissão de pacotes e a detecção de erros.

A subcamada MAC do padrão IEEE 802.15.4 possibilita opcionalmente a utilização de estruturas do tipo *superframes*, *timeslots* e de balizadores (*beacons*) que permitem sincronização dos dispositivos e a identificação da rede. Quando utilizados, os *superframes* são definidos pelo coordenador da rede e os balizadores enviados no primeiro *slot* de cada *superframe*.

A política de acesso utilizada no padrão IEEE 802.15.4 baseia-se no método de *Carrier Sense Multiple Access with Collision Avoidance* (CSMA-CA). Duas formas diferentes de operação são definidas em função da utilização ou não de balizadores na rede. Para confirmar a recepção de *frame*, pode-se opcionalmente enviar *frames* de *acknowledgment* (ACK). Neste caso específico, o método de CSMA-CA não será aplicado e o *frame* pode ser enviado imediatamente.

Para detectar erros durante a troca de pacotes de dados entre os nós da rede, o padrão IEEE 802.15.4 utiliza mecanismos de CRC de 16 bits conforme padronizado pela International Telecommunication Union-Telecommunication Standardization Sector (ITU-T). Todo o pacote de dados, antes de ser transmitido, tem o CRC calculado. O resultado é

enviado junto à mensagem para posterior verificação no receptor. Em caso de falha, a mensagem é descartada.

Apesar de todas as propostas inseridas no padrão IEE 802.15.4, o determinismo essencial a aplicações industriais não pode ser nativamente garantido (YOO et al., 2010). Assim, algumas especificações recentes de protocolos para comunicação sem fio tem preferido utilizar estratégias próprias para alcançar esse objetivo. O protocolo WH é um destes exemplos.

2.2 O Protocolo *Wireless*HART

O padrão WH, primeiro protocolo de comunicação aberto sem fios para aplicação de controle em tempo real, foi desenvolvido pela HART Communication Foundation (HCF) em Setembro de 2007 como uma extensão da revisão 7 da especificação HART. Tinha por objetivo oferecer uma interface sem fios aos dispositivos de controle e monitoração de processos industriais mantendo a simplicidade e a robustez do padrão HART com um custo acessível de instalação e manutenção em campo (KIM et al., 2008).

A padronização do protocolo WH teve como um dos pontos principais a preocupação constante em manter compatibilidade com os produtos, ferramentas e sistemas HART existentes. Um dispositivo WH utiliza a mesma estrutura de comandos que os dispositivos HART. Desta forma, usuários com experiência no protocolo HART rapidamente poderiam migrar para a nova plataforma (CHEN; NIXON; MOK, 2010).

A topologia de rede formada por uma rede de sensores WH é do tipo malha onde cada nó tem a capacidade de atuar como um roteador de mensagens para nós adjacentes. Esta prática aumenta o alcance da rede e permite a criação de rotas redundantes de comunicação contribuindo para o aumento da confiabilidade da rede. Na Figura 3 podem ser identificados alguns elementos de uma rede WH.

Os **dispositivos de campo** são os dispositivos diretamente conectados ao processo para realizar tarefas de medição e controle. Ele são os produtores e os consumidores de pacotes de dados em uma rede WH. Sua alimentação pode ser feita diretamente através da rede elétrica ou por baterias e possuem a capacidade de atuar como roteadores para os

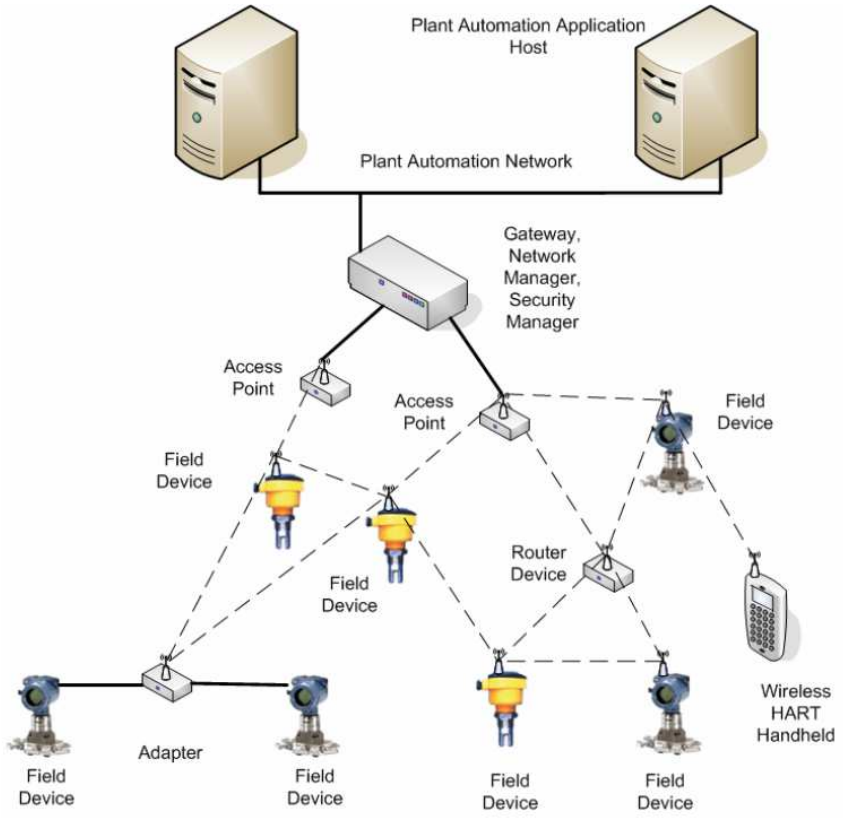


Figura 3: Rede *Wireless*HART típica (CHEN; NIXON; MOK, 2010)

dispositivos de campo em sua vizinhança.

O ***gateway*** é a entidade responsável por fazer a conexão entre a rede WH e os demais dispositivos da rede de automação do chão de fábrica permitindo que os dados fluam entre as duas redes. O *gateway* pode ser utilizado como um conversor de protocolos entre a rede de chão de fábrica e o dispositivos da rede WH. Do ponto de vista lógico, o ponto de acesso, o gerenciador de segurança e o gerenciador da rede podem fazer parte do *gateway* ou estar físicamente separados em diferentes dispositivos na infraestrutura de rede. O *gateway* possui um identificador único na rede WH.

O **ponto de acesso** (*Network Access Point* ou *Access Point*), é o dispositivo responsável pela interconexão física entre a rede WH e o *gateway*. Um *gateway* pode utilizar mais de um ponto de acesso para melhorar o fluxo de dados de entrada e saída da rede.

O **gerenciador de segurança** (*Security Manager*) tem a função de criar, armazenar e gerenciar as chaves utilizadas na criptografia dos pacotes de dados. O modelo de segurança adotado pelo WH é baseado na segurança dos dados fim a fim. Isto é, as informações

são cifradas e apenas o destino final tem a capacidade de interpretá-la corretamente para sua utilização.

O **gerenciador da rede** (*Network Manager*) tem por função realizar o gerenciamento global centralizado da rede. Tarefas como definir o momento correto em que cada dispositivo deve acessar o meio, como serão as rotas para a entrega fim a fim das mensagem e controlar o ingresso de novos membros a rede são algumas de suas atribuições. O gerenciador da rede se comunica com os dispositivos da rede para obter diagnósticos e a partir destes relatórios, ajustar a topologia da rede para manter comunicação estável mesmo na presença de interferências eletromagnéticas, obstáculos temporários ou falha de algum nó sensor intermediário. Assim como o *gateway*, o gerenciador da rede também tem um único identificador na rede.

O **roteador** (*Router*) é um dispositivo especializado que tem a função de retransmissão de mensagens dentro da rede. Em uma rede WH, os roteadores não são necessários uma vez que todos os dispositivos de rede tem a capacidade de realizar operações de reencaminhamento de mensagens. Entretanto eles podem ser benéficos para estender o alcance da rede.

Um **adaptador** (*Adapter*) é um dispositivo que permite um dispositivo HART se comunicar dentro da rede WH. Ele se comporta como um dispositivo de campo e coordena o fluxo de informações entre a rede sem fios e os dispositivos de campo HART. Um adaptador não está conectado ao processo mas suporta todos os comando exigidos por um dispositivo de campo.

O último dispositivo que pode ser encontrado em uma rede WH é o ***handheld device***. Este equipamento é utilizado para instalação, controle, monitoração e manutenção da rede. Ele é portátil e normalmente é operado pelo pessoal técnico da fábrica.

O número máximo de dispositivos em uma rede WH é limitado. Tipicamente em redes em malha, o tráfego se intensifica nos dispositivos de campo que tem conexão direta com o *gateway*. Em função dos recursos limitados destes dispositivos, diversos fabricantes tem limitado o número de nós permitidos na rede entre 50 a 100 dispositivos. (PETERSEN; CARLSEN, 2011).

A HCF definiu as camadas física, enlace, rede, transporte e aplicação para o protocolo WH. Sua representação simplificada utilizando o modelo de comunicação OSI de 7 camadas pode ser vista na Figura 4.

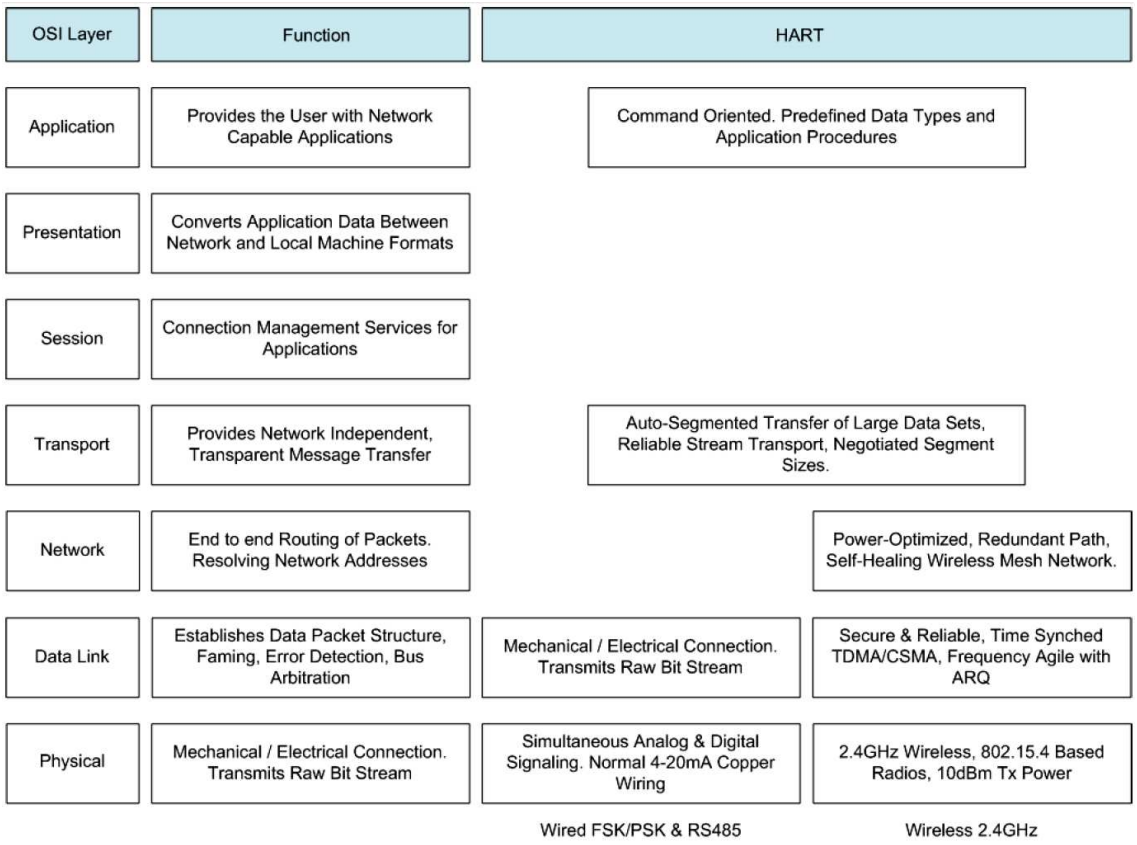


Figura 4: Modelo OSI do protocolo *Wireless*HART (CHEN; NIXON; MOK, 2010)

2.2.1 Camada física

A especificação da camada física do protocolo WH (HART COMMUNICATION FOUNDATION, 2007a) é um subconjunto simplificado do que foi definido para a camada física no padrão IEEE 802.15.4. O foco dessa especificação está em definir o meio físico, os canais de comunicação dentro do espectro de frequência utilizado, potência máxima de transmissão e sensibilidade dos receptores.

A norma do protocolo WH especifica que a comunicação via rádio frequência seja feita através dos canais 11 a 25 da banda *Industrial, Scientifical e Medical* (ISM) do espectro de 2,4 GHz. O canal 26, por questões de abrangência global, foi excluído e não deve ser utilizado. Na tabela 2 é apresentado cada um dos canais utilizados pelo

protocolo WH, com sua respectiva frequência central. Observa-se ainda um afastamento fixo de 5MHz entre canais subsequentes.

Tabela 2: Canais utilizados no protocolo *Wireless*HART

Canal	Frequência Central (GHz)
11	2.405
12	2.410
13	2.415
14	2.420
15	2.425
16	2.430
17	2.435
18	2.440
19	2.445
20	2.450
21	2.455
22	2.460
23	2.465
24	2.470
25	2.475

Fonte: HCF SPEC-065, Rev. 1.0

A potência de transmissão, limitada a 10 mW, e a sensibilidade de recepção dos transceptores foram mantidas conforme padrão IEEE 802.15.4. Desta forma, rádios comerciais homologados para o padrão IEEE 802.15.4 poderiam ser utilizados no desenvolvimento do protocolo WH.

2.2.2 Camada de enlace de dados

A camada de enlace de dados é a responsável pela confiabilidade na transferência de dados entre dispositivos vizinhos da rede. Tem por função principal detectar e corrigir possíveis erros que possam ocorrer na camada física devido a interferências ou ruídos presentes no meio físico. O protocolo WH definiu sua própria camada de enlace de dados (HART COMMUNICATION FOUNDATION, 2008a) abandonando a definição proposta pelo padrão IEEE 802.15.4. Isto foi feito para garantir o determinismo e comunicação livre de colisões necessária à aplicações industriais.

O controle de acesso ao meio típico utilizado é baseado no *Time Division Multiple Access* (TDMA). Dentro deste conceito, foram definidos intervalos temporais de 10 ms,

chamados *timeslots*, onde cada nó pode ter a permissão de transmitir ou receber seus dados. Toda comunicação entre dois dispositivos deve obrigatoriamente ocorrer dentro de um único *timeslot*. *Timeslots* são identificados através de seu *Absolute Slot Number* (ASN) incrementado a cada novo *timeslot* e inicializado com zero na criação da rede.

O *timeslot* WH é apresentado na Figura 5. Nele, a transmissão de uma mensagem deve ocorrer um certo tempo após seu início. Este atraso foi propositalmente especificado para permitir que os dispositivos envolvidos na comunicação sintonizem o canal definido para a comunicação. Por questões de sincronização, o receptor da mensagem deve escutar o canal antes do momento exato da transmissão dos dados. Após o fim do envio do pacote de dados, os dispositivos invertem o sentido de comunicação de seus *transceptores* e o dispositivo destino da mensagem indica, através de um ACK, se ele recebeu a mensagem com sucesso.

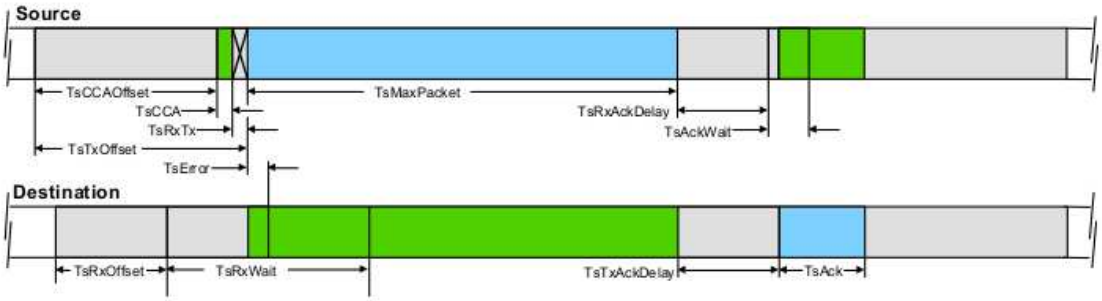


Figura 5: *Timeslot Wireless*HART (HCF SPEC-075 Rev. 1.1)

A detecção e sincronização do início de um *timeslot* é fundamental para o sucesso da comunicação TDMA proposta no protocolo WH. Em consequência disto, mecanismos de sincronização foram especificados para garantir que todos os dispositivos pertencentes à rede estejam devidamente sincronizados.

Um conjunto de *timeslots* sequencias formam um *superframe*. Todos os dispositivos da rede devem obrigatoriamente suportar mais de um *superframe* que são ciclicamente repetidos na rede. Por norma, no mínimo um *superframe* deve estar ativo na rede. Na Figura 6 é mostrado o *superframe* e o *timeslot* utilizado no TMDA do protocolo WH.

Combinado com o TDMA, o protocolo WH implementa trocas de canal físico utilizado na comunicação a cada nova mensagem transmitida pelos dispositivos da rede.

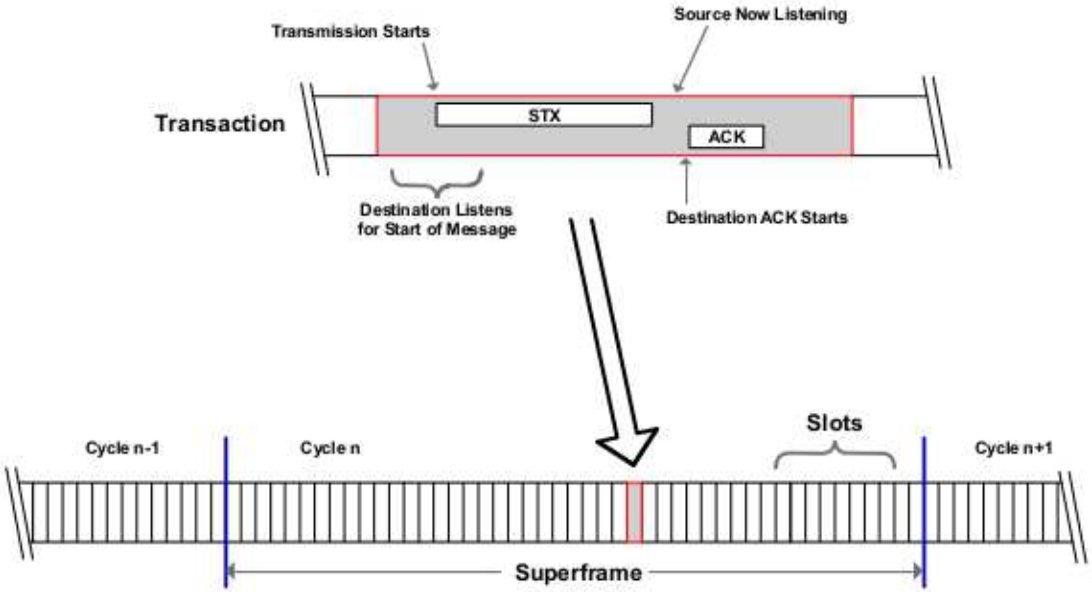


Figura 6: *Superframe Wireless*HART (HCF SPEC-075 Rev. 1.1)

Esta técnica, representada na Figura 7, provê imunidade a ruídos persistentes, comuns em ambientes industriais, aumentando a confiabilidade da rede. (SONG et al., 2008).

A associação de *superframes*, *timeslots* e o canal a ser utilizado na comunicação forma um *link* de comunicação entre os dispositivos vizinhos na rede. A entidade responsável por criar e administrar os *superframes*, *timeslots* e *links* de comunicação dando permissão de acesso ao meio a cada um dos dispositivos de rede é o gerenciador da rede. A partir das informações fornecidas pelo gerenciador da rede, cada dispositivo sabe exatamente quando pode acessar a rede, entretanto, cabe a cada um destes dispositivos a responsabilidade por armazenar localmente estes dados que podem periodicamente ser alterados.

A estrutura de um pacote de dados da camada de enlace de dados (DLPDU) é apresentada na Figura 8. Neste pacote de dados é definido o tipo de mensagem que está trafegando na rede, as mensagem que são prioritárias, a informação de que chave de rede que será utilizada na geração do *Message Integrity Code* (MIC) e a verificação de erros do pacote.

Cinco tipos de pacotes de dados foram definidos na camada de enlace de dados:

a) Pacotes de dados: contém dados sendo trocados entre os dispositivos de redes;

b) Pacotes de descoberta: são enviados periodicamente para permitir aos dispositivos de

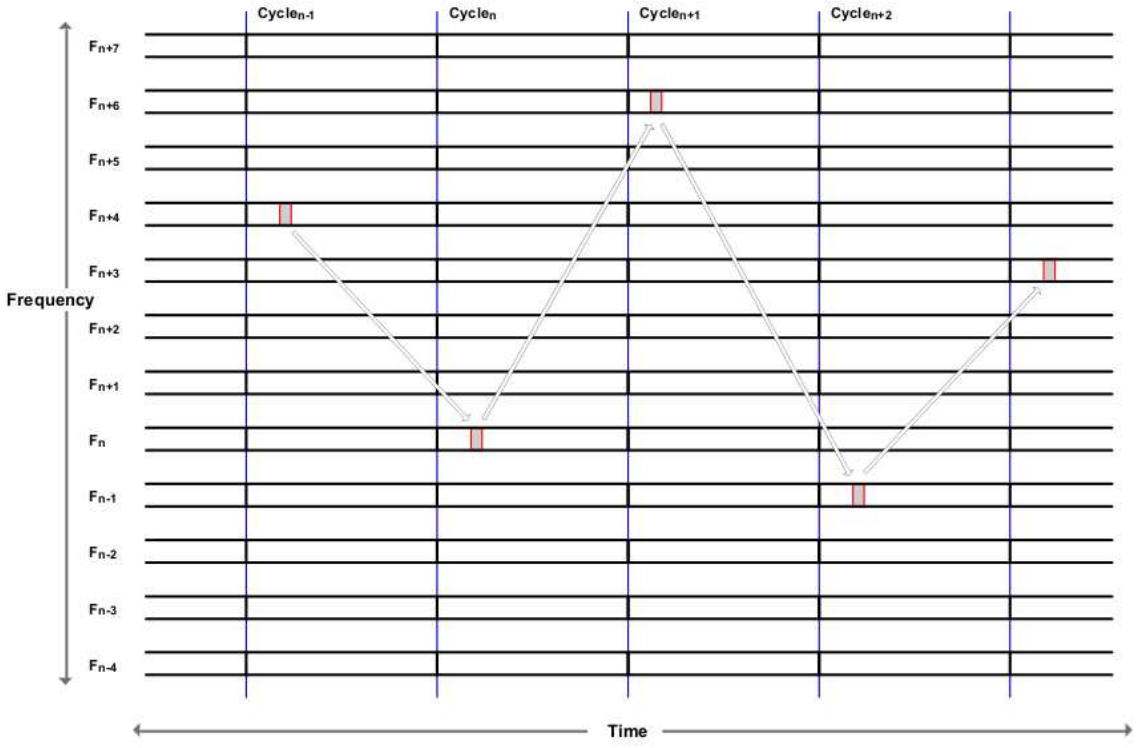


Figura 7: Saltos de frequência no protocolo *Wireless*HART (HCF SPEC-075 Rev. 1.1)

rede conhecer sua vizinhança;

c) Pacotes de anúncio: contém as informações necessárias para os vizinhos que desejam ingressar na rede.

d) Pacotes de desconexão: são utilizados para avisar a vizinhança que um determinado dispositivo de rede está deixando a rede;

e) Pacotes de confirmação: enviados pelos receptores para confirmar ao transmissor a recepção com sucesso de uma mensagem.

Para a verificação de autenticidade das mensagens enviadas pelos dispositivos de rede, duas chaves distintas são utilizadas na geração do MIC na camada de enlace de dados. A primeira, chamada de chave bem conhecida (*well-known key*), é compartilhada por todos os dispositivos WH, pois tem um valor fixo. É utilizada exclusivamente nos pacotes de anúncio da rede e quando um dispositivo está se associando a rede. A segunda chave, a chave de rede (*network key*) é criada pelo gerenciador de segurança e encaminhada a cada um dos dispositivo pertencentes à mesma rede WH através do gerenciador da rede. Esta

chave é utilizada em todas as demais transações na rede.

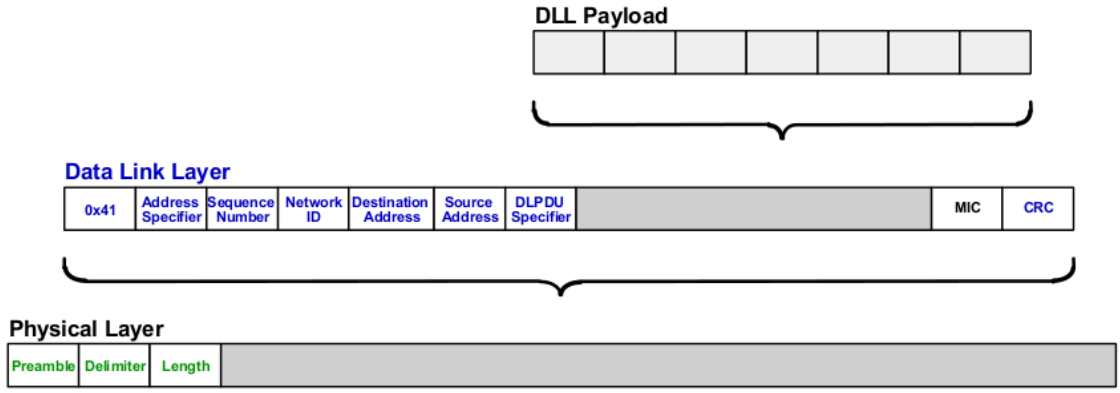


Figura 8: DLPDU do protocolo *Wireless*HART (HCF SPEC-075 Rev. 1.1)

Para evitar erros durante o processo de transmissão dos dados, foi especificada a utilização do algoritmo CRC-16 bits aplicado sobre a mensagem inteira. O polinômio gerador definido por norma é $x^{16} + x^{12} + x^5 + 1$. Assim, quando uma mensagem chega, o CRC-16 é calculado e comparado com o CRC-16 presente na DLPDU. Se eles não são iguais, há erros na mensagem e o pacote de dados deve ser descartado.

O pacote de dados definido na Figura 8 mostra dois campos de endereçamento: origem e destino. Assim, a camada de enlace de dados tem a responsabilidade de entregar um pacote de dados entre nós vizinhos. A responsabilidade sobre o roteamento da mensagem entre sua origem e seu destino final é função da camada de rede.

2.2.3 Camada de rede

A camada de rede é a responsável pelo processo de roteamento, segurança e o endereçamento para entrega das mensagens a seus destinos finais. Quanto a roteamento da rede, a norma (HART COMMUNICATION FOUNDATION, 2009) definiu três tipos que devem estar presentes em todos os dispositivos WH.

No primeiro, chamado **roteamento na origem**, a rota para a entrega final da mensagem está definida na própria mensagem. Deste modo, a medida que o pacote de dados trafega nó a nó na rede, os dispositivos intermediários sabem, a partir de campos específicos do pacote de dados, para qual nó subsequente a mensagem deve ser reencaminhada. Desta forma, não é necessário nenhum conhecimento adicional de rota. Basta seguir o que

foi definido na mensagem. Como neste tipo de roteamento, as rotas não são redundantes, falhas na entrega das mensagens pode ocorrer. A especificação do protocolo WH definiu que seu uso seja limitado apenas a procedimentos de teste na rede.

O segundo tipo é o **roteamento por grafos**. Neste tipo de roteamento, o gerenciador da rede cria uma estrutura de caminhos que interconecta os dispositivos da rede. Esta estrutura, chamada grafo, é identificada por um número único e enviada aos dispositivos da rede. Uma rede pode ter múltiplos grafos e os nós da rede podem aparecer em mais de um grafo formando caminhos redundantes. A informação sobre o grafo sendo utilizado no roteamento da mensagem está presente em um campo chamado *Graph ID* no *Network Protocol Data Unit* (NPDU) apresentado na Figura 9. Ao receber um pacote, o dispositivo de rede verifica o tipo de roteamento e procura no grafo identificado no pacote de dados, para qual vizinho deve reencaminhar a mensagem. Esse procedimento é repetido dispositivo a dispositivo até o destinatário final dos dados. Esse roteamento é mais robusto, uma vez que o gerenciador da rede define caminhos redundantes de acesso aos dispositivos alterando os grafos da rede dinamicamente em função de mudanças na topologia da rede.

O último tipo é o **roteamento por *superframe*** que é um caso especial de roteamento por grafos. Neste tipo de roteamento, os dispositivos são instruídos a enviar seus pacotes seguindo a estrutura de *links* definidas dentro do *superframe*. Todo dispositivo participante da rota deve conhecer o *superframe* e seus *links* para que os dados possam ser entregues a seu destino final. Com o roteamento por *superframe*, a identificação do grafo (Graph ID) é definida como sendo a identificação do *superframe* (Superframe ID). Se o valor do campo não é superior a 255, então o roteamento utilizado é o roteamento por *superframe*. Se o valor for 256 ou superior, então o roteamento é por grafos. Como consequência, uma identificação de grafo válida deve ser superior a 255 (CHEN; NIXON; MOK, 2010).

Na Figura 9 é apresentada a NPDU utilizada pelo protocolo WH. Ele é dividido em três partes. Na primeira, identificada por *network layer* estão os campos necessários para o roteamento das mensagens através da rede. Um de seus campos, identificado por *time to live* (TTL), controla o encaminhamento da mensagem entre os nós da rede. Todo

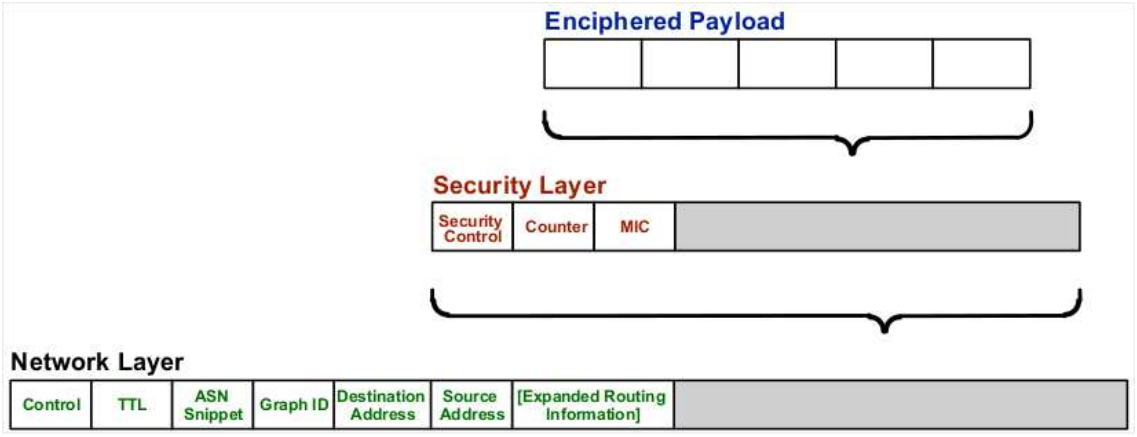


Figura 9: NPDU do protocolo *Wireless*HART (HCF SPEC-085 Rev. 1.2)

dispositivo que envia uma mensagem deve decrementar o TTL. O receptor, ao verificar que o TTL é zero, deve descartar a mensagem. Este procedimento garante que, caso o destino não seja alcançado, o pacote será destruído.

A parte de dados da camada de rede, identificada por *security layer* na Figura 9, apresenta os dados essenciais para a configuração da segurança fim a fim das mensagem na rede. O primeiro campo, identificado como *security control*, define o tipo e a chave utilizada na criptografia da subcamada seguinte. No nível de camada de rede, duas chaves estão definidas: a chave de agregação (*Join Key*) e a chave de sessão(*Section Key*). Ambas atuam, em momento diferentes, no processo de validação do MIC da camada de rede e na criptografia dos dados das camadas superiores.

A última parte definida no NPDU é a sua parte de dados. Por questões de segurança, ela é sempre criptografada. Deste modo, a integridade da mensagem é mantida até seu destino final evitando alterações nos dados pelos dispositivos intermediários, responsáveis pelo roteamento da mensagem. O conteúdo criptografado corresponde aos dados da camada de transporte apresentada a seguir.

2.2.4 Camada de transporte

A camada de transporte é utilizada para garantir que a comunicação fim a fim entre dois dispositivos da rede seja feita com sucesso. Do mesmo modo que é feita na camada de enlace de dados, onde a confirmação de entrega da mensagem entre vizinhos da rede é feita por pacotes de ACK, a camada de transporte se preocupa com a confirmação da

entrega no destino final dos dados. Este método permite que os pacotes sejam enviados e sua entrega seja rastreada garantindo sincronismo na transmissão e recepção dos dados entre os nós envolvidos na transação.

Na Figura 10 é mostrado o *Transport Layer Packet* (TPDU). Nesta Figura pode-se observar que o protocolo WH permite que múltiplos comandos HART sejam enviados em uma única TPDU. Nativamente, comandos HART de 16 bits são suportados pelo protocolo WH.

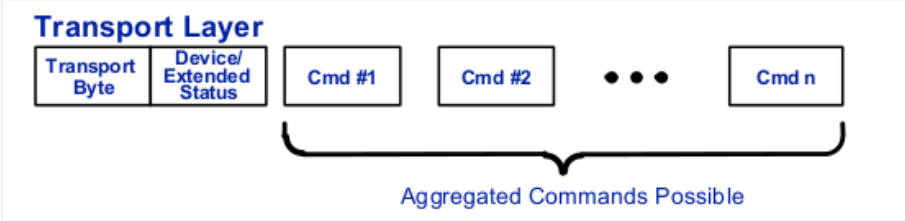


Figura 10: TPDU do protocolo *Wireless*HART (HCF SPEC-085 Rev. 1.2)

2.2.5 Camada de aplicação

A camada de aplicação é a camada mais alta na hierarquia proposta no modelo OSI. Ela define os comandos necessários para a comunicação entre os elementos da rede. A camada de aplicação do protocolo WH herda a camada de aplicação do protocolo HART. Com isso, toda a estrutura do protocolo WH, que inclui comandos, respostas a estes comandos e tipos de dados utilizado na comunicação, é mantida conforme especificada no protocolo HART. Essa decisão da HCF possibilitou uma comunicação que independe do meio físico em que os dispositivos de rede estão conectados.

A especificação da camada de aplicação (HART COMMUNICATION FOUNDATION, 2007b) define que cada comando seja identificado por um número único entre 0 e 65535. Devido a similaridade de funções e obrigatoriedade de implementação, grupos de comandos foram criados. O resultado dessa agregação gerou as seguintes classes de comandos:

a) **Comandos universais**: compreende um conjunto de comandos obrigatórios que devem ser implementados em dispositivos HART;

b) **Comandos comuns**: correspondem um conjunto de comandos com implementação opcional;

c) **Comandos privados**: representam um conjunto especial de comandos utilizado durante o processo de desenvolvimento do dispositivo;

d) **Comandos de uma família de dispositivos**: compreendem um conjunto de comandos comuns a mesma família de dispositivos. Sensores de temperatura, pressão e válvulas são alguns exemplos;

e) **Comandos específicos**: são comandos criados pelos fabricantes para utilização exclusiva em um determinado dispositivo de campo;

f) **Comandos para dispositivos sem fio**: referem a todos os comandos de implementação obrigatórios para os dispositivos WH.

Para dispositivos WH, a classe dos comandos para dispositivos sem fio tem extrema importância. Ela define o identificador único de cada comando, a estrutura de parâmetros e a definição das respostas para operações como, por exemplo, escrever links (comando 967), escrever rotas (comando 974) e ler os vizinhos (comando 787) de um determinado dispositivo de rede. Todos os demais comandos de implementação obrigatória para os dispositivos de rede são cobertos e estão descritos na norma (HART COMMUNICATION FOUNDATION, 2008b).

Através das interfaces presentes no *gateway* WH e utilizando os comandos definidos na camada de aplicação, é possível obter informações dos dispositivos na rede sem fio. Um exemplo disso é apresentado em (WINTER et al., 2011) que utilizou o protocolo HART-IP para obter informações sobre o roteamento e dados da vizinhança de cada um dos dispositivos da rede.

2.3 O Protocolo HART-IP

A seção 10 da norma (HART COMMUNICATION FOUNDATION, 2011) define o protocolo HART-IP. Nesta seção são descritos os procedimentos necessários para que

os dispositivos HART se conectem em redes baseadas no protocolo IP. HART-IP é um mecanismo relativamente simples de comunicação que suporta tanto o protocolo TCP quanto o UDP em sua implementação. Não existe uma definição quanto aos requisitos de *timeout* na entrega dos pacotes. Entretanto, a aplicação deve levar em consideração o congestionamento da rede e falhas possíveis na transmissão para sua definição.

A arquitetura geral do protocolo HART-IP, mostrada na Figura 11, define dois tipos de elementos: o servidor HART-IP e o cliente. Um servidor HART-IP pode ser um dispositivo de campo HART, um *gateway* WH para acesso aos dispositivos de campo WH ou um sistema de IO que se conecte aos tradicionais sistemas HART 4-20mA. Dispositivos conversores HART-IP para serial também são possíveis.

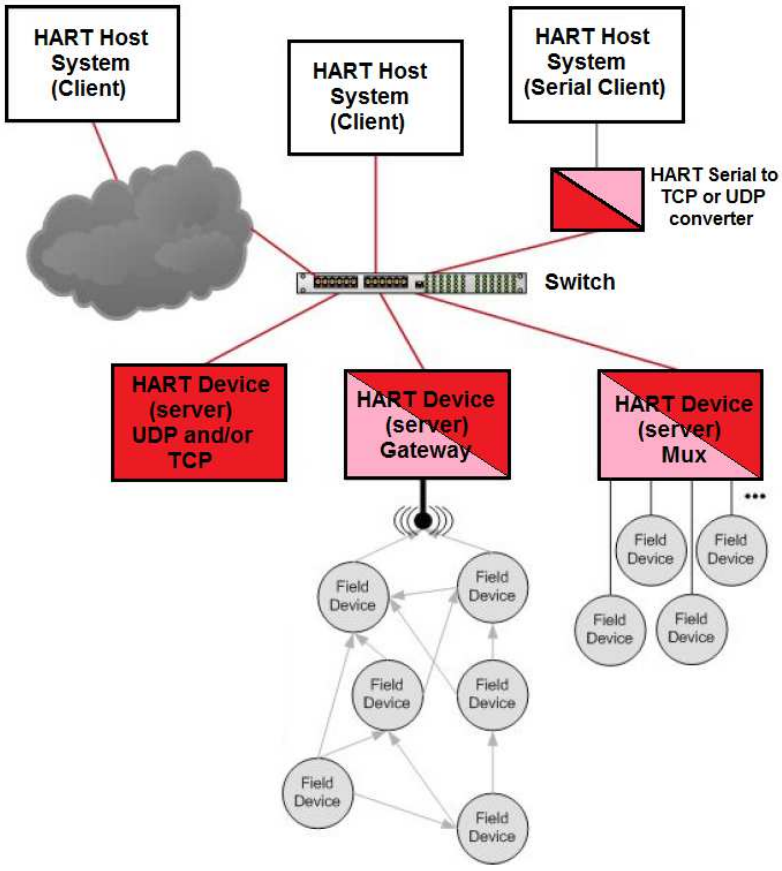


Figura 11: Dispositivos HART-IP (HCF SPEC-085 Rev. 2.0)

O servidor HART-IP aguarda pedidos HART. Ao receber um pedido HART, a mensagem é processada e retornada para o cliente que fez o pedido. A porta padrão utilizada na comunicação é a porta 5094. Entretanto, a modificação desse valor padrão pode ser

alterada em função de necessidades específicas da rede. O cliente HART-IP permite que uma aplicação se comunique com um dispositivo remoto. O cliente monta uma requisição HART-IP com as informações necessárias à aplicação e as envia ao servidor HART-IP. Os pedidos podem ser construídos tanto dentro de pacotes UDP quanto TCP. O servidor deve responder utilizando o mesmo tipo de pacote de dados.

Alguns cuidados adicionais são indicados na norma. Um deles se refere ao processo de conexão entre o cliente HART-IP e o servidor. Neste ponto, a norma recomenda que o conexão entre o cliente HART-IP e o servidor seja mantida aberta. evitando aberturas e fechamento desnecessários a cada transação.

No caso específico da rede WH utilizada nesse trabalho, a aplicação cliente HART-IP está localizada em um microcomputador fora da rede sem fio enquanto que o servidor HART-IP é implementado no *firmware* do *gateway* WH. Assim, através da rede *Ethernet*, a aplicação se conecta na porta padrão e coleta os dados necessários dos dispositivos de campo. A especificação dos campos e formatação das mensagens também é apresentado em (HART COMMUNICATION FOUNDATION, 2011).

2.4 Síntese do capítulo

Neste capítulo foram apresentadas as duas normas que servem de base para o entendimento dos demais capítulos desse trabalho. Na primeira parte do capítulo, apresentou-se o padrão de comunicação sem fio IEEE 802.15.4. Este padrão tem sido frequentemente utilizado em redes de sensores sem fio. Entretanto não possui robustez suficiente para aplicações industriais. Em seguida, o protocolo WH foi apresentado. Este protocolo utiliza como base a camada física do padrão IEEE 802.15.4 e redefine as camadas superiores com o objetivo de fornecer uma solução capaz de ser utilizado em ambiente fabril. Finalizando o capítulo, é apresentado o protocolo HART-IP, implementado no *gateway* para prover acesso aos dados dos dispositivos de campo.

3 ANÁLISE DO ESTADO DA ARTE

Este capítulo tem por objetivo fazer uma análise do estado da arte dos analisadores de rede sem fio estudados nestes trabalho. Os trabalhos mais relevantes serão analisados expondo suas características principais e seus objetivos. Um breve comparativo entre eles é feito no final do capítulo.

3.1 Revisão bibliográfica

Diversas propostas estão sendo desenvolvidas com o objetivo de coletar dados de redes sem fio. Entretanto, este trabalho escolheu analisar cinco abordagens que se destacaram por focar diretamente em redes WH ou o padrão IEEE 802.15.4, base do protocolo WH. Cada uma destas abordagens é apresentada a seguir.

3.1.1 Wi-Analys

A HCF especifica um conjunto de ferramentas para ensaios de conformidade visando certificação dos dispositivos WH através da suite Wi-HTest (HAN et al., 2009). Uma dessas ferramentas, chamado *Wi-Analys*, é um analisador de protocolo que tem a responsabilidade de fazer a captura das mensagens trocadas entre os dispositivos e registrar os dados coletados medindo as temporizações obtidas durante a comunicação. Tais dados são então encaminhados para uma ferramenta posterior que define se o dispositivo sob teste deverá ou não ser certificado.

A ferramenta *Wi-Analys*, apresentada na Figura 12, é composta de uma unidade receptora e um software sendo executado em um microcomputador. A conexão entre estas

duas entidades é feita através de um cabo USB. A unidade receptora é responsável por fazer a coleta dos pacotes de dados que trafegam no meio físico enquanto que o software do microcomputador realiza a organização, filtragem e a apresentação dos dados. O software permite que as informações sejam coletadas através da porta USB ou carregadas através de arquivos de log coletados anteriormente. Todas as mensagens capturadas são interpretadas, camada a camada, e cada um dos campos do protocolo são apresentados em colunas na tela para o usuário do sistema.

Figura 12: Analisador de redes *Wireless*HART Wi-Analys

Internamente, a unidade receptora do *Wi-Analys* é composta por 15 transceptores padrão IEEE 802.15.4 conectados em uma única antena através de *splitters*. Cada um destes transceptores sintoniza um canal diferente dentro do espectro de 2.4 GHz. Todos estes rádios são conectados a uma FPGA que realiza periodicamente a amostragem de cada um dos canais. Os dados então são agregados, buferizados e enviados para a porta USB

do microcomputador. Nesta arquitetura, a unidade receptora tem a capacidade de coletar dados, de forma simultânea, de todos os 15 canais do espectro de 2.4GHz definidos para o protocolo WH com uma taxa máxima de 1000 mensagens por segundo.

Apesar da intenção de uso final deste analisador ser focado no processo de certificação de conformidade dos dispositivos WH, o *Wi-Analys* é um produto da HCF que pode ser utilizado de maneira isolada da suite *Wi-HTest*. Neste caso, ele atua como uma ferramenta de monitoração da rede WH auxiliando os projetistas de sistema e desenvolvedores na implementação do protocolo nas etapas iniciais do desenvolvimento de novos dispositivos de campo.

3.1.2 Analisador de 16 canais

O analisador descrito em (KRATZIG et al., 2009) propõe um analisador de redes IEEE 802.15.4 capaz de coletar dados simultaneamente em todos os 16 canais do espectro de 2.4GHz. Apesar de não focar nenhum protocolo específico, foi projetado para atender as exigências temporais impostas pelo método TDMA utilizado no protocolo WH. A arquitetura da solução proposta é apresentada na Figura 13 onde pode-se observar que a solução foi dividida em três partes distintas: a unidade de radio frequência, a unidade de processamento de sinais e uma unidade remota de controle que foi implementada em um microcomputador.

A unidade de rádio frequência é composta por antena, *splitter* e 16 transceptores CC2420 da Texas Instruments. A comunicação entre cada um dos transceptores e a unidade de processamento de sinais é feita de forma independente através da interface de comunicação SPI. Nesta estrutura, os transceptores CC2420 são os escravos do barramento SPI. Adicionalmente aos quatro fios utilizados pela porta SPI, cada um dos transceptores utiliza mais seis fios de controle, totalizando dez fios conectados entre cada transceptor e a unidade de processamento de sinais.

A unidade de processamento de sinais é implementada em uma FPGA Spartan-3A DSP da Xilinx. A parte principal da FPGA é o softcore MicroBlaze que se interliga, via barramento interno, ao *Transceiver IP-Core*, ao controlador de *Ethernet* e ao controlador de interrupções do sistema. O *Transceiver IP-Core* foi desenvolvido para controlar e se

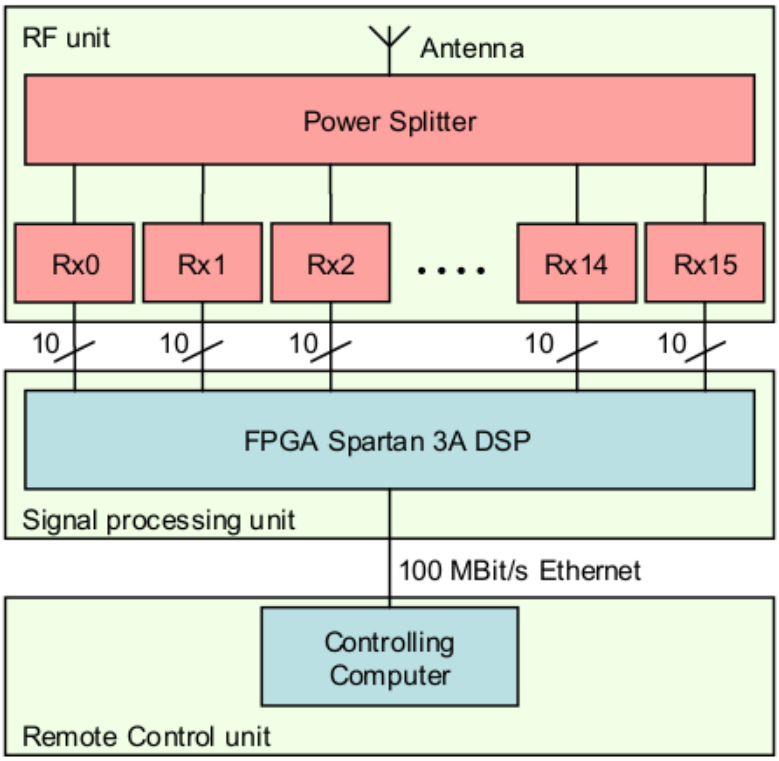


Figura 13: Analisador proposto por (KRATZIG et al., 2009)

comunicar com os receptores de rádio frequência enquanto que o controlador *Ethernet* é o responsável pela interface de comunicação com a unidade de controle remoto.

O *Transceiver IP-Core* é composto por 16 instâncias do módulo mestre da interface SPI. Cada uma destas instâncias se comunica com os transceptores presentes na unidade de rádio frequência. O módulo mestre tem por função realizar a configuração dos registradores do transceptores, gerar o sinais essenciais a comunicação SPI e ler o buffer de recepção dos transceptores. Cada mensagem padrão IEEE 802.15.4 recebida pelos transceptores vem acompanhada da informação de intensidade de sinal (RSSL) e de uma marca temporal indicando quando o dado foi capturado no tempo. Estes dados são agregados e armazenados em um buffer que é posteriormente transferido para a unidade de controle remoto.

O último componente da topologia proposta por (KRATZIG et al., 2009) é a unidade de controle remoto. Esta unidade é conectada à unidade de processamento de sinais através de uma porta *Ethernet*. Através desta porta, a unidade de controle remoto realiza a configuração do sistema e a captura dos dados coletados pelos transceptores. Todos

os dados coletados pelo sistema proposto são armazenados em arquivos texto no microcomputador permitindo sua posterior análise através de alguma ferramenta de análise. A ferramenta de análise não é descrita no trabalho pois o foco está na parte de coleta dos dados, não se preocupando com a interpretação dos dados obtidos pelos sistema.

3.1.3 Analisador IEEE 802.15.4 monocanal

Assim como na proposta de analisador de protocolo descrita acima, o trabalho realizado em (MRAZ et al., 2011) foca em redes padrão IEEE 802.15.4. O objetivo deste trabalho é o desenvolvimento de uma plataforma de análise de protocolos sem fio baseado na rede padrão IEEE 802.15.4 que possa ser livremente distribuído através de uma licença pública (LGPL). A topologia proposta neste trabalho é dividida em duas entidades, conforme mostrado na Figura 14.

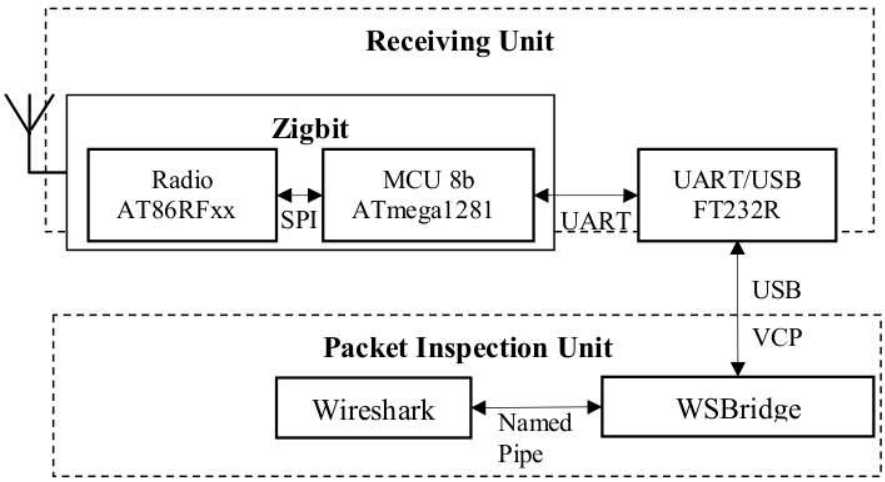


Figura 14: Analisador proposto por (MRAZ et al., 2011)

A primeira entidade, chamada de unidade de recepção, é a responsável por captura dos pacotes no meio físico. É composta por um transceptor de rádio frequência AT86RFxx da Atmel, um microcontrolador, um oscilador, um circuito integrado conversor UART-USB e alguns componentes passivos. O microcontrolador utilizado neste trabalho foi o Atmega1281, um dispositivo de 8 bits da família AVR. Através de sua porta SPI, os dados capturados no ar pelo transceptor são transportados até o microcontrolador que armazena o frame recebido e acrescenta um *timestamp*. Em seguida, o conjunto *timestamp* mais pacote de dados é transferido para o buffer da porta de comunicação serial assim que o

pacote anteriormente capturado tenha sua transmissão finalizada. A interface de comunicação utilizada para leitura dos dados coletados na unidade de recepção é a a porta USB. Entretanto, como essa porta de comunicação não é nativa no microcontrolador utilizado, o circuito integrado FT232R da FTDI foi incluído no projeto para fazer a conversão entre a porta serial e a porta USB.

Conectada na porta USB da unidade de recepção, encontra-se a segunda entidade proposta na solução. Esta entidade, chamada de unidade de inspeção dos pacotes, é composta por um microcomputador e por dois softwares necessários para análise das mensagens do microcomputador. O primeiro deles é o software WireShark que é utilizado para análise dos dados coletados. O segundo sofware é o *WSBrigde* que faz as operações necessárias para ler os dados na porta USB e encaminhá-los, através de *named pipes*, ao programa WireShark. Como esta aplicação suporta nativamente *named pipes*, o *WireShark* não precisou ser alterado.

A utilização de cabo USB com tamanho máximo limitado a 5 metros, a necessidade da utilização do programa WSBridge e restrições quanto a taxa máxima de transferência de dados na comunicação serial foram alguns pontos negativos citados pelos autores. Uma solução alternativa encontrada para remover estas restrições foi a utilização da interface *Ethernet* na interligação entre as entidades do sistema. Entretanto, como o trabalho ainda está em desenvolvimento, nenhum resultado prático foi exposto.

3.1.4 Z-Monitor

A solução apresentada em (KOUBAA et al., 2011) é denominada de Z-Monitor. Seu objetivo é prover uma solução para monitoração e testes de redes padrão IEEE 802.15.4 que seja aberta, extensível e modular sem exigir nenhum tipo de hardware especial para a realização da tarefa de coleta dos dados. A topologia proposta nesse trabalho é dividida em duas partes principais conforme pode ser vista na Figura 15.

A primeira parte compreende ao hardware responsável pela coleta dos dados. Sua função nesta estrutura é apenas realizar a conversão de meios fazendo uma ponte entre o ar e a interface de comunicação com o microcomputador. Deste modo, qualquer transceptor compatível com o padrão IEEE 802.15.4 poderia ser utilizado como hardware coletor de

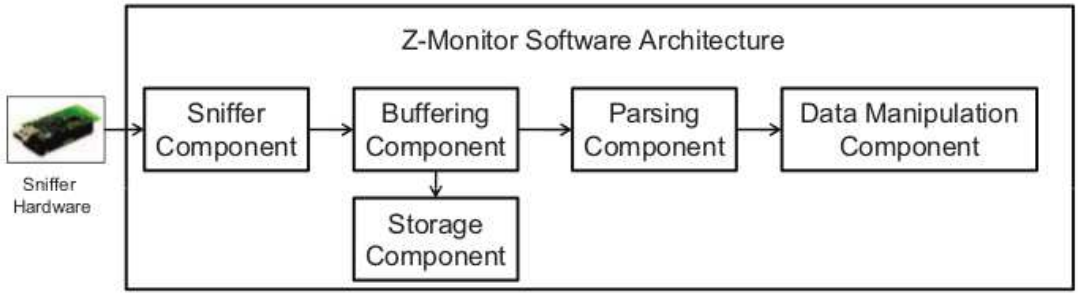


Figura 15: Analisador proposto por (KOUBAA et al., 2011)

dados. Nos ensaios experimentais mostrados no trabalho, foi utilizado o mote TelosB executando a aplicação tknsniffer do TinyOS para a captura dos dados que eram direcionados para uma porta USB conectada ao microcomputador.

A segunda parte é composta por um microcomputador e pelo software Z-Monitor que era o foco do trabalho proposto. O Z-Monitor coletava os pacotes que chegavam pela porta USB e os armazenava em um buffer. Em seguida, os dados eram interpretados e apresentados ao usuário através de uma interface gráfica.

O projeto do software foi implementado por meio de cinco componentes principais através de classes da linguagem JAVA. Um destes componentes, *sniffer component*, tem a responsabilidade de coletar as mensagens recebidas do hardware de captura e encaminhá-la para o *buffer component* que realizava as funções de buferização.

No desenvolvimento do software, foi previsto necessidade de armazenamento de dados em arquivos ou em banco de dados. Estas operações, que tinham por objetivo auxiliar a análise dos dados posteriormente, foram implementadas no componente *Storage Component*.

O componente mais importante da aplicação é chamado *parsing component*. Através do conceito de herança, este componente permite que novos protocolos possam ser facilmente adicionados ao software estendendo suas capacidades. Entretanto, na implementação original do Z-monitor, apenas os interpretadores dos protocolos ZigBee e 6LoWPAN estão disponíveis. Apesar da ferramenta permitir criação de módulos capazes de interpretar novos protocolos, a aplicabilidade ao WH não é totalmente coberta.

3.1.5 Analisador WH distribuído

Diferentemente das soluções descritas anteriormente, uma solução distribuída de análise de redes WH foi inicialmente proposta em (FERRARI et al., 2009). Nesta proposta, um número arbitrário de unidades coletoras de dados, chamadas *probes*, foram espalhados pelo chão de fábrica com o objetivo de coletar pacotes de dados WH em diversos pontos da rede. Estas estruturas foram então interligadas a uma estação central de monitoração através de uma complexa estrutura de cabos *ethernet* e *switches Gigabit*. O objetivo desta proposta era avaliar a rede como um todo e não somente em um ponto específico da rede conforme apresentado nas soluções anteriores. O trabalho sugere ainda a possibilidade de utilização dos dados coletados pela ferramenta para realimentar o gerenciador da rede auxiliando-o no processo de manutenção e ajustes da rede. A Figura 16 apresenta esta solução.

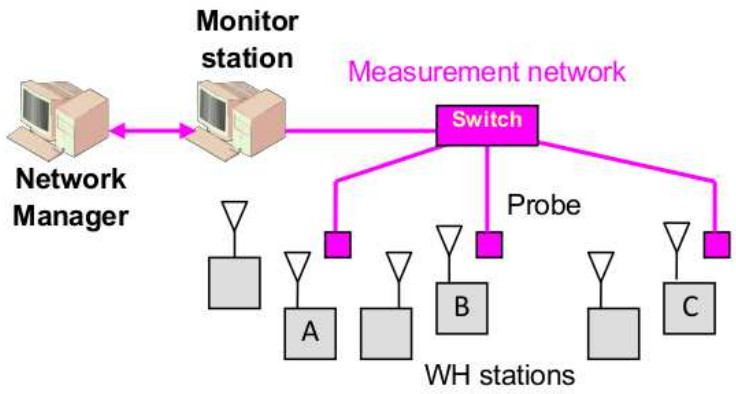


Figura 16: Analisador proposto por (FERRARI et al., 2009)

A estrutura interna de cada *probe*, mostrada na Figura 17, consiste em até 15 transceptores MC13192 da Freescale e uma FPGA Stratix-II da Altera. Na FPGA foram sintetizados um softcore, 15 controladores SPI, 1 controlador *ethernet* e um IP para gerenciar o mecanismo de sincronização entre as diversas *probes*. Quando um pacote de dados é detectado por um dos transceptores, cada um sintonizando um canal, uma interrupção é enviada à FPGA. Esta, através de seus respectivos controladores SPI, realiza a coleta dos dados e inclui a informação sobre o canal por onde os dados foram recebidos e uma marcação temporal antes de encaminhá-la à central de monitoração.

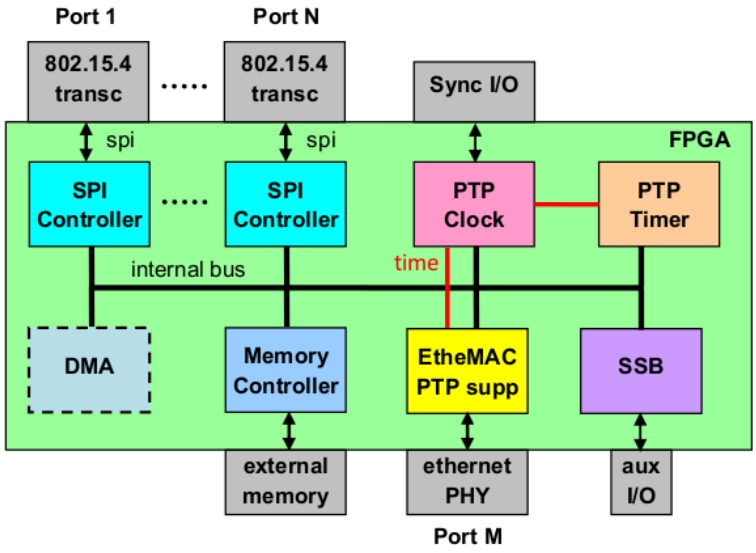


Figura 17: *Probes* coletoras proposta por (FERRARI et al., 2009)

A central de monitoração foi implementada em microcomputador que trata os pacotes recebidos, descarta os inválidos e ignora os repetidos. Para o sucesso da implementação, a sincronização entre as *probes* teve que ser cuidadosamente estudada, uma vez que um pacote de dados poderia ser capturado por mais de uma *probe*. Diversos métodos de sincronismos foram implementados e avaliados como a utilização de GPS, a sincronização por pulso periódico ou ainda a utilização de protocolo IEEE1588 (DEPARI et al., 2009).

3.2 Análise comparativa dos trabalhos mais relevantes

Nos trabalhos analisados foi observada a utilização de diversas arquiteturas para análise de redes sem fio. Alguns trabalhos, exclusivamente para análise de redes padrão IEEE 802.15.4, utilizaram hardwares disponíveis comercialmente onde apenas um único transceptor RF era utilizado para aquisição dos dados transmitidos no meio físico. Nestas soluções, onde apenas um canal pode ser sintonizado por vez, modificações de software precisam ser feitas para que os elementos coletores de dados possam ser utilizados na análise de redes WH. Tais restrições, impostas pelo mecanismo de TDMA e pelos saltos de frequências utilizados durante a comunicação, praticamente inviabilizam soluções proprietárias onde o foco do projeto não englobou redes WH e onde o *firmware* de controle não estão livremente disponíveis para alterações.

Por esta razão, algumas soluções têm sido desenvolvidas em âmbito acadêmico. Nestes trabalhos, a solução mais adotada nos trabalhos focados em WH é a utilização de 16 *transceptores* de RF onde cada um dos *transceptores* é colocado em modo recepção com frequência prefixado em um dos canais do espectro de 2.4 GHz. Como a captação dos dados pelos transceptores é feita de modo paralelo, mesmo ocorrendo saltos de frequências durante a comunicação, o sistema é capaz de capturar os pacotes de dados a serem analisados. Esta solução ainda adiciona outras vantagens pois torna desnecessária a crítica sincronização dos *timeslots*, o conhecimento das estruturas necessárias para troca dos canais da rede além de permitir captura de comunicação de mais de uma rede simultâneamente. Em contra partida, esta estrutura necessita de mecanismos adicionais de sincronismo para que as informações recebidas em cada canal tenha correlação temporal e sejam efetivamente lidas na mesma ordem em que foram recebidas. Para resolver essa questão, diversos sinais de controle precisam ser inseridos no sistema e a inclusão de um módulo especial de coordenação tem sido utilizado para desempenhar esta tarefa.

O trabalho desenvolvido por (HAN et al., 2009) é a referência oficial da HCF quando se trata de análise de redes WH. Foi desenvolvido para uso em laboratórios de certificação de dispositivos de campo que exige, para funcionamento correto do sistema, uma conexão com a porta USB para captura das informações coletadas. Desta forma, os dados capturados no ar precisam ser imediatamente enviados e armazenados no microcomputador, que pode fazer análise imediata do que está sendo transferido. As soluções apresentadas pela HCF são proprietárias, o que não permite meios de se customizar a ferramenta para inclusão de novas funcionalidades no sistema. Também não há previsão de armazenamento local dos dados coletados no dispositivos obrigando que, em caso de utilização em campo, uma estrutura envolvendo microcomputador, cabos e baterias sejam utilizadas.

Seguindo a mesma linha de desenvolvimento do Wi-Analys, o trabalho proposto por (KRATZIG et al., 2009) também apresenta uma estrutura multicanal com gerenciamento centralizado através de uma FPGA. Entretanto com uma alteração no ponto de vista de interfaceamento entre as unidades. A porta USB, com limitação máxima de comprimento de 5 metros, foi substituída por uma porta de comunicação *Ethernet* permitindo estender

a distância entre as unidades de processamento de sinais e a unidade de controle remoto. Essa nova abordagem permite que a unidade de análise, localizada em um microcomputador, possa estar fisicamente afastada da unidade de coleta e processamento. Em contrapartida, a necessidade de acesso à rede *ethernet* próximo ao ponto sob análise limita a área de atuação do sistema. A utilização das duas estruturas no mesmo local, interligadas por um cabo cruzado, traz consigo as mesmas desvantagens apresentadas pelo Wi-Analys.

Com foco em analisar toda a rede WH, o trabalho apresentado por (FERRARI et al., 2009) propõe a utilização de uma série de coletores de dados espalhados pelo ambiente sob análise. Cada unidade coletora segue a estrutura multicanal com interface *Ethernet* sem armazenamento local. Para realizar a tarefa de interligação dos coletores de dados uma série de *switches* precisam ser utilizados para que os dados possam ser transferidos no momento da coleta. Essa proposta impõe mecanismos adicionais de comunicação entre os nós para garantir precisão de sincronismo na captura dos dados. A proposta deste trabalho está mais focada em analisar desempenho no trânsito dos pacotes de dados pela rede do que analisar o conteúdo das mensagens sendo transmitido. A necessidade de utilização de switches, assim como nas abordagens anteriores, restringe a flexibilidade e a mobilidade da proposta quando pontos de difícil acesso precisam ser analisados.

A proposta de análise apresentada por (MRAZ et al., 2011) define uma unidade de recepção de *hardware* para coleta de dados baseado em um único *transceptor*. Nesta estrutura, que em um primeiro momento pode ser descartada para utilização em redes WH, apresenta algumas características interessantes do ponto de vista organizacional do sistema. A integração com o software *WireShark* possibilita que novos protocolos sejam adicionados à ferramenta e a utilização de hardware coletora de dados baseada em um microcontrolador permite que o *firmware* possa ser alterado visando dar inteligência ao módulo para capturar fluxos de mensagens WH.

Alguns outros trabalhos limitaram sua atuação apenas às ferramentas de software de análise desenvolvidas para serem executadas em microcomputador. O trabalho proposto por (KOUBAA et al., 2011), conhecido como Z-Monitor, é um deles. Utilizando *hardware* comercialmente disponíveis para realizar as funções de coleta de dados de redes

padrão IEEE 802.15.4, o sistema propõe uma arquitetura aberta através de um conjunto de classes para análise dos dados de diversos protocolos em que não consta, originalmente, o protocolo WH. A proposta da ferramenta é promissora, entretanto a utilização de um *hardware* especial, capaz de implementar TDMA e saltos de canal, será necessário para o interfaceamento com a ferramenta.

De forma resumida, a tabela 3 faz um comparativo apresentando as características principais de cada um dos trabalhos estudados.

Tabela 3: Comparação entre os trabalhos analisados

Analisador	Hardware	Interface	Armazenamento	Protocolo
(HAN et al., 2009)	Multicanal	USB	Após coleta	*Wireless*HART
(KRATZIG et al., 2009)	Multicanal	Ethernet	Após coleta	*Wireless*HART
(MRAZ et al., 2011)	Monocanal	Ethernet	Após coleta	IEEE 802.15.4
(KOUBAA et al., 2011)	Monocanal	USB	Após coleta	IEEE 802.15.4
(FERRARI et al., 2009)	Multicanal	Ethernet	Após coleta	*Wireless*HART

A partir da análise destes trabalhos, percebeu-se que a utilização destas ferramentas não poderia ser facilmente empregada na coleta de dados em aplicações de chão de fábrica. Nenhuma dessas ferramentas previu uso de baterias na alimentação do sistema exigindo conexão por fios que restringem sua mobilidade. O emprego de microcomputadores portáteis, que poderiam resolver esta situação, limitam a duração dos ensaios à algumas horas em função da duração de suas baterias. O espaço ocupado por estes sistemas também os tornam inapropriados para análise de redes em locais de difícil acesso em campo. O armazenamento de dados local também não foi levado em consideração durante as etapas de projeto destas ferramentas. Deste modo, a interligação entre o dispositivo coletor, armazenador e analisador se torna obrigatório para que os dados coletados possam ser armazenados permitindo que análises futuras possam ser feitas com o mesmo conjunto de dados.

3.3 Síntese do capítulo

Neste capítulo foi compilada uma revisão bibliográfica envolvendo o estado da arte dos trabalhos de analise de redes com enfoque em redes sem fio. Um aprofundamento

de *hardware* se fez necessário para o entendimento de como cada um dos trabalhos lida com as características temporais do protocolo WH. Em seguida, finalizando o capítulo, uma comparação entre as soluções estudadas foi feita apresentando aspectos relevantes de cada arquitetura. O capítulo finaliza com um quadro resumo e indica abordagens que podem ser melhor aproveitadas para a análise de redes WH em campo.

4 O ANALISADOR DE REDES *WIRELESS*HART

As propostas desenvolvidas para a análise de rede WH são descritas nesse capítulo. Inicialmente os principais desafios no processo de coleta de dados em uma rede WH são apresentados. Duas abordagens para o problema são definidas onde são explicadas suas estruturas internas, seus pontos positivos e negativos.

4.1 Desafios e limitações na análise de redes *Wireless*HART

O acesso ao meio utilizado pelo protocolo WH baseia-se em dois princípios: tempo e frequência. Para que dois dispositivos WH se comuniquem na rede é necessário que o par esteja devidamente configurado no canal e no tempo correto para que a mensagem possa ser transmitida pelo dispositivo origem e recebida com sucesso pelo dispositivo destino.

A sincronização entre os dispositivos em uma rede WH é essencial para o mecanismo de comunicação. Como o acesso ao meio físico é dividido em fatias de tempo bem definidas, todos os dispositivos da rede devem ser capazes de se sincronizar e se manter sincronizado com os *timeslots* da rede. Este processo tem extrema importância uma vez que todas as operações de transmissão e recepção de mensagem na rede foram definidas como atrasos em relação a um mesmo ponto de referência que é definido por norma como sendo o início de cada *timeslot*. Desta forma, perder a sincronização na rede irá inevitavelmente provocar falhas na entrega de mensagens.

Outro mecanismo utilizado pelo protocolo WH com o objetivo de aumentar a confiabilidade da comunicação mas que gera desafios adicionais ao projeto de um analisador de redes baseia-se no conceito de diversidade de canais. Cada oportunidade de comuni-

cação entre os dispositivos ocorre em um canal diferente dentro do espectro de 2.4 GHz. Assim, além do sincronismo com o *timeslot*, é necessário que os dispositivos possuam conhecimento de qual canal será utilizado na comunicação.

O algoritmo de cálculo do canal a ser utilizada na comunicação possui quatro parâmetros: *Offset* do canal, o ASN do *timeslot*, a tabela e o número de canais ativos na rede. O parâmetro offset do canal é armazenado na tabela de *links* de comunicação de cada dispositivo. É interessante salientar que cada dispositivo de rede conhece apenas os seus próprios *links* de comunicação. O processo de adição e remoção de *links* de comunicação em cada um dos dispositivos é feito pelo gerenciador da rede. O ASN é um número de 40 bits que é incrementado a cada *timeslot*. Como o *timeslot* é iniciado a cada 10 ms, a repetição do ASN somente ocorrerá em centenas de anos.

A última informação necessária para o cálculo do canal é a tabela de canais ativos. De todos os 16 canais especificados na camada física do padrão IEEE 802.15.4 para o espectro de 2.4 GHZ, 15 somente são utilizados pelo protocolo WH. Destes 15 canais, nem todos precisam ser utilizados na comunicação. A configuração do mapa de canais a ser utilizado é um dos parâmetros passados ao gerenciador da rede e é um dado essencial que precisa ser encaminhado a cada um dos dispositivos participantes da rede. Um dos modos do mapa de canais ativos ser transmitido aos nós da rede é através da mensagem de anúncio da rede utilizada durante o processo de ajuntamento na rede WH.

De posse do mapa de canais, dos links de comunicação e sincronizado com os *timeslots*, um novo dispositivo está apto a receber e transmitir mensagens entre os dispositivos de sua vizinhança. Entretanto, para que se possa interpretar e validar os comandos trafegando na rede, o dispositivo precisa conhecer as chaves criptográficas utilizadas na rede. Das quatro chaves criptográficas definidas no protocolo, duas delas podem ser antecipadamente conhecidas: A chave bem conhecida que é uma chave que tem valor constante definido por norma e a chave de agregação que é repassada aos dispositivos através do processo de comissionamento do nó sensor. Estas duas chaves são utilizadas no momento em que é realizado o ingresso na rede. Uma vez que o dispositivo está inserido na rede, as duas chaves restantes são enviadas ao novo integrante pelo gerenciador da rede: a chave

de rede e a chave de sessão. A chave de rede é utilizada para autenticidade em nível de camada de enlace de dados e a chave de sessão com a função de criptografia dos comandos presentes nas camadas superiores da pilha do protocolo. As três primeiras chaves (bem conhecida, de agregação e de rede) são compartilhadas entre os nós da rede enquanto que a chave de sessão é única para cada par de dispositivos presentes na mesma sessão.

Assim, o projeto de um analisador de redes com foco no protocolo WH deve abranger desde sincronização temporal com a rede para acompanhamento dos *timeslot* e do ASN da rede, conhecimento de estruturas fundamentais como *superframes* e *links* de comunicação dos dispositivos de rede na área de cobertura do analisador até a manutenção das chaves criptográficas para interpretação das mensagens cifradas trafegando na rede. A solução para análise de redes WH proposta neste trabalho pretende vencer estes desafios sendo apresentada no item a seguir.

4.2 Arquitetura do analisador de rede proposto

Conforme apresentado no capítulo 3, soluções de análises de rede atualmente sendo desenvolvidas no meio acadêmico, pode-se perceber uma variedade muito grande de arquiteturas propostas para os desafios impostos ao se coletar, interpretar e analisar mensagens coletadas no meio físico de uma rede sem fios.

Em todas as ferramentas analisadas mostrou-se uma divisão muito clara entre os elementos propostos. Em geral, a análise de redes era constituída de um dispositivo de coleta de dados no meio físico, uma interface para dar vazão aos dados coletados e um microcomputador onde era executado a ferramenta de análise dos dados coletados. Estas estruturas frequentemente utilizavam a porta de comunicação USB ou *ethernet* para a rápida vazão dos dados capturadas no meio físico entre o dispositivo coletor e o dispositivo analisador conforme é apresentado na Figura 18.

Diversos trabalhos analisados demonstraram ser promissora esta divisão funcional. A facilidade de migração de meio físico ou a independência de implementação de um protocolo de comunicação específico na unidade coletora foram alguns dos pontos positivos mencionados. Tornou-se extremamente fácil migrar de um protocolo para outro

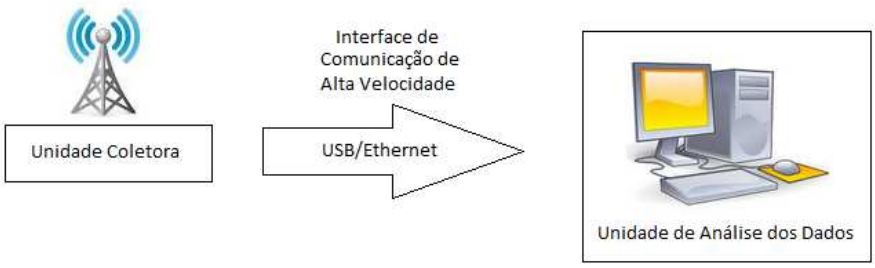


Figura 18: Entidades elementares em um analisador de redes

substituindo o dispositivos de coleta de dados sem alterar a interface de comunicação com o microcomputador. A inclusão de novos módulos no software de análise permitiria também a fácil expansão da ferramenta que também tinha a responsabilidade por todo o tratamento do fluxo de dados recebido pela interface de comunicação. Desta forma, o coletor das mensagens no meio físico atuaria apenas como um conversor de meio entre o ar e a interface de comunicação com o PC.

Entretanto, quando se pretende analisar redes WH, a entidade responsável pela coleta de dados precisa ser mais elaborada. Aspectos como sincronismo na rede com os *timeslots* e mudanças de canais frequentemente de modo coordenado entre os dispositivos de rede impossibilitam que a estrutura da unidade coletora seja baseada no conversor de meio utilizada extensivamente entre os trabalhos analisados.

Outro fator essencial a ser levado em consideração no projeto do analisador de redes WH refere-se à interface de comunicação entre as entidades propostas pelo sistema. Nos trabalhos relacionados apresentados no capitulo 3, a comunicação ocorre em tempo real onde os dados capturados pelo dispositivo de coleta são imediatamente encaminhados à unidade de análise. Entretanto, esta topologia obriga a utilização de fios causando transtornos quando se pretende ter mobilidade e flexibilidade para analisar dados de pontos remotos de uma rede instalada no campo. A exigência de fontes de alimentação também dificulta as aquisições de dados pois restringe o ponto a ser observado.

O presente trabalho propõe uma abordagem inovadora ao problema de análise de redes WH onde o processo de aquisição e análise de dados coletados é dividido em etapas. Para realizar essa tarefa, duas entidades foram definidas conforme pode ser visto na Figura 19.

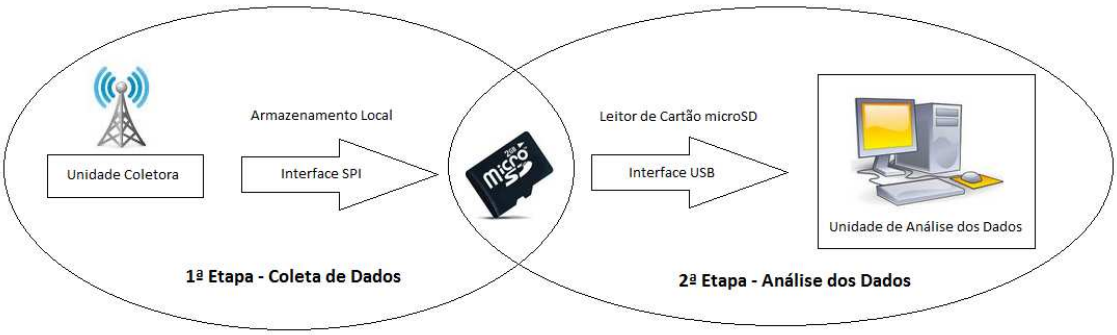


Figura 19: Etapas propostas na coleta de dados

A primeira entidade definida na estrutura do analisador WH é a **unidade coletora de dados** que tem a função de sintonizar cada um dos canais definidos na norma IEEE 802.15.4 e converter os sinais captados pela antena para um fluxo de dados digitais a ser armazenado em um cartão microSD. A unidade coletora precisa ser criteriosamente posicionada. Cabe ressaltar que a unidade coletora de dados também apresenta uma área de cobertura limitada e, desta forma, os dispositivos a serem analisados precisam estar dentro do alcance do coletor.

A segunda entidade proposta no trabalho é a **unidade analisadora de dados** que compreende um microcomputador e um software específico que realiza a leitura das mensagens WH presentes no cartão microSD, decriptografando e analisando as mensagens sendo transmitidas entre os dispositivos da rede sem fios. A análise feita pelo software proposto pode gerar informações estatísticas, apresentar a topologia da rede formada ou ainda exibir análises referentes ao roteamento entre os nós da rede sem fio. Por ser um software desenvolvido em linguagem de alto nível, novas análises podem facilmente ser implementadas estendendo as funções do analisador de rede.

A utilização de cartão SD como elemento armazenador de dados intermediário entre as entidades do sistema permite uma quebra temporal entre o procedimento de coleta e análise dos dados. Este procedimento, não observado em nenhum trabalho relacionado, elimina a necessidades de fios interligando as unidades dando mobilidade à solução. O processo de coleta e análise dos dados se tornam dois procedimentos distintos realizados em momentos e ambientes totalmente não relacionados. Assim, enquanto a coleta dos dados pode ser feita em ambiente fabril, a análise pode ser feita posteriormente em

laboratório.

A primeira etapa do processo de análise da rede é identificada na Figura 19 como coleta de dados. Ela compreende as tarefas realizadas pela unidade coletora de dados, isto é, sintonia do canal físico, captura dos frames e armazenamento de dados WH trafegando entre os dispositivos de rede no cartão SD.

O estudo do posicionamento do coletor de dados deve ser feito criteriosamente de forma que os dispositivos a serem analisados estejam dentro de sua área de cobertura. Caso uma área maior precise ser analisada, mais coletores de dados podem ser utilizados para expandir o alcance de interesse. Entretanto, a intersecção da área de cobertura pode trazer novos desafios conforme mostrado na Figura 20.

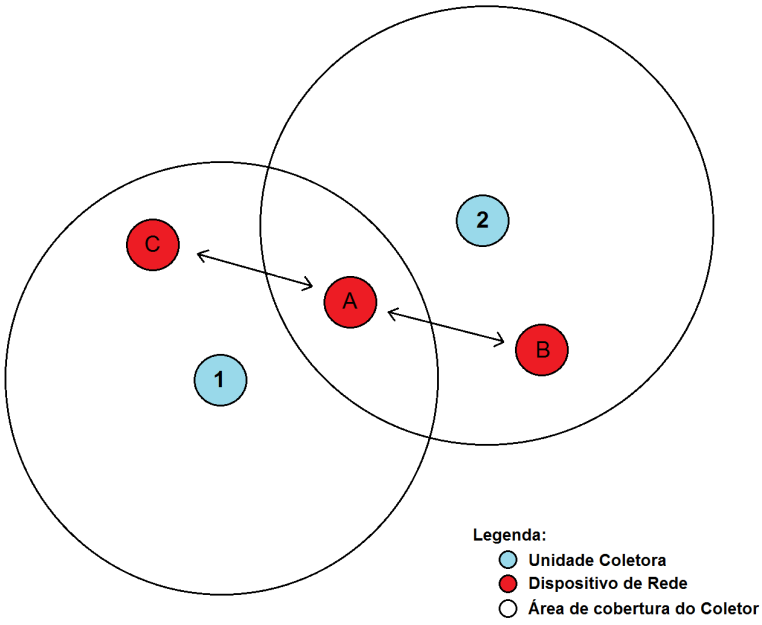


Figura 20: Rede com múltiplas unidades coletoras

As mensagens trocadas entre os dispositivos de rede A e B são captadas pela unidade coletora 2 enquanto que a unidade coletora 1 é responsável pela monitoração dos dispositivos de rede A e C. Observa-se que o dispositivo A está na área de coberta de ambas unidades coletores o que significa dizer que seus pacotes de dados são armazenados de forma duplicada pelas unidades coletoras de dados em seus respectivos cartões de memória. Caberá à unidade de análise de rede, posteriormente, eliminar possíveis causas de inconsistências de informação.

A segunda etapa do processo de análise da rede, chamada de análise dos dados, consiste em obter e analisar as mensagens WH armazenadas no cartão SD gravados na primeira etapa do processo. Uma vez que o cartão SD for recuperado da unidade de coleta de dados, os dados precisam ser importados para o microcomputador. Desta forma, a unidade de análise de dados deve ser composta por um microcomputador que possua a capacidade de ler cartões SD. Outros meios de acesso aos arquivos presentes no cartão SD também podem ser utilizados como leitores externos acessíveis através da porta USB. Com os arquivos de coleta recuperados, o software de análise de rede deve realizar as operações necessárias para importação dos dados, decodificação e análise e apresentação dos pacotes de dados capturadas através de uma interface de usuário.

A arquitetura de cada uma das entidade envolvidas nestas etapas é descrita com detalhes nas seções seguintes.

4.3 Unidade coletora de dados

Para a realização da tarefa de análise de redes WH, o presente trabalho propõe duas arquiteturas diferentes para a unidade coleta de dados. A primeira arquitetura proposta, chamada de **coletor de dados monocanal**, é apresentada no item 4.3.1 enquanto a segunda, apresentada no item 4.3.2, foi denominada **coletor de dados multicanal**.

Apesar de possuírem a mesma função primária, isto é, sintonizar o canal correto e coletar as mensagem WH gravando-as em um arquivo com formato padronizado no cartão SD, ambas propostas diferem muito em seus aspectos conceituais e construtivos. Entretanto compartilham uma característica inovadora no trabalho, que é a integração da unidade coletora de dados em um dispositivo de campo WH. Desta forma, as unidades coletoras de dados podem atuar como dispositivos de campo tendo responsabilidade de rotear pacotes de dados, distribuir anúncios da rede e responder a comandos WH mantendo inalterada a função inicial na estrutura do analisador de rede proposto.

Transformar a unidade de coleta de dados em um dispositivo de campo WH traz aspectos positivos a essa nova estrutura. Em um primeiro momento permite aumentar a abrangência da rede pois possibilita comunicação com os dispositivos dentro de sua área

de cobertura. Além disso, os processos essenciais aos dispositivos de campo como sincronismo com os *timeslots* da rede, identificação dos pacotes de dados e interpretação dos comandos passam a ser compartilhados com a unidade de coleta de dados reduzindo o tempo de implementação pelo reuso de bibliotecas e pacotes de softwares já bem testados.

O benefício mais significativo da incorporação da unidade de coleta de dados como elemento de uma rede WH reside na possibilidade de desenvolver comandos para gerenciamento à distância da unidade. O protocolo WH define uma faixa de comandos que permitem estender as funcionalidades de dispositivos de campo. Neste caso, a unidade coletora de dados pode responder aos comandos de iniciar coleta, finalizar coleta e gerenciar os dados capturados. O envio das mensagem armazenadas no cartão SD poderia ser feito pela própria rede WH.

Do ponto de vista de *hardware*, a solução utilizada na unidade coletora de dados monocanal consiste apenas em um *transceptor* IEEE 802.15.4 que salta, de canal em canal, captando as mensagens a serem armazenadas. É uma solução com *hardware* simplificado, de baixíssimo custo e consumo de baterias. Entretanto, apresenta maior esforço para implementação de *firmware* de controle da unidade de coleta de dados. Além disso, um *software* complementar necessita ser desenvolvido para o seu funcionamento completo.

Alternativas à abordagem monocanal são frequentemente encontradas na literatura. Via de regra, todos os analisadores de redes focados no protocolo WH apresentados no capítulo 3 se baseiam nesse conceito. Nesta estrutura, todos os 15 canais definidos pela norma do protocolo WH são capturados de modo paralelo por 15 *transceptores* previamente configurados. Cada um deles é sintonizado em um canal específico. Não é incomum a estrutura proposta em alguns trabalhos também apresentar um *transceptor* adicional que permite estender a solução de coleta para qualquer rede sem fio baseada no padrão de comunicação IEEE 802.15.4. Alguns entraves surgem quando comparados com a abordagem monocanal. O maior consumo energético que reduz o tempo de coleta, o custo mais elevado para fabricação e o tamanho da solução final que dificulta o posicionamento em locais de difícil acesso são alguns deles.

4.3.1 Coletor de dados monocanal

A característica principal do coletor de dados monocanal é possuir apenas um *transceptor* de RF. Essa idéia é largamente utilizada em redes baseadas no padrão IEEE 802.15.4 onde o canal utilizado pela rede é mantido estático após a inicialização da rede. Entretanto, no caso específico de redes WH que implementam salto entre os canais a cada comunicação para aumentar a confiabilidade na entrega das mensagens, essa solução traz novos desafios que precisam ser vencidos.

A utilização do TDMA que garante previsibilidade e determinismo nas transações associado ao rigor das exigências temporais e o complexo algoritmo de criptografia exigem que *hardware* para análise de redes disponíveis comercialmente não possam ser diretamente utilizados. É fundamental que mecanismos adicionais em *firmware*, como a utilização de um sistema operacional de tempo real, e em *hardware* como periférico para decodificação e precisão no circuito oscilador sejam implementados para garantir o sucesso na coleta de dados pelo dispositivo.

Mesmo que todas estas exigências fossem cumpridas com rigor, o coletor de dados monocanal ainda não teria todos os dados que necessita para desempenhar suas funções. Ele precisaria conhecer em que canais capturar as mensagens WH sendo transmitidas na sua vizinhança e a obtenção dessa informação, por si só, não é uma tarefa trivial.

A definição sobre quando e em que canal um dispositivo deve se comunicar é definido exclusivamente pelo gerenciador da rede e enviado, de forma individualizada, para cada um dos dispositivos. Ou seja, um dispositivo não conhece os *links* de comunicação de outro e consequentemente não sabe quando e onde coletar dados. O dispositivo tem somente as informações necessárias para o estabelecimento de sua própria comunicação.

Uma abordagem para se resolver essa questão seria permitir que o coletor de dados monocanal capture os anúncios da rede e interprete as mensagens para obter os *links* de comunicação em que os novos dispositivos irão se associar à rede. A partir da escuta destes *links*, o coletor de dados monocanal seria capaz de acompanhar o processo de ajuntamento na rede de novos membros capturando suas mensagens e interpretando-as para descobrir os *links* de comunicação definidos pelo gerenciador da rede para cada um dos

novos integrantes da rede. Entretanto, essa proposta exigiria alto poder de processamento e memória demandando muitos recursos da unidade de coleta de dados. Além do mais, o processo de análise da rede somente poderia ser feito com os dispositivos associados após a inicialização do coletor de dados monocanal.

Uma abordagem alternativa sugerida por esse trabalho é apresentada na Figura 21. Nesta figura são apresentados os dois elementos essenciais para o processo de coleta de mensagens WH a partir da solução com apenas um *transceptor*. São eles: a **unidade coletora de dados** e o **gerenciador da unidade coletora de dados**.

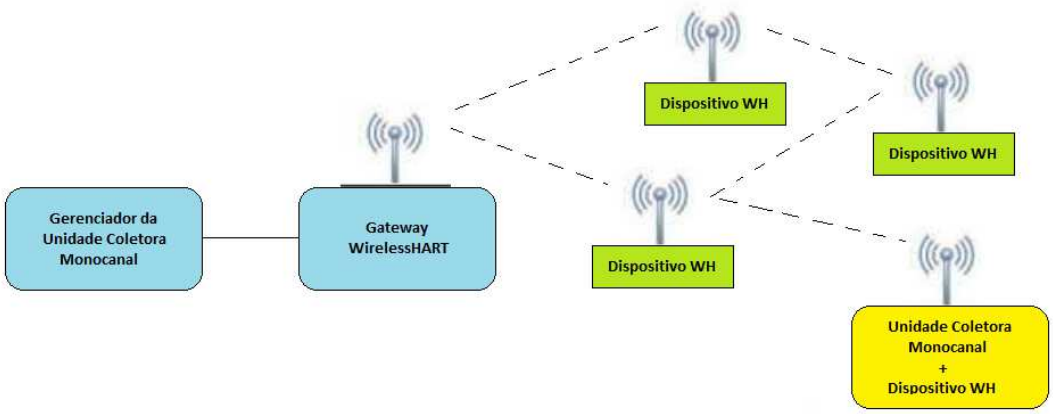


Figura 21: Coletor de dados monocanal integrado a uma rede *Wireless*HART

A unidade coletora de dados proposta nessa abordagem mantém suas características básicas. Isto é, sintonização de canal, captura de mensagens e armazenamento de dados coletados em memória não-volátil. Entretanto, conforme exposto no item 4.3, herda suas funções básicas de uma estrutura de dispositivo de campo. Assim, mecanismos e estruturas básicas de hardware e software passam a ser compartilhados, tornando a unidade coletora uma extensão de um dispositivo de campo com pequenas modificações no *firmware* original.

Há algumas vantagens na extensão do dispositivo de campo para atuar como uma unidade coletora de dados. A vantagem mais significativa nesta associação consiste em aproveitar a estrutura de protocolo WH para envio de comandos para administração remota da unidade. Um destes comandos, de implementação obrigatória por norma nos dispositivos de campo, permite que o gerenciador da rede WH adicione novos *links* de comunicação

nos dispositivos. Como a tabela de *links* de comunicação é compartilhada entre as entidades, a unidade coletora de dados automaticamente passa a obter novas estruturas de dados essenciais ao seu processo de coleta de mensagens. Uma pequena alteração neste comando permite que outras entidades da rede, ou de fora dela, contribuam com o processo de coletora de dados na rede.

Sendo um dispositivo de campo, a unidade coletora de dados somente tem acesso aos seus próprios *links* de comunicação. É de vital importância a obtenção dos *links* de comunicação pertencentes aos dispositivos na vizinhança da unidade coletora, independente de possuir comunicação direta ou não. Como no protocolo WH não há comunicação fim a fim entre dois dispositivos de campo, é necessário uma entidade externa para realizar tal tarefa. E é justamente neste ponto que passa a ter função a segunda entidade proposta na arquitetura da unidade coletora de dados monocanal: o gerenciador da unidade coletora de dados.

Localizado fora dos limites da rede sem fios, o gerenciador da unidade coletora se comunica com cada um dos dispositivos de campo dentro da área de cobertura da unidade coletora de dados. Para cada um dos dispositivos encontrados, o gerenciador obtém informações de *links* e *superframes* utilizados na comunicação do dispositivo acessado com os seus vizinhos. Estas informações são então reunidas em forma de tabelas que precisam ser processadas antes de serem encaminhadas à unidade coletora de dados.

O gerenciador da unidade coletora precisa resolver algumas inconsistências inerentes ao processo de aquisição de dados. Ao obter *links* de comunicação entre dois dispositivos que se comunicam, um transmitindo e outro recebendo dados no mesmo *timeslot*, a duplicidade de informação presente nas tabelas internas do gerenciador deve ser eliminada por um algoritmo posterior. Inteligência também se faz necessária para tratar os *links* de comunicação, convertendo-os para *links* de recepção de *broadcast* antes de enviá-los à unidade coletora de dados. Esta simples manipulação nos dados automaticamente garante que a unidade coletora receberá o dado pois possuirá um *timeslot* de recepção programada como evitará que a confirmação de recepção seja transmitida.

Uma vez que os *links* de comunicação já estejam tratados, o gerenciador deve atualizar

as tabelas internas da unidade coletora. Esse procedimento, que é feito pelo gerenciador da unidade coletora através da escrita *link* por *link* utiliza um comando WH padronizado e amplamente descrito na norma. Entretanto, a restrição para que tal comando seja aceito apenas se forem enviados pelo gerenciador da rede deve ser removida. Após a finalização deste processo, a unidade coletora de dados está apta a iniciar o seu funcionamento normal.

Por ter apenas um *transceptor* de RF, a unidade coletora de dados e o dispositivo de campo devem, de modo colaborativo, realizar suas funções sem que uma entidade interfira nas funções da outra. Nesta estrutura compartilhada, o dispositivo de campo deve percorrer a tabela de *links* de comunicação, calculando e sintonizando os canais para transmissão ou recepção de dados. O correto tratamento, interpretação e decodificação dos dados são também papéis essenciais a serem executados pelo dispositivo de campo para que a comunicação dentro da rede seja mantida. Cabe, por fim à unidade coletora de dados, realizar o processo de coleta e armazenamento dos dados sem causar transtornos temporais na crítica estrutura de tempo imposta pelo protocolo.

4.3.2 Coletor de dados multicanal

Com grau de complexidade inferior, a estrutura do coletor de dados multicanal surge como alternativa. Nessa arquitetura estão presentes 15 *transceptores* de RF que sintonizam cada um dos 15 canais na faixa de frequência de 2.4 GHz. A utilização de apenas 15 canais, suficiente para o processo de coleta de pacotes de dados em redes WH, restringe a arquitetura proposta, tornando-a incompatível para o uso de redes baseadas no padrão 802.15.4. Desta forma, pensando em uma possível extensão a outros protocolos industriais, optou-se por expandir a arquitetura do coletor de dados multicanais proposto nesse trabalho para uma estrutura com 16 *transceptores* paralelos onde, mesmo que o último não tenha função específica no protocolo WH, torna a proposta mais abrangente.

Essa abordagem com múltiplos *transceptores* tem sido frequentemente empregada na análise de redes WH. Apesar dessa solução apresentar custo comparativamente mais elevado que as soluções baseadas em *transceptor* único, é a única que garante coleta simultânea dos dados presentes em vários canais em um determinado instante no tempo.

Esta característica, a princípio desnecessária quando se analisa apenas uma rede, se torna essencial quando várias redes WH coexistem no mesmo ambiente físico.

Outra vantagem dessa abordagem, quando comparada com a unidade coletora de dados monocanal apresentada anteriormente, é que neste caso não há a exigência de elementos externos de gerenciamento. Como não há saltos de canais a serem realizados pela unidade coletora, o conhecimento dos *links* de comunicação se torna desnecessário pois há sempre um *transceptor* pronto capturando a mensagem no ar, independente de que canal ela esteja.

A necessidade de sincronismo com os *timeslots* e precisão nos circuitos osciladores da unidade coletora também passam a ter papel secundário uma vez que, como os *transceptores* estão sempre em modo recepção, o sincronismo exigido para detecção dos *timeslots* não se torna essencial. As mensagem serão sempre recebidas independente do instante no tempo em que elas sejam transmitidas.

Em contrapartida, como não há uma comunicação direta entre cada um dos *transceptores*, mecanismos adicionais devem ser criados com o objetivo de controlar a leitura dos dados capturados e ordenar cronologicamente as mensagens coletados. A presença de uma estrutura central, interna ao coletor de dados, capaz de realizar tais operações é vital para o funcionamento do sistema. A unidade coletora de dados multicanal, com todos os seus elementos, é apresentada na Figura 22.

O primeiro elemento da arquitetura da unidade coletora de dados multicanal é o rádio coletor. Este dispositivo, elemento de captura dos dados, deve realizar as funções de sintonização do canal, conversão de meio físico e armazenamento temporário das informações coletadas. O rádio coletor possui também uma interface de comunicação de alta velocidade, tipicamente SPI, por onde o fluxo de dados deve ser transferido.

Dezesseis rádios coletores são propostos na unidade coletora de dados multicanais. De modo a facilitar a implementação futura, a arquitetura define sinais de controle adicionais que tem por objetivo permitir a configuração do canal a ser observado, controlar o tráfego do fluxo de dados na porta de comunicação e gerar informação de sincronismo para cada um dos rádios coletores. A utilização de sinais de controle nos rádios coletores permite

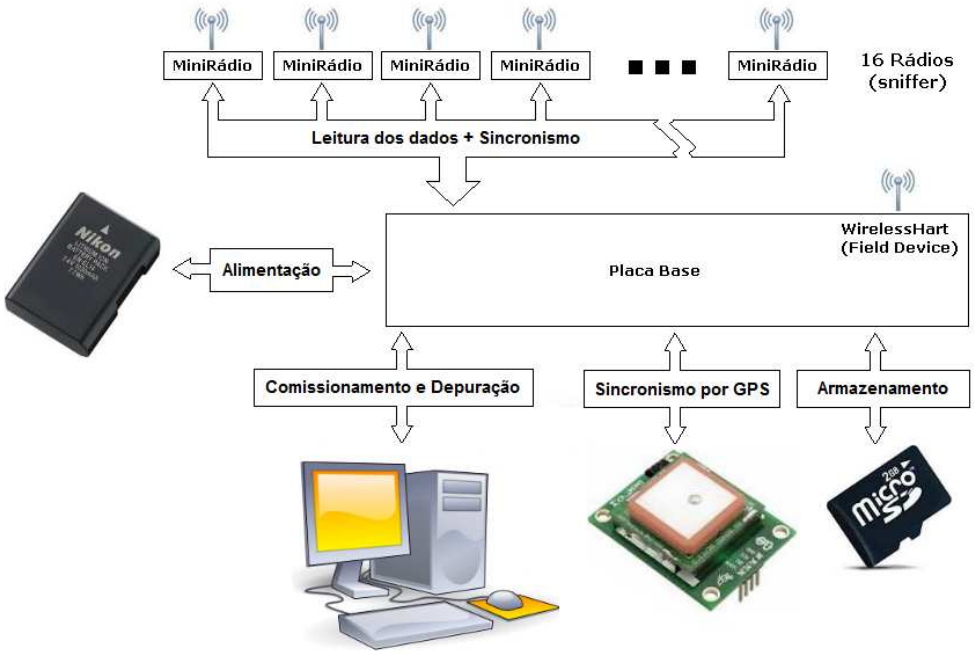


Figura 22: Elementos do coletor de dados multicanal

modularidade de projeto e facilidade de manutenção da solução. A realocação dos rádios coletores é facilitada uma vez que a informação de qual canal sintonizar é uma informação de entrada e não uma constante interna na estrutura de cada um dos rádio coletores.

A coordenação das atividades dos rádios coletores de dados é feita pelo gerenciador da unidade coletora multicanal. Esta entidade, única na arquitetura proposta, é o coração funcional da unidade. Tem por função configurar e coordenar as atividade de comunicação com os rádios coletores para obter as mensagens WH capturadas em cada um dos canais. Atua também no processamento e ordenação dos dados coletados de modo que o armazenamento dos pacotes, em memória não volátil, seja feito conforme ordem cronológica em que foram recebidos nos rádios coletores.

O gerenciador da unidade coletora, assim como ocorre no coletor monocanal, também faz parte da rede WH, entretanto com propósitos distintos. Na unidade coletora monocanal, a associação, na mesma entidade de rede, das funções de análise e de dispositivo de campo carrega consigo benefícios fundamentais para a arquitetura montada. Sem essa associação a unidade coletora de dados monocanal não teria informações suficientes para realizar o seu trabalho.

Na proposta do coletor de dados multicanal, essa associação possibilita vantagens re-

lativamente menos significativas. A possibilidade de monitoração das baterias do sistema, a capacidade de transferência dos dados armazenados na memória não volátil pela própria rede são algumas funções que podem ser implementadas aproveitando a estrutura de comandos WH. Outra vantagem nessa estrutura é a possibilidade de captura das chaves criptográficas da redes de modo automático.

Do ponto de vista funcional, todo o tráfego de dados WH é capturado pelos rádios coletores. O sincronismo entre os rádios coletores é garantido por um sinal de controle, enviado pelo gerenciador, a cada um dos rádios coletores. Este sinal deve ser monitorado para que uma marca temporal seja mantida constante em todo o sistema. Nos rádios coletores, após a recepção dos dados, a marca temporal é adicionada ao fluxo de dados que deve ser armazenado localmente à espera da comunicação a ser comandada pelo gerenciador da unidade de coleta de dados multicanal.

Periodicamente, o gerenciador da unidade coletora deve fazer uma varredura em cada um dos rádios coletores. Caso exista apenas uma rede WH e essa varredura seja feita em todos os canais dentro de um período de 10 ms, apenas uma mensagem WH será capturada. Caso contrário, o fluxo de dados lido, acompanhado da marca de tempo, deve ser ordenado. A etapa posterior ao processo compreende o armazenamento em memória não volátil dos dados. O modo como os dados serão formatados e gravados na memória não volátil é uma função da unidade analisadora utilizada. Deste modo, a escolha da unidade analisadora de dados influencia diretamente no projeto do sistema coletor de dados.

4.4 Unidade analisadora de dados

Para realizar as atividade de interpretação e decodificação das mensagens WH capturadas pela rede, se torna essencial o desenvolvimento de uma ferramenta de análise de dados. Muitas são as abordagens observadas na literatura para desempenhar desse papel. O trabalho desenvolvido por (MRAZ et al., 2011), baseado em redes padrão IEEE 802.15.4, propõe que a análise dos dados seja feita através do módulos adicionais a serem acrescentados no software *Wireshark*. O trabalho realizado por (KOUBAA et al., 2011)

implementa sua própria ferramenta de análise de redes com o cuidado de torná-la extensível a partir da implementação de classes de interpretadores de protocolos permitindo futura expansão.

A abordagem utilizada neste trabalho segue a mesma linha da reutilização de ferramentas já desenvolvidas. Assim, a proposta feita em (KUNZEL, 2012), que tem foco específico na análise de roteamento de rede WH, se torna uma opção promissora. O objetivo principal foi analisar as estratégias de roteamento da rede WH através de algoritmos implementados em um software. Um dos meios propostos no trabalho para a obtenção das mensagens trafegando na rede WH é a utilização do analisador de redes *Wi-Analys* que coleta os pacotes de dados no ar e os armazena em arquivo texto. A ferramenta de análise de redes WH proposta por (KUNZEL, 2012) foi a opção escolhida como unidade analisadora de dados para a integração com este trabalho.

O formato do arquivo de importação a ser gerado pela ferramenta é um arquivo texto, em formato ASCII, onde os dados são separados por vírgula. A configuração dos campos a serem mostrados é dependente das configurações de filtragem feitas na interface gráfica do *Wi-Analys*. O trabalho desenvolvido por (KUNZEL, 2012) definiu alguns campos essenciais a serem filtrados na aquisição feita pelo *Wi-Analys*. Destes campos, o canal físico recebido, o pacote em formato RAW e o índice da coleta de pacote são essenciais.

A ferramenta proposta por (KUNZEL, 2012) carrega o arquivo texto gerado pelo *Wi-Analys*, interpreta os comandos presentes dentro do pacotes de dados WH e monta grafos de comunicação, topologias de rede e informações referentes à vizinhança dos dispositivos de campo. Através de uma interface gráfica, também é possível analisar as estruturas de *superframes* e *links* de comunicação entre os dispositivos. Todas estas etapas implementadas pelo *software* de análise são representadas na Figura 23

A utilização de arquivos texto na importação dos dados da ferramenta facilita o processo de integração. As unidades coletoras de dados presentes nesse trabalho apenas geram os arquivos de coleta, em formato texto, utilizando a estruturas similares ao padrão exigido pelo sistema de análise desenvolvido por (KUNZEL, 2012). A captura e interpretação continua sendo feito de modo transparente pela unidade analisadora.

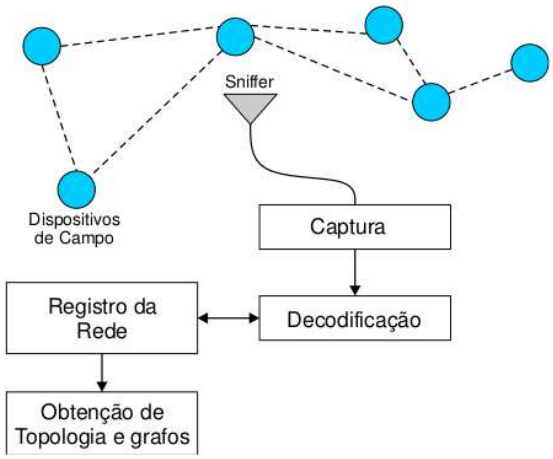


Figura 23: Etapas do processo de análise proposto por (KUNZEL, 2012)

Outra vantagem dessa integração está no fato da expansão da ferramenta de análise. Uma vez que todo o processo de interpretação, decriptografia e análise do software já foi desenvolvido em linguagem de alto nível, a adição de novas funcionalidades é facilitada e beneficia a expansão do sistema proposto.

4.5 Análise comparativa entre as abordagens propostas

Uma das características de uma rede WH é que apenas um de todos os quinze canais definidos para o espectro de 2.4 GHz pode ser utilizado simultaneamente no mesmo instante de tempo. A implicação desta imposição da norma WH é que, na mesma rede WH, não há mais do que uma única comunicação entre dois dispositivos de rede ao mesmo tempo. Desta forma a abordagem monocanal, que apresenta *hardware* otimizado para esta situação, se tornando a opção mais adequada. Entretanto, quando mais de uma rede WH precisa ser estudada, a utilização de uma abordagem multicanal se faz necessária uma vez que a unidade coletora de dados monocanal não possui transceptores suficientes para coletar dados em dois canais no mesmo instante de tempo.

Outra desvantagem da abordagem monocanal quando comparada com a multicanal é a necessidade de uma entidade gerenciadora externa. Essa entidade, que periodicamente se comunica com os dispositivos de campo na vizinhança da unidade coletora monocanal, tem papel fundamental no processo de escrita dos *links* de escuta necessários ao correto funcionamento do sistema. Sem essa entidade, apenas os pacotes de dados recebidos

ou transmitidos pela unidade coletora de dados poderiam ser utilizados no processo de análise da rede.

O processo de obtenção dos *links* de comunicação com os dispositivos de campo realizado pelo gerenciador da unidade coletora monocanal também reduz a banda de comunicação de dados da rede WH. Neste processo, onde o gerenciador envia mensagems HART-IP ao *gateway* e este as reencaminha aos dispositivo de campo, os *timeslots* de comunicação são ocupados para leitura de *links* de comunicação e *superframes* de cada um dos dispositivos na vizinhança da unidade coletora. O número de *timeslots* utilizados para o gerenciamento na abordagem monocanal é diretamente relacionado à topologia da rede formada. Desta forma, quanto maior o número de nós intermediários entre o ponto de acesso e a unidade coletora, menor a vazão de dados global na rede. De modo similar, o aumento do número de dispositivos na vizinhança da unidade coletora de dados monocanal também deteriora o desempenho geral da rede.

Entretanto, a abordagem monocanal também apresenta vantagens. A possibilidade de ser facilmente implementada a partir de um *firmware* de dispositivo de campo e a reutilização de *hardware* já concebido causa uma redução dos custos de desenvolvimento da nova ferramenta. A otimização das dimensões físicas da proposta monocanal também permite que o dispositivo seja instalado em pontos de difícil acesso no chão de fábrica. Em comparação com a abordagem multicanal, seu custo é mais baixo e o consumo de baterias menor resultando em um maior tempo de coleta de dados em campo.

4.6 Síntese do capítulo

Neste capítulo foi apresentada a estrutura do analisador de dados WH proposto onde duas abordagens foram discutidas. A primeira, baseada em uma estrutura monocanal, utiliza a própria rede sob observação para receber os parâmetros necessários para a sua operação através de elemento gerenciador externo à rede sem fios. Uma segunda abordagem foi apresentada, onde são utilizados diversos *transceptores* para coleta paralela em todos os canais definidos pelo protocolo. Em seguida, foi definida a ferramenta utilizada para realizar a análise dos dados capturados. O capítulo foi finalizado fazendo uma análise

comparativa entre as duas estruturas propostas nesse trabalho.

5 IMPLEMENTAÇÃO E RESULTADOS

Neste capítulo, as implementações das duas propostas de unidades coletoras de dados desenvolvidas nesse trabalho são apresentadas. Inicialmente, a implementação da unidade coletora monocanal é abordada. São apresentados o hardware utilizado e as modificações necessárias a serem feitas para que as atividades de coleta de dados da rede WH sejam realizadas. Seguindo o capítulo, detalhes de projeto de hardware da unidade coletora multicanal desenvolvidos são explorados. Finalizando o capítulo, são apresentados os resultados experimentais obtidos deste trabalho.

5.1 Implementação do coletor monocanal

A proposta do coletora de dados monocanal desenvolvida no trabalho exige a implementação de duas entidades distintas que quando executadas de maneira coordenada, tem a capacidade de coletar pacotes de dados capturados no ar. A primeira entidade nessa estrutura é a unidade coletora de dados, que no conceito apresentado no escopo desse trabalho, deve estender suas funções a partir de um dispositivo de campo. Dessa forma, todos os desafios impostos no desenvolvimento de um dispositivo de campo também devem ser levados em consideração durante as etapas de concepção da unidade coletora.

O desenvolvimento de um dispositivo de campo WH envolve o projeto de *hardware* e *firmware* de controle do dispositivo. Do ponto de vista de *hardware*, a frequência de operação na ordem de 2.4 GHz e a precisão de frequência do oscilador exigido para o TDMA são detalhes que precisam ser levados em consideração (MULLER et al., 2010). Duas abordagem poderiam ser seguidas no processo de implementação da unidade coletora de

dados. Destas opções, o desenvolvimento de um *hardware* específico para a unidade coletora seria a alternativa mais trabalhosa e com custo mais elevado. A outra opção, baseada na utilização de *hardwares* de nós sensores já desenvolvidos, agiliza a implementação da solução monocanal.

5.1.1 Hardware da unidade coletora de dados monocanal

O *hardware* utilizado na implementação da unidade coletora de dados monocanal é conhecido como **Namimote**. Conforme descrito em (MULLER et al., 2012) o Namimote foi desenvolvido no escopo do projeto Namitec, para ser utilizado como nó sensor em futuras aplicações utilizando redes de sensores sem fio baseadas no padrão IEEE 802.15.4. O seu projeto foi idealizado para ser utilizado em sensoriamento remoto onde foram previstas funções como: alimentação por baterias, sensores de luminosidade e temperatura, acelerômetro de três eixos e cartão microSD para registro local das informações. O Namimote, com seus componentes principais em destaque, é apresentado, na Figura 24.

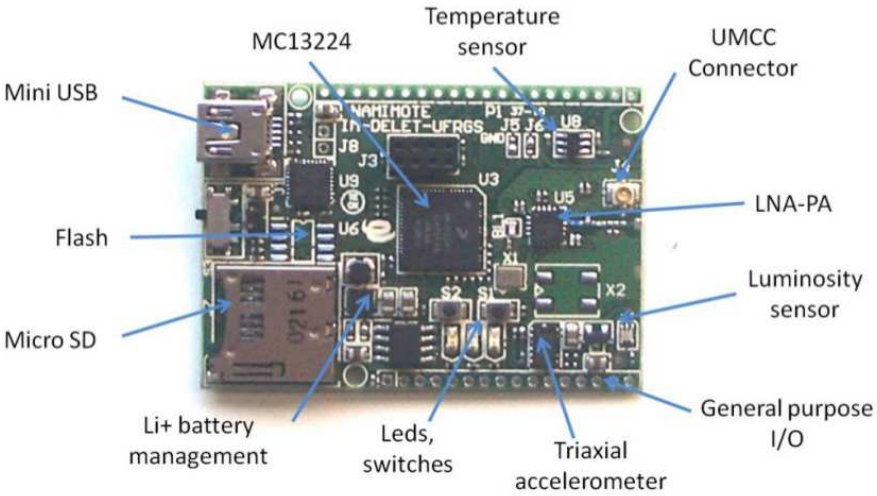


Figura 24: Hardware do namimote (MULLER et al., 2012)

O microcontrolador escolhido para coordenar as funções do namimote é o MC13224 (FREESCALE, 2010), um *System on a Chip* (SoC) da Freescale, que integra duas portas seriais, duas porta SPI, porta I2C e um *transceptor* padrão IEEE 802.15.4. Apresenta núcleo ARM 7 de 32 bits e periféricos adicionais, em *hardware*, para aceleração da MAC e o cálculo do algoritmo de segurança. O sistema ainda é composto por 128 kB de memória flash. Contudo, o *firmware* precisa ser copiado para os 96 kB de memória RAM,

compartilhado entre a área de dados e código, para ser executado.

Do ponto de vista de *hardware*, o Namimote apresenta as características necessárias para sua utilização como unidade coletora de dados, não demandando nenhuma alteração no *hardware*. A presença de cartão microSD para armazenamento local dos dados e alimentação por baterias permitem que o dispositivo tenha mobilidade na rede pois eliminam a necessidade de fios. A integração entre o microcontrolador embarcado e o *transceptor* em um único circuito integrado reduzem o tamanho da solução facilitando seu posicionamento em pontos de difícil acesso em uma planta industrial.

Outro ponto decisivo para a escolha do namimote para utilização como hardware na implementação da proposta da unidade coletora monocanal é o fato do microcontrolador MC13224, núcleo do SoC da Freescale, já ter sido utilizada no desenvolvimento de dispositivos de campo WH anteriormente (MULLER et al., 2010). Assim, a incorporação do *firmware* de controle do dispositivo de campo ao *hardware* do namimote seria simplificado.

5.1.2 O Firmware da unidade coletora de dados monocanal

O *firmware* de um dispositivo de campo é a base sobre a qual foram feitas as alterações necessárias para estender as suas funcionalidades primárias e incluir as rotinas essenciais ao processo de análise da rede WH. O *firmware* base do dispositivo foi desenvolvido em linguagem C utilizando o compilador IAR Embbeded Workbench 5.5 da empresa IAR Systems. Foi estruturado utilizando o sistema operacional CMX, através de 7 tarefas concorrentes, que cooperam nas atividades de comunicação com a rede sem fio e interpretação dos dados, camada a camada, das mensagens recebidas. Uma representação simplificada das interações entre as tarefas implementadas no *firmware* do dispositivo de campo é apresentada na Figura 25.

Das sete tarefas do sistema operacional implementadas no dispositivo, seis delas colaboram para manter as atividades básicas do dispositivo de rede WH. Este conjunto de tarefas, funções e estruturas de dados é chamado de pilha WH. A comunicação entre as tarefas é realizada através de estruturas gerenciadas pelo próprio sistema operacional. Caixas de mensagens e semáforos são algumas estruturas frequentemente utilizadas. A

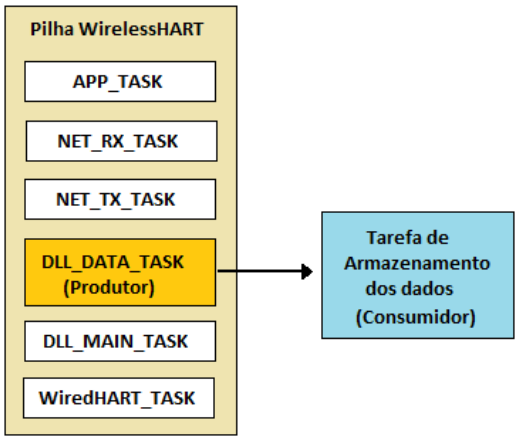


Figura 25: Tarefas concorrentes do *firmware* da unidade coletora

última tarefa na estrutura apresentada na Figura 25 não pertence a pilha WH pois é específica do dispositivo a ser implementado.

A primeira etapa no processo de adaptação do *firmware* tinha como objetivo reimplementar a tarefa específica do dispositivo de campo para realizar o armazenamento dos dados coletados. Neste processo, uma abordagem produtor-consumidor foi utilizada, onde alguns trechos de código da pilha WH foram alterados para atuar como produtores dos dados. Coube à tarefa específica do dispositivo de campo realizar o papel de consumidor dos dados.

Na estrutura da pilha WH, os pontos escolhidos para a implementação dos produtores de dados situaram-se na camada de enlace de dados. Esta camada, responsável pelo sincronismo no TDMA e pela captura de todos os pacotes de dados recebidos e transmitidos pelo *transceptor* de RF, teve sua funcionalidade alterada com o objetivo de cumprir as tarefas de registro de mensagens da rede.

A Figura 26 apresenta os três cenários possíveis que precisam ser capturados pela unidade coletora de dados monocanal. No primeiro cenário, onde um dispositivo qualquer da rede está se comunicando diretamente com a unidade coletora, o ponto 1 indica o instante em que uma mensagem foi recebida pela unidade coletora de dados enquanto o ponto 2 indica quando a unidade coletora finaliza a transmissão do pacote de ACK.

O segundo cenário corresponde ao momento em que a unidade coletora de dados participa ativamente do roteamento de mensagens. Nesse caso, após receber uma men-

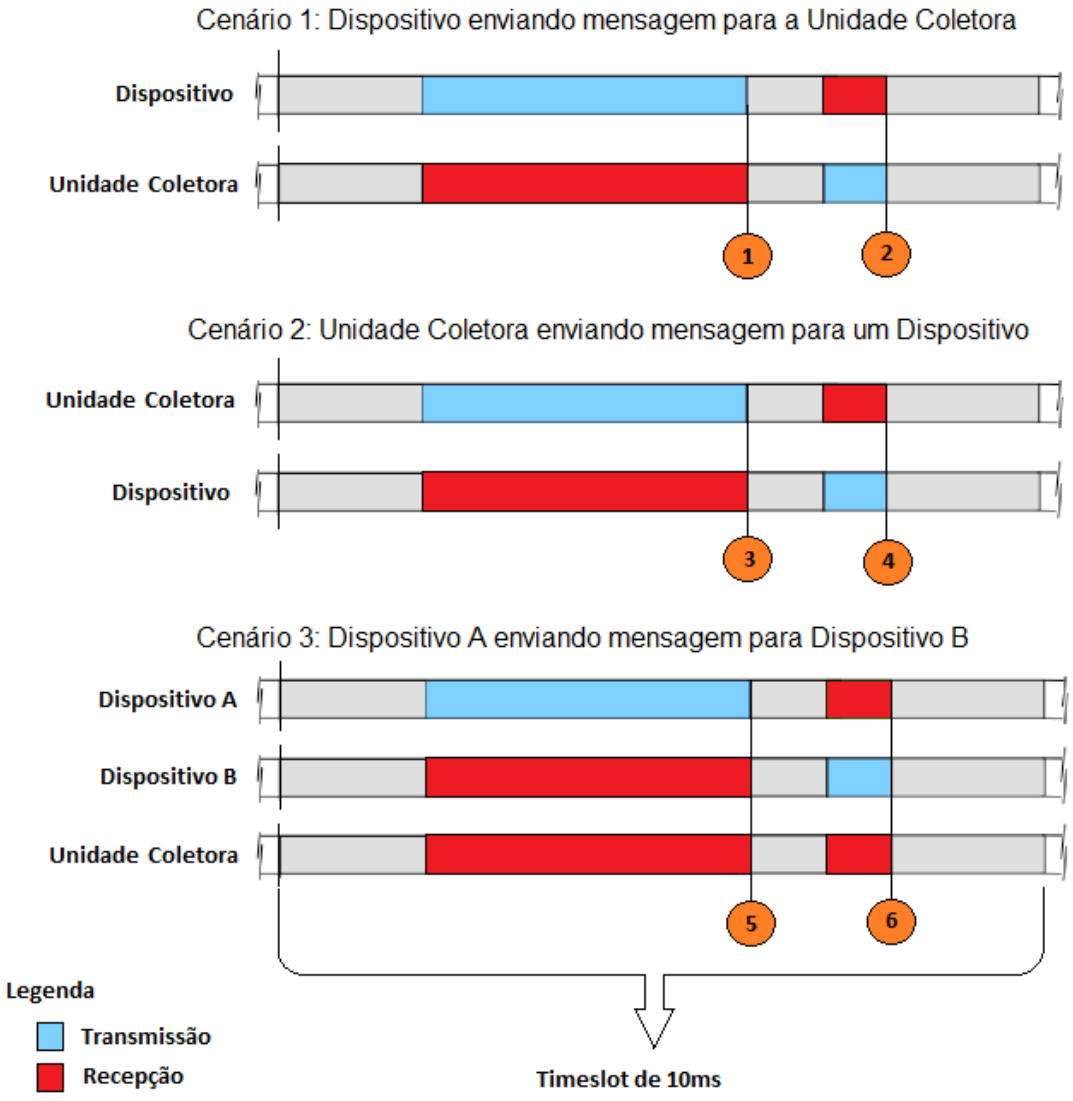


Figura 26: Pontos de captura de mensagens *Wireless*HART

sagem e perceber que essa mensagem não é para si, ela precisa encaminhar os dados ao dispositivo seguinte da rede. Ao final desse processo, indicado pelo ponto 3, a unidade coletora de dados monocanal deve aguardar o fim da recepção do ACK, no ponto 4. Caso o ACK não seja recebido, ela deve reenviar os dados no próximo *timeslot* disponível para comunicação com este mesmo dispositivo de campo.

O último cenário corresponde ao processo de *link* de coleta de dados. Nos dois cenários anteriores, em que a unidade coletora de dados monocanal participa ativamente das mensagens transmitidas pela rede, nenhuma informação adicional é necessária para que a mesma realize suas tarefas de coleta de dados. Entretanto, no terceiro cenário, é essencial a participação do gerenciador da unidade coletora monocanal que programará a unidade coletora para escutar os pontos de interesse, identificados como 5 e 6, sem participar efetivamente da comunicação. Para que o processo de coleta de dados em uma rede WH tenha sucesso é necessário que todos os pontos enumerados na Figura 26 sejam armazenados e isto somente é possível através de alterações na pilha WH.

No ponto 1 da Figura 26 alguns serviços da camada de enlace de dados devem ser chamados para que a mensagem atinja as camadas superiores no modelo implementado. Um dos serviços mais utilizados na estrutura do *firmware* é o serviço de indicação de dados que tem por função realizar a recepção e o correto tratamento de todos os pacotes de dados recebidos pelo dispositivos de campo.

Dentro do serviço de indicação de dados, algumas operações são feitas sobre o pacote de dados recebido. A verificação do identificador do protocolo e da identificação da rede são alguns exemplos. Caso as verificações sejam realizadas com sucesso, o cálculo do MIC em nível de enlace é executado para confirmar a validade da mensagem. Ao final da realização de todas estas operações, os dados recebidos são encaminhados para armazenamento.

Algumas informações adicionais, em nível de camada física e de enlace de dados, obtidas durante o processo de aquisição da mensagem também são encaminhadas. O ASN, canal físico sintonizado, o *Link quality indicator*(LQI) definido pelo padrão IEEE 802.15.4, o *receive signal level*(RSL) do padrão WH e o tipo de mensagem (transmissão

ou recepção) acompanham a mensagem original que é armazenada.

Essa primeira modificação não garante sucesso no processo de coleta de dados para todas as situações previstas no mecanismo de comunicação do protocolo conforme apresentado na Figura 26. A implementação anterior resolve apenas a captura dos dados nos pontos 1 e 4, onde pacotes de dados (ou confirmação de entregas) são recebidos pela unidade coletora de dados. Entretanto, os demais pontos ainda permanecem sem serem coletados.

A partir de uma análise da Figura 26, pode-se perceber que os pontos 2 e 3 correspondem a todos as mensagens, sejam dados ou ACK, enviados pela unidade de coleta de dados monocanal. Desta forma, a função responsável pela transmissão também foi alterada. Seguindo a mesma lógica de implementação onde o tempo de processamento dos dados não pode ser significativo, o *firmware* foi alterado para registrar o pacote de dados a ser transmitido, o canal, o tipo e o ASN da mensagem. Apesar dos parâmetros LQI e RSL continuarem existindo na chamada da função de produção dos dados, eles foram passados como constantes (zero) uma vez que são irrelevantes durante a etapa de transmissão da mensagem.

Como os *links* de escuta foram programados como *links* de recepção de *broadcast* pelo gerenciador da unidade coletora de dados monocanal e enviados à unidade coletora de dados, o ponto 5 indicado Figura 26 automaticamente foi coberto. Entretanto, um mecanismo adicional precisa ser desenvolvido para que as mensagens indicadas pelo ponto 6 também possam ser capturadas. Diferente do que ocorre com o *firmware* original, o dispositivo deve verificar o tipo de mensagem recebida e, se for uma mensagem de dados, se auto-reprogramar para escutar a confirmação da mensagem a ser recebida na sequência. As alterações envolvidas neste ponto foram as mais significativas pois exigiam a reconfiguração da máquina de estados e *timers* internos do *firmware*. Uma vez implementada, a recepção da confirmação da mensagem ocorre naturalmente como se fosse uma confirmação de mensagem para a própria unidade coletora de dados.

Um processo essencial na análise de rede WH é a captura das chaves criptográficas utilizadas na criptografia das mensagem em nível de rede. Sem o conhecimento das cha-

ves utilizadas na criptografia na parte de dados do NPDU, a unidade de análise de rede não consegue decifrar os comandos sendo enviados aos dispositivos de rede. Um dos modos de obter estas chaves é através do acompanhamento do processo de ajuntamento de novos dispositivos na rede.

Para garantir que todas as chaves necessárias ao processo sejam coletadas, é fundamental que a unidade coletora de dados monocanal seja o primeiro dispositivo a ingressar na rede. Durante o processo de ajuntamento na rede, o dispositivo de campo captura e analisa o pacote de anúncio para obter os *superframes* e os *timeslots* por onde o dispositivo deve iniciar o processo de ingresso na rede. No *firmware* original, estes *links* são incluídos nas tabelas internas do dispositivo de forma temporária. Na alteração realizada no *firmware* da unidade coletora eles foram mantidos de modo permanente. Cabe ressaltar que esta alteração foi observada posteriormente, durante a etapa de ensaios da solução, para remover uma limitação imposta pelo gateway utilizado nos teste que não permitia a leitura dos *links* de comunicação do ponto de acesso atráves do gerenciador da unidade coletora.

A passagem das mensagens capturadas entre o produtor, representado pela camada de enlace de dados, e o consumidor, implementado em uma tarefa, ocorria através da chamada de uma função em linguagem C. Como a camada de enlace de dados tinha a maior prioridade no sistema, o processamento dentro da rotina de interface deveria ser enxuta para não penalizar o sincronismo do sistema. Desta forma, apenas são executados cópia de áreas de dados (memcpy) entre as estruturas de controle dos buffers internos do consumidor e os parâmetros passados na chamada da rotina pelos produtores de dados.

O fluxograma do consumidor é apresentado na Figura 27. Seu funcionamento foi implementado através de um laço fechado que verifica se a primeira posição do buffer intermediário está livre ou não. Caso dados sejam detectados, um processo de conversão se iniciariam traduzindo as mensagens binárias recebidas para seus valores ASCII correspondentes a serem armazenados em arquivos textos. Ao final do processo, a mensagem no buffer é liberada. O desmembramento da solução em um problema produtor-consumidor trouxe benefícios temporais na solução, entretanto, gerou aumento do uso de mémoria na

implementação. Esse incremento na alocação de memória causou alguns transtornos, e em casos mais extremos, inviabilizou o processo de compilação do *firmware*. Algumas configurações adicionais precisaram ser alteradas.

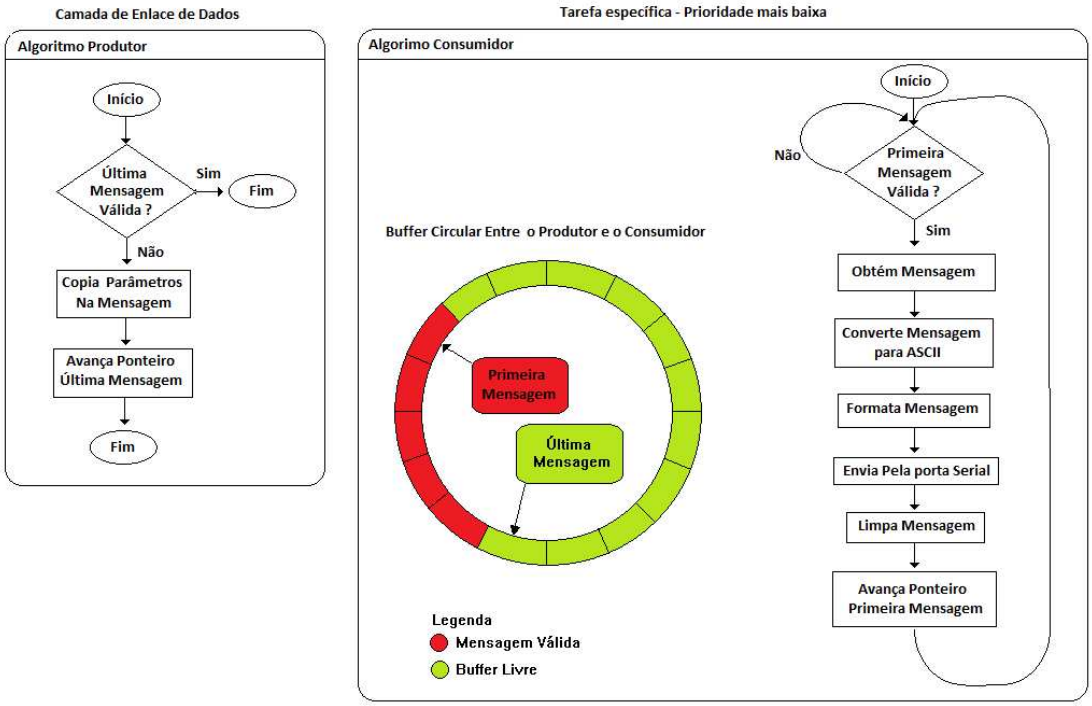


Figura 27: Fluxogramas do produtor e consumidor implementado

O comando 777, identificado como *read device capabilities*, define uma série de parâmetros que são passados ao gerenciador da rede no momento em que o dispositivo quer se associar à rede. Alguns destes parâmetros são o número máximo de buffers de comunicação e o número máximo de vizinhos com que o dispositivo de rede consegue se comunicar. Estes dois parâmetros estão diretamente relacionados à memória RAM utilizada no tratamento dos pacotes de dados e no tamanho das tabelas internas do dispositivo.

Na implementação do comando 777 no *firmware* da unidade coletora de dados monocanal, o parâmetro de número máximo de vizinhos foi reduzido para 1 de forma que o dispositivo entre na rede WH mas não participe ativamente no processo de roteamento de pacotes. O segundo parâmetro alterado foi o número máximo de buffer, que foi reduzido para 8, liberando mais buffers para as atividades da unidade coletora de dados.

Outra alteração com o objetivo de aumentar memória e processamento da unidade coletora envolveu em desabilitar os modos de depuração e o modo Burst. Nos dois casos,

a intenção foi preservar recursos para a inclusão das biliotecas de manipulação do cartão microSD. Entretanto, tais alterações não foram suficientes e o dispositivo não pode salvar as informações diretamente no cartão SD. Apesar do porte das bibliotecas da porta SPI, do cartão SD e do sistema de arquivos FAT terem sido feitos com sucesso, os buffers necessários à leitura e escrita dos dados exigiram blocos contínuos de 512 bytes que inviabilizaram a solução quando compiladas conjuntamente com as funções de coleta de dados. De forma a dar continuidade ao trabalho, a tarefa desenvolvida para atuar como consumidor de dados foi modificada para transferir os dados coletados pela porta serial onde um software externo os capturava e os armazenava em arquivos para posterior análise. Não se descarta, em uma evolução natural do trabalho, que um outro namimote capture o fluxo de dados na porta serial e os armazene efetivamente em memória não volátil para permitir sua utilização em campo.

Apesar das alterações executadas no *firmware* do dispositivo de campo para a implementação da unidade coletora de dados, a solução de coleta de dados monocanal não está completa. Uma unidade coletora de dados monocanal, por si, consegue se associar a rede e capturar suas próprias mensagens. Para que o dispositivo colete pacotes de dados transmitidos pelos vizinhos é necessário informações adicionais enviadas pelo gerenciador da unidade coletora de dados.

5.1.3 O Gerenciador da unidade coletora de dados monocanal

O gerenciador da unidade coletora é um *software* desenvolvido em linguagem C usando o compilador Visual Studio 2008 para ser executado em microcomputador utilizando o sistema operacional Windows. Tem a função de buscar os *links* de comunicação de cada um dos vizinhos e reencaminhá-los à unidade coletora de dados. Para isso, o *software* necessita de um acesso à rede WH através das interfaces de comunicação disponibilizadas por um *gateway* WH.

O *gateway* WH utilizado nesse trabalho é o Emerson Smart Gateway modelo 1420a apresentado na Figura 28. Ele possui interfaces de comunicação RS485 e duas portas Ethernet. Nestas interfaces são disponibilizados os protocolo ModBus e HART-IP para comunicação com os dispositivos da rede sem fios. O software do gerenciador da unidade

coletora de dados monocanal foi desenvolvido para se comunicar atráves da porta Ethernet utilizando o protocolo HART-IP.

Figura 28: Gateway *Wireless*HART 1420A

O *software* foi construído de modo que sua operação seja autônoma. Isto é, nenhuma intervenção do usuário é necessária. O console do sistema foi utilizado exclusivamente como meio de depuração do software. Essa abordagem permite que futuramente a solução possa ser facilmente migrada para o conceito de um serviço sendo executado em qualquer microcomputador da planta do chão de fábrica desde que o mesmo tenha liberação de acesso às interfaces do *gateway* WH.

As configurações necessárias para a execução do software são mínimas. A parametrização da inicialização do software consiste apenas em ajustes na configuração de IP e porta para acesso ao *gateway* além de informar o identificador único da unidade coletora de dados monocanal definida no *firmware* da unidade coletora. Estes parâmetros foram definidos como constantes dentro do *software* desenvolvido.

As rotinas responsáveis pelas tarefas de envio, recepção e tratamento dos pacotes UDP para o *gateway* WH utilizando o protocolo HART-IP foram reaproveitadas dos trabalhos realizados por (WINTER et al., 2011). Entretanto, alguns novos comandos precisaram ser

desenvolvidos para que os *links* e *superframes* coletados pudessem ser enviados à unidade de campo.

O gerenciador da unidade coletora foi implementado em um único processo onde a cada comando enviado ao *gateway*, o processamento ficava bloqueado aguardando uma resposta. Para evitar que o dispositivo permanecesse bloqueado indefinidamente, um *timeout* de 60 segundos foi implementado para cancelar a operação. Neste caso, a máquina de estados de comando era reiniciada automaticamente para seu estado inicial. A visão geral de todas as etapas implementadas no *software* é mostrada na Figura 29.

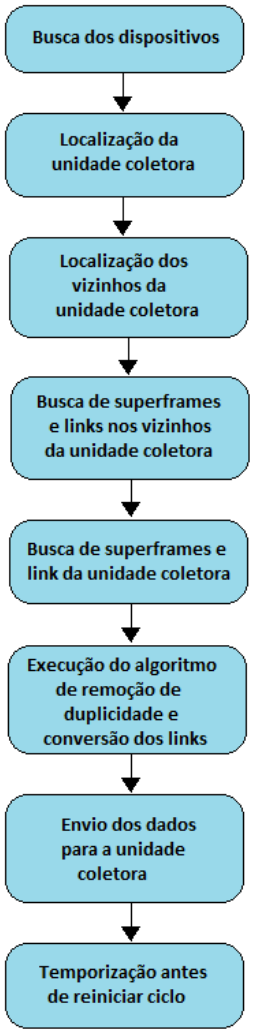


Figura 29: Fluxograma implementado do gerenciador da unidade coletora monocanal

O primeiro estado implementado realiza a operação de descoberta de todos os elementos presentes na redes WH. O comando utilizado para essa tarefa foi o comando 814 da

norma WH. Este comando, encaminhado ao *gateway* retornava todos os dispositivos de campo ativos com seus respectivos identificadores únicos. Estes dispositivos, e seus identificadores, eram armazenados em uma tabela chamada de dispositivos ativos. É neste ponto que o gerenciador da unidade coletora determina se a unidade coletora de dados está ou não presente na rede sem fio. Caso não a encontre, o *software* reenvia o comando.

Ao localizar a unidade coletora de dados, o próximo estado é atingido. Neste estado, o *software* do gerenciador percorre a tabela de dispositivos ativos e envia para o *gateway* o comando 832 passando como parâmetro o identificador único do dispositivo. No retorno do comando, é enviado o apelido (*nickname*) que complementa as informações da tabela de dispositivos ativos. Esse passo é essencial uma vez que o HART-IP exige que os comandos sejam enviados utilizando o identificador único mas as informações coletadas sempre referenciam os vizinhos através dos apelidos. De modo simplificado, a montagem dessa tabela garante uma conversão rápida entre identificadores únicos e apelidos de todos os dispositivos da rede.

O próximo passo do *software* do gerenciador é enviar, diretamente à unidade coletora, dois comandos. O primeiro é o comando 780 que retorna todos os dispositivos com os quais a unidade coletora tem *links* de comunicação. O segundo comando enviado é o 787 que indica todos os dispositivos descobertos na vizinhança da unidade coletora de dados e que não se comunicam diretamente com ela. A reunião das respostas destes dois comandos define quais dispositivos estão na área de cobertura da unidade coletora de dados monocanal e, indiretamente, informam quais dispositivos a unidade coletora de dados consegue acompanhar a comunicação. Os dados obtidos são também armazenados em tabelas. Essa é chamada de tabela de dispositivos na vinhança.

O gerenciador da unidade coletora percorre a tabela de dispositivos na vizinhança e envia, para cada um deles, os comandos 783 e 784 que obtém como resposta a lista de *superframes* e *link* dos dispositivos vizinhos à unidade coletora de dados. Duas tabelas são geradas. A primeira é chamada de tabela de *superframes* da vizinhança e contém as informações referentes aos *superframes* conhecidos pelos dispositivos no entorno da unidade coletora de dados. A outra tabela, chamada de tabela de *links* da vizinhança, atua arma-

zenando todas as informações obtidas no processo de leitura dos *links* nos dispositivos dentro da área de cobertura do coletor.

Duas tabelas ainda precisam ser preenchidas: a tabela de *superframes* e a tabela de *links* da unidade coletora de dados monocanal. O preenchimento segue a lógica anterior onde são enviados os comandos 783 e 784 para o coletor de dados. Ao final desse processo, o algoritmo de seleção de *superframes* e *link* a serem escritos na unidade coletora é executado.

O algoritmo de seleção dos dados percorre as tabelas de *links* e *superframes* dos dispositivos na vizinhança e as tabelas de *links* e *superframes* da unidade coletora removendo dados duplicados, comparando diferenças entre as tabelas e gerando duas novas tabelas: a tabela de *superframes* e a tabela de *links* a serem escritos na unidade coletora de dados. Três parâmetros são alterados nos links antes do envio à unidade coletora: O tipo do *link* é configurado como *broadcast*, o *link* é definido como de recepção e o destino do *link* é configurado como 0xFFFF. O processo é finalizado com o envio das informações obtidas à unidade coletora através do comando 967. Um resumo da sequência de comandos enviados neste processo é apresentado na Figura 30.

O *software* do gerenciador da unidade coletora de dados realiza estes passos ciclicamente, com intervalo constante de 30 segundos entre cada interação. Caso todas as informações coletadas no ciclo anterior não sejam alteradas, apenas as etapas de leitura são realizadas.

5.2 Implementação do coletor de dados multicanal

A abordagem que tem sido frequentemente utilizada na análise de rede WH é, sem dúvida, a proposta multicanal. Neste proposta, onde diversos *transceptores* fazem a varredura dos canais de forma paralela, o reaproveitamento de um *hardware* já concebido não é uma possibilidade. É necessário que o projeto da unidade coletora multicanal inicie a partir do projeto do *hardware* que foi o foco deste trabalho. O *hardware* desenvolvido para essa função se baseou no projeto de *hardware* de duas placas que se interconectam. A primeira, projetada de maneira modular, foi chamada de **rádio coletor**. Dezesseis rá-

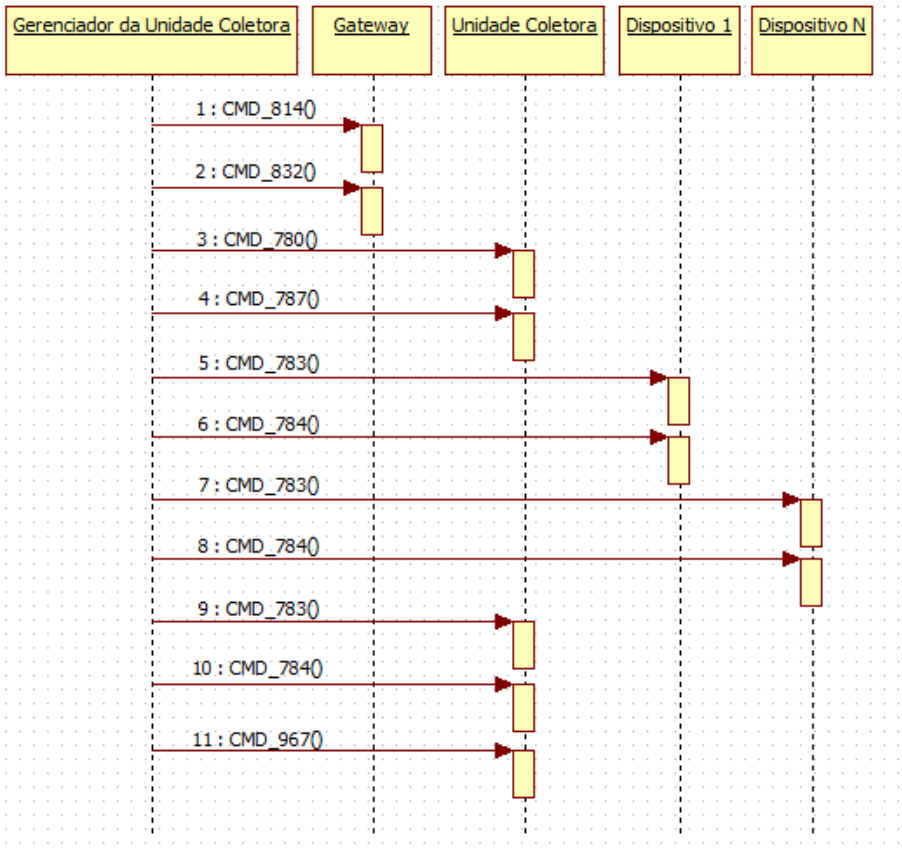


Figura 30: Sequência de comandos executados pelo gerenciador da unidade coletora monocanal

dios coletores se conectam à segunda placa desenvolvida que foi chamada de **placa base** da unidade coletora de dados multicanal.

O rádio coletor é o elemento que faz a conversão dos sinais eletromagnéticos para sinais digitais utilizados no sistema. A estrutura de hardware do rádio coletor é composta basicamente pelo microcontrolador MC13224 da Freescale, uma antena PIFA (FREESCALE, 2006) impressa na placa de circuito impresso e um único conector para comunicação com a placa base da unidade coletora de dados multicanal. Por esse conector, o rádio coletor recebe a alimentação, alguns pinos de endereçamento com a definição de qual canal o rádio deve sintonizar, o sinal para sincronização entre os rádios coletores e a interface SPI para leitura dos dados coletados. O rádio coletor atua como escravo SPI, enquanto que o microcontrolador da placa base da unidade coletora de dados multicanal é o mestre.

O microcontrolador do rádio coletor deverá ser configurado, por *firmware* a ser desenvolvido, para modo recepção fazendo com que ele capture todos dados que estejam na frequência sintonizada. O canal a ser coletado é obtido através de 4 fios de endereçamento definidos pela placa base e enviados ao rádio coletor através do conector de interligação dos dois sistemas. Desta forma, o desenvolvimento do *firwmare* do rádio coletor seria único uma vez que a configuração de canais ocorreria através do *hardware*. Outra implicação desse fato é que o canal a ser observado pelo rádio coletor está diretamente relacionado à posição física em que ele fosse ligado no sistema. Para a troca de canais entre rádios basta trocar seu posicionamento. Caso seja necessário desabilitar algum rádio, o mesmo deve ser desconectado do sistema.

Ao receber um pacote de dados pela antena PIFA, o *firmware* deverá armazená-lo em memória temporária para aguardar comunicação na porta SPI gerenciada pela placa base. O projeto de *hardware* do rádio coletor desenvolvido neste trabalho é apresentado na Figura 31.

A placa base é o coração do dispositivo de campo WH com analisador de rede multicanal integrado. Nela são conectados os 16 rádios coletores. A Figura 32 mostra seus componentes principais.

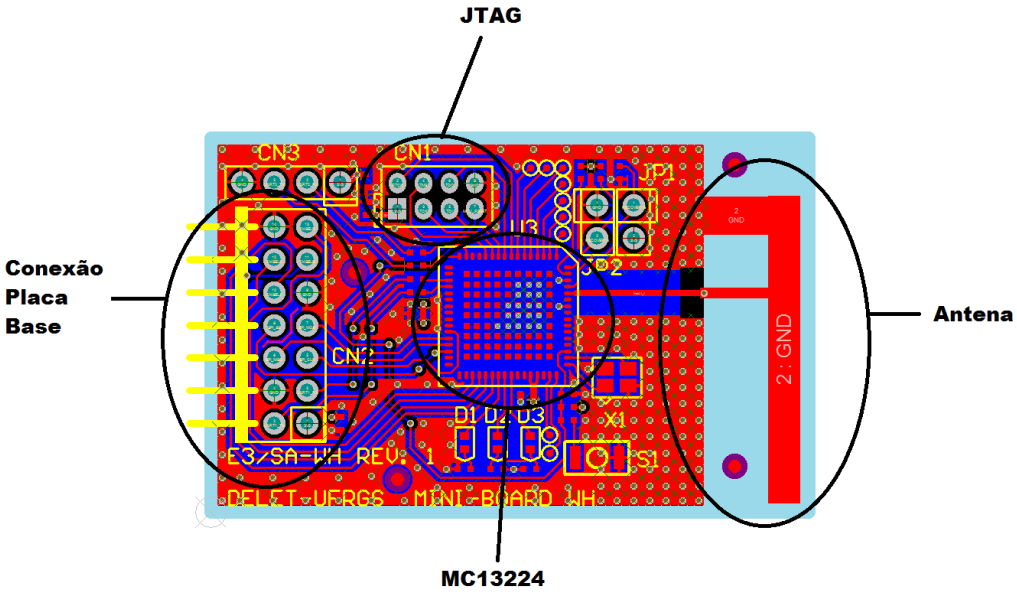


Figura 31: Projeto de hardware do rádio coletor

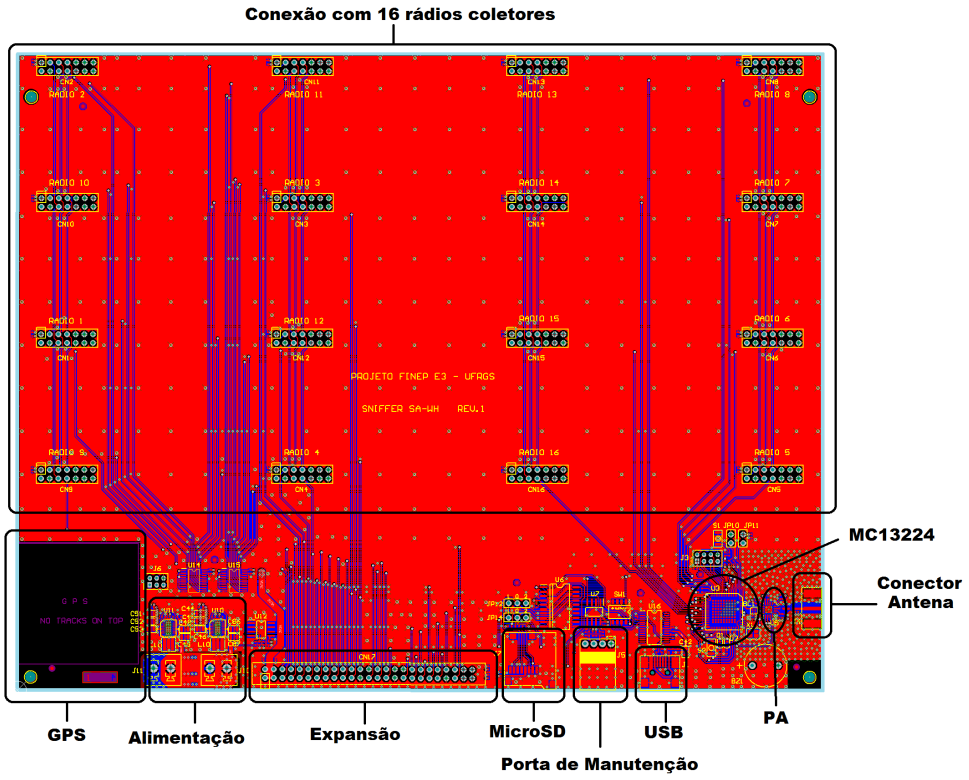


Figura 32: Diagrama de blocos da placa base do coletor multicanal

a) **Módulo de alimentação**: Composto por dois reguladores de tensão, sendo o primeiro responsável pela alimentação do microcontrolador e circuitos adicionais da placa base e o segundo, pela alimentação dos rádios coletores. O microcontrolador pode ligar ou desligar a alimentação dos coletores com o objetivo de reduzir o consumo e aumentar a vida útil das baterias, quando não estiver fazendo aquisição de dados da rede.

b) **Módulo de sincronização**: O módulo de sincronização possui um GPS com saída serial e buffers não inversores. O sinal do GPS é encaminhado ao microcontrolador e a todos os outros 16 rádios, atuando como relógio de sincronismo global entre os diversos componentes do sistema. Além da hora GMT, dados como latitude e longitude também podem ser extraídos do GPS, para obtenção do posicionamento geográfico do dispositivo de campo.

c) **Módulo de armazenamento de dados**: Este módulo é composto por um cartão de memória microSD com sistema de arquivos FAT. É o responsável pelo armazenamento local não volátil das informações. O microcontrolador do rádio principal acessa o cartão microSD através da porta SPI para leitura e gravação dos dados.

d) **Módulo de depuração e/ou comissionamento**: É composto por portas USB e RS-485. A interface USB é utilizada para depuração do equipamento enquanto que a porta RS-485 é utilizada para comissionamento, conforme previsto na norma do protocolo WH. Por compartilharem a mesma serial do microcontrolador, são utilizadas micro chaves para troca de função.

e) **Módulo de comunicação WH**: Este módulo é composto pelo microcontrolador MC13224 que tem como função fazer a coleta dos dados de todos os rádios através da porta SPI e armazená-los no cartão microSD. Possui a pilha WH completa, o que possibilita associação na rede, reconhecimento das estruturas de roteamento além de estar apto a receber comandos remotos.

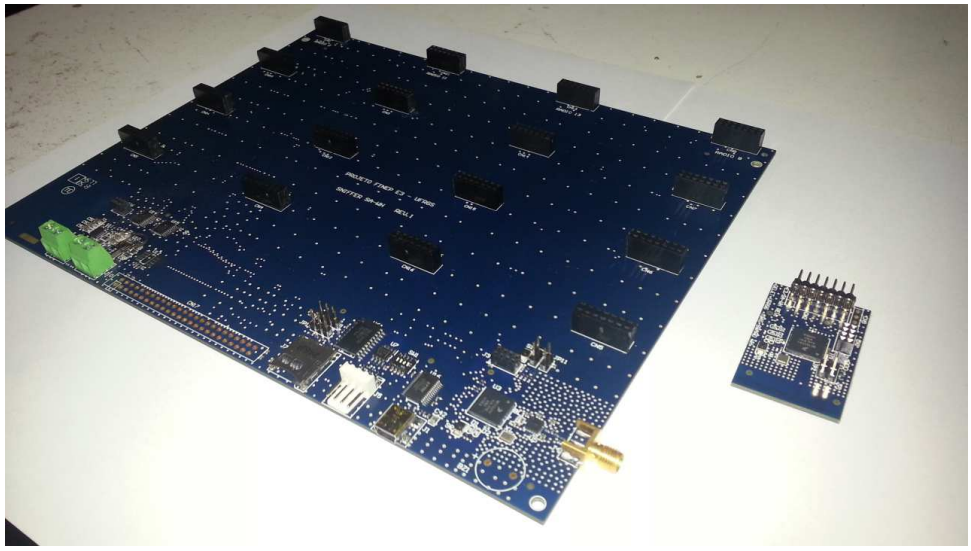
O funcionamento geral da unidade coletora multicanal é controlado pela placa base. É através do seu *transceptor* que o dispositivo de campo se integra a uma rede WH.

O *firmware* de controle da placa base deve gerenciar todas as tarefas de associação à rede, roteamento de pacotes e resposta a comandos sejam pela rede sem fio quanto pela porta de comissionamento. Além disto, deve incluir algumas tarefas adicionais para o gerenciamento do GPS integrado ao sistema, coleta de dados dos rádios coletores e a ordenação e gravação dos dados em cartão micro SD.

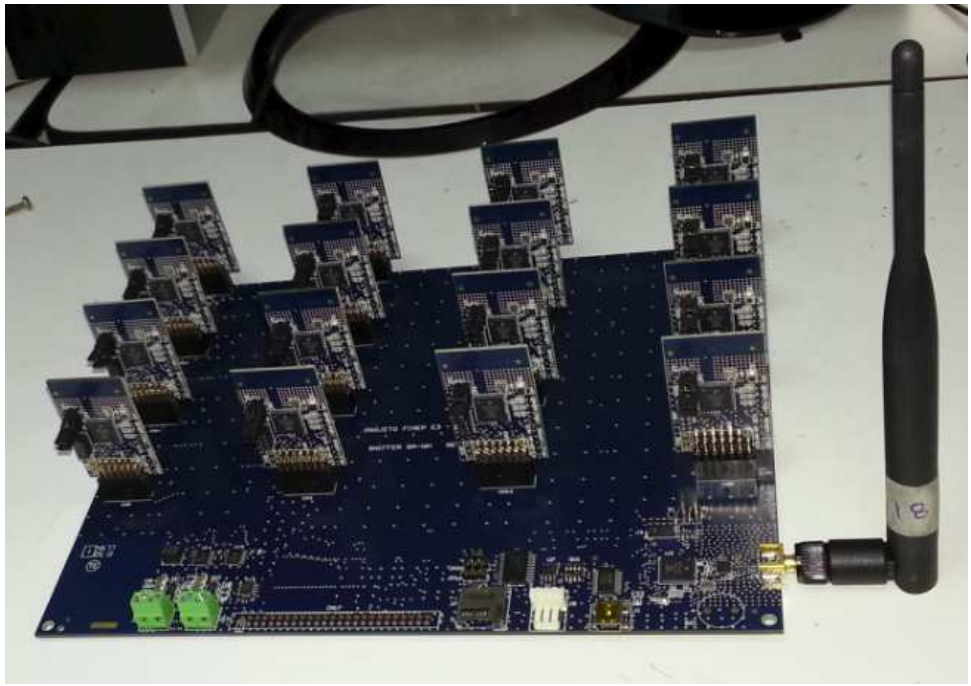
O GPS integrado ao sistema prevê comunicação serial RS232 através de uma conexão a três fios (TX, RX e GND). Desta forma a placa base tem responsabilidade de realizar sua configuração na inicialização do sistema. Como o sinal do GPS é encaminhado a cada um dos rádios coletores através de *buffers* não inversores, o atraso inserido no sinal é mínimo de modo que todos os dados (latitude, longitude, data e hora) podem ser compartilhada com precisão entre todos os elementos do sistema.

A leitura dos dados dos rádios coletores deve ser feito de modo sequencial utilizando o algoritmo *round robin*. Foram definidos 16 sinais de controle (*Chip Select*) para os rádio coletores implementado como escravo SPI. Desta forma, a placa base deve sinalizar com qual escravo SPI quer se comunicar, enviar os pulsos de clock e aguardar a resposta. Caso o rádio coletor não tenha dados a enviar, no caso de não ter coletado dados no canal sintonizado por ele, a comunicação deve ser imediatamente cancelada e a requisição novamente feita ao rádio coletor seguinte.

O projeto do *hardware* das placas dos rádio coletor e da placa base da unidade foi concebido com a utilização de componentes com tecnologia SMD e o layout do projeto foi realizado utilizando placas com 4 camadas de cobre. A Figura 33(a) apresenta as placas fabricadas para o *hardware* da unidade coletora de dados multicanal. Na esquerda é apresentado a placa base enquanto que na direita é exposto o rádio coletor. A montagem completa da solução é apresentada na Figura 33(b).



(a) Placa base e rádio coletor



(b) Unidade coletora de dados multicanal montada

Figura 33: Placas da unidade coletora de dados multicanal

Em função de atrasos nos processos produtivos e na importação dos componentes essenciais à montagem, não foi possível concluir o projeto do *firmware* dentro do prazo de conclusão deste trabalho. Assim, a implementação do *firwmare* de controle da unidade coletora de dados multicanal será desenvolvida em um trabalho futuro.

Outra abordagem a ser dada ao *hardware* da proposta de análise de redes WH multicanal apresentada neste trabalho consiste em realizar alterações nos rádios coletores de modo a alterar sua função principal. Deste forma, ao invés de realizar a tarefa de coleta de dados, os rádios coletores poderiam se transformados em rádios transmissores, com frequência pré sintonizada, capazes de gerar interferências. Este novo dispositivo gerador de interferências poderia ser utilizado em estudos para a avaliação de coexistência entre redes WH como o proposto em (WINTER, 2013).

5.3 Resultados experimentais

Um cenário de testes precisou ser montado para realizar ensaios na proposta do coletor de dados monocanal. Cinco dispositivos de campo foram utilizados nos ensaios: um transmissor de temperatura da Emerson modelo TT648, três rádio protótipos WH descritos em (MULLER et al., 2010) e o namimote utilizado como unidade coletora de dados. Um microcomputador onde o software gerenciador da unidade coletora monocanal foi executado e o *gateway* WH Emerson modelo 1420A também fizeram parte da estrutura necessária à obtenção dos resultados experimentais. Estes equipamentos são apresentados na Figura 34.

Os ensaios foram realizado nas dependências do Laboratório de Sistemas de Controle, Automação e Robótica (LASCAR) da Escola de Engenharia da Universidade Federal do Rio Grande do Sul (UFRGS) e tinham por objetivo avaliar o funcionamento da unidade de coleta de dados monocanal e sua interação com o gerenciador da unidade coletora. A validação da formatação dos dados e a integração com a ferramenta de análise desenvolvida por (KUNZEL, 2012) também estavam no escopo dos testes realizados.

Conforme explicado no item 5.1.2, a implementação da unidade coletora de dados monocanal sofreu com falta de recursos para executar as funções idealizadas na proposta

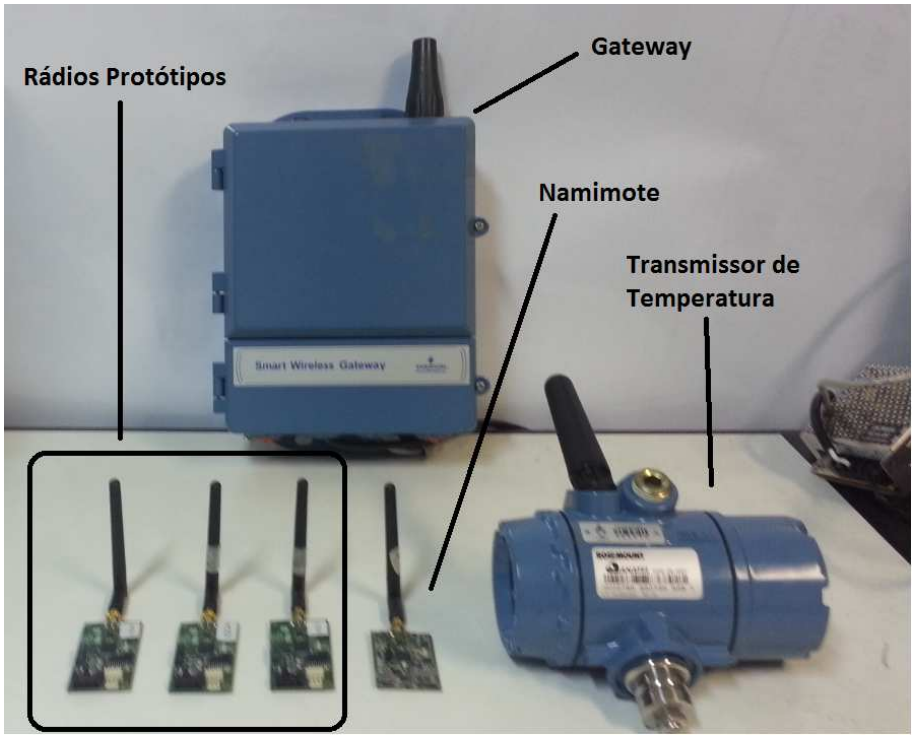


Figura 34: Equipamentos utilizados nos ensaios

do trabalho. As atividades de armazenamento de dados em cartão SD foram substituídas. Em seu lugar, funções de transferência foram desenvolvidas de modo que o fluxo de dados a ser armazenado no cartão SD fosse transferido através da porta serial. Um microcomputador obtinha os dados e os armazenava em arquivo texto. Toda formatação dos dados continuou sendo feita pelo namimote enquanto que o software putty, com a opção de geração de logs habilitada, apenas registrava em arquivo o que ele recebia pela porta serial. O microcomputador, no caso específico deste ensaio, tinha duas funções: unidade de armazenamento de dados e execução do gerenciador da unidade coletora de dados.

O primeiro passo no ensaio foi garantir que nenhum dispositivo WH estivesse ativo na rede. Todos os dispositivos de campo presentes no laboratório foram desligados e o *gateway* reiniciado. Após o reestabelecimento do *gateway*, a unidade coletora de dados foi energizada para iniciar seu processo de ajuntamento na rede WH. Uma vez que a unidade coletora de dados ficou ativa na rede, o software de gerenciamento da unidade coletora foi iniciado. Em seguida, um a um os dispositivos de rede foram energizados para permitir um ajuntamento ordenado na rede.

A medida que os dispositivos de campo se associam à rede, o *gateway* os inclui na

tabela de dispositivos ativos. Como o gerenciador periodicamente se comunica com o *gateway*, os novos dispositivos foram automaticamente incluídos na lista de dispositivos ativos. Esse passo é documentado na Figura 35 onde se percebe 5 dispositivos ativos (*nicknames* 2, 3, 4, 5 e 6) na rede. Um destes dispositivos é a própria unidade coletora identificada pelo *nickname 4*.

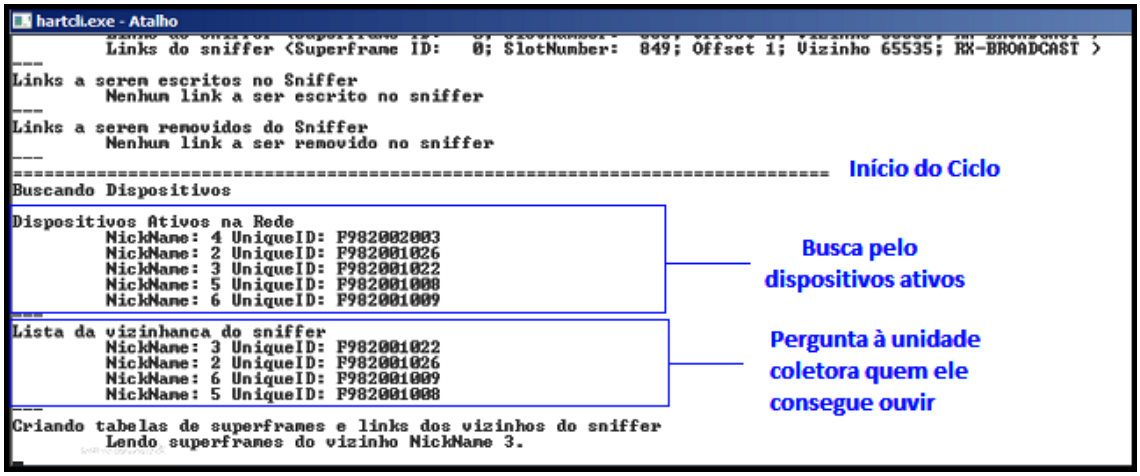


Figura 35: Detecção de dispositivos na rede e vizinhos da unidade coletora

O passo seguinte, ainda documentado na Figura 35, é questionar a unidade coletora de dados monocanal quem ela percebe em sua vizinhança. Desta forma, o gerenciador da unidade coletora apenas programará os *links* de coleta para os dispositivos que a unidade coletora de dados monocanal consegue efetivamente ouvir. Em função da proximidade dos dispositivos de campo utilizados nos ensaios, a unidade coletora de dados conseguiu detectar todos os dispositivos utilizados na rede.

Uma vez que a vizinhança da unidade coletora seja conhecida, o gerenciador da unidade coletora inicia o processo de busca de *links* de comunicação com cada dispositivo visto pela unidade coletora. O resultado obtido pelo gerenciador da unidade coletora a partir da consulta dos *links* de comunicação dos dispositivos identificados pelos *nicknames* 2, 3, 5 e 6 é apresentado na Figura 36. Nesta figura ainda é mostrado o *superframe* a que esse *link* pertence, o índice dentro do *superframe* e o tipo e direção de cada *link* para cada dispositivo.

O próxima passo do fluxograma implementado no gerenciador da unidade coletora consiste em obter os *links* de comunicação da unidade coletora de dados monocanal. Esse

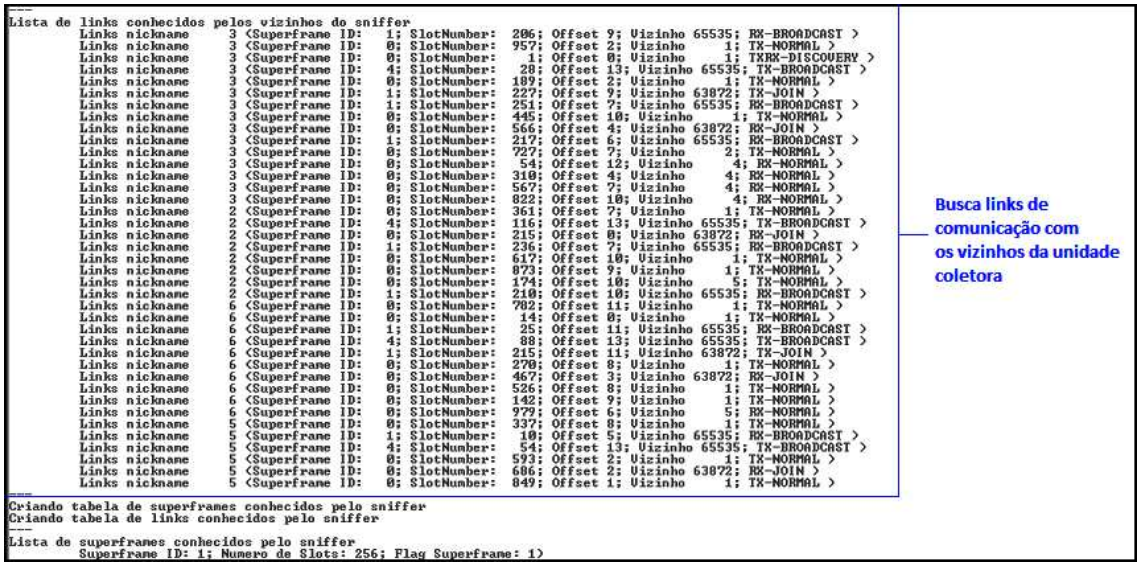


Figura 36: Leitura de *superframes* e *links* na vizinhança da unidade coletora

processo, apresentado na Figura 37, deve ser feito de modo a eliminar duplicidades de dados, antes que o processamento da tabela de *links* seja feito. Após o algoritmo verificar e descartar os dados redundantes e converter os *links* de coleta, inicia-se o processo de escrita nos novos *links* de coleta na unidade coletora de dados monocanal que encerra o ciclo de trabalho do gerenciador da unidade coletora. Todo este processo é repetido ciclicamente em intervalos regulares de 30 segundos.

Dois formatos diferentes foram propostos para a saída de dados enviado ao microcomputador para armazenamento. O motivo pelo qual estes dois padrões foram implementados reside no fato de que o tipo de arquivo exigido pelo software de análise proposto por (KUNZEL, 2012) é rígido. Qualquer campo adicional precisava reescrever o interpretador de arquivo da ferramenta. Como este não era o foco do trabalho, informações adicionais precisam ser fornecidas com um padrão alternativo. E uma destas informações adicionais foi o objeto de coleta neste primeiro ensaio.

O meio encontrado para avaliar a carga de processamento adicional inserida na unidade coletora de dados foi avaliar quanto ela estava se desviando do momento exato em que deveria enviar uma mensagem. A diferença entre o início do envio da mensagem e o instante no tempo em que idealmente a mensagem deveria ser enviada é medido pelo dispositivo de campo que recebe a mensagem. Essa informação, reencaminhada ao dispositivo transmissor dentro do pacote de ACK, é utilizada no processo de sincronização

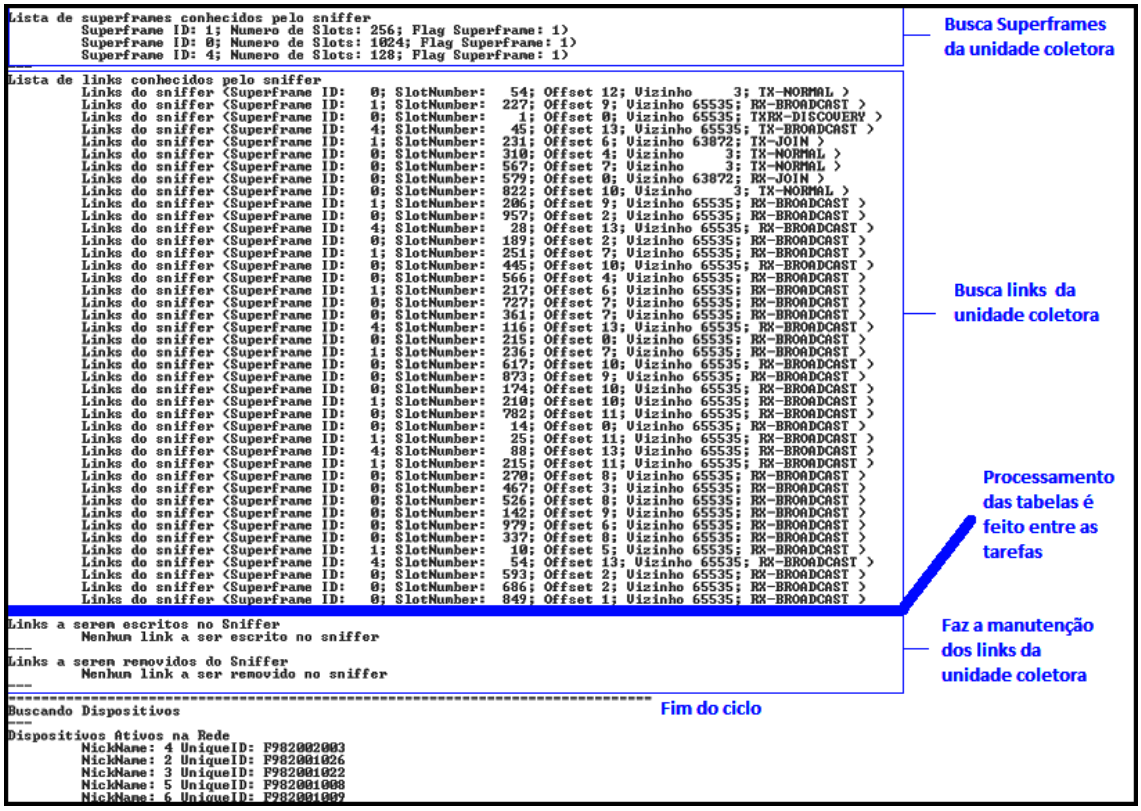
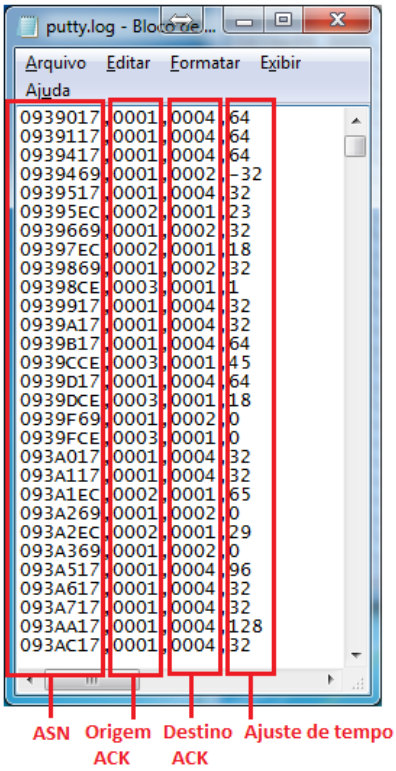


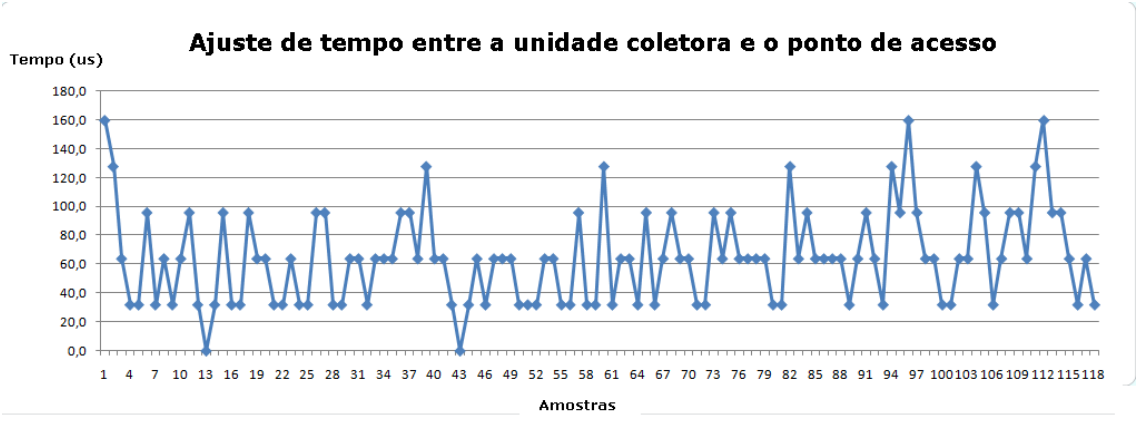
Figura 37: Leitura de *superframes*, *links* e processos de manutenção da unidade coletora

do TDMA, caso o dispositivo receptor seja uma fonte de relógio confiável na rede.

Inicialmente, a unidade coletora foi programada para coletar apenas algumas informações de todos os ACKs trafegando na rede e registrar seus dados no arquivo. O arquivo texto gerado é apresentado na Figura 38(a). Este arquivo, gerado durante 1 hora de ensaio e apresentando tamanho total de 440 kBytes, contém apenas o ajuste temporal presente no pacote de ACK, o dispositivo origem e destino dos pacotes. Demais informações do pacote de ACK foram descartadas. Uma filtragem foi feita para que um gráfico mostrasse apenas os ajustes temporais capturados entre a unidade coletora e o ponto de acesso que era fonte de relógio da rede. Esse gráfico, mostrando as primeiras amostras, é exposto na Figura 38(b).



(a) Formato do arquivo de ajuste temporal



(b) Gráfico de ajuste temporal

Figura 38: Resultado do ensaio de ajuste temporal

A tabela 4 resume os resultados experimentais obtidos no ensaio do desvio temporal descrito anteriormente. Os tempos obtidos por dois dispositivos de campo desenvolvidos por (MULLER et al., 2010) foram utilizados como elementos de comparação com a unidade coletora de dados monocanal. Os tempos de máximo e mínimo e a média calculada indicam analiticamente o impacto da integração entre as funções de coleta de dados em um dispositivo de campo. Os dados do ajuste de tempo apresentado na tabela 4 dão uma indicação sobre o comportamento apresentado (avanço ou atraso) pelo dispositivo no preciso mecanismo de sincronização com os *timeslots* da rede.

Tabela 4: Ajuste temporal entre dispositivos de campo e o ponto de acesso

Dispositivo	Tempo Mínimo(us)	Tempo Médio(us)	Tempo Máximo(us)
Prototipo WH - 1022	-64,0	-2,24	+64,0
Prototipo WH - 1023	-96,0	+2,56	+64,0
Unidade Coletora	0,0	+76,16	+160,0

Em um segundo ensaio com duração de 90 minutos, o procedimento de reinicialização da rede foi feito. Os dispositivos foram reinseridos na rede e a unidade coletora de dados foi novamente a primeira a ser agregada. A intenção desse segundo teste foi verificar a integração com a unidade de análise de rede proposta por (KUNZEL, 2012) e validar a estrutura do formato do arquivo, implementado no namimote, para executar a transferência dos dados entre as ferramentas. Com todos os procedimentos mantidos conforme o primeiro teste, a unidade coletora de dados seria capaz de capturar as chaves criptográficas necessárias para a decriptografia dos pacotes. O arquivo resultante, que apresentou 4,3 Mbytes de tamanho total, é apresentado na Figura 39.

Após o processo de geração do arquivo de integração, a unidade de análise de dados foi executada. Os pacotes de dados WH eram interpretados e decodificados. A topologia da rede mostrada pelo gateway, na Figura 40(a), era vista pelo software de análise de rede conforme apresentado na Figura 40(b).

Na parte inferior da Figura 40(b), pode-se verificar a associação entre os apelidos dos dispositivos de campo com os seus respectivos *HART Tag*. Nesta figura ainda é possível obter a topologia da rede formada, representada em forma de grafo, onde cada nó repre-

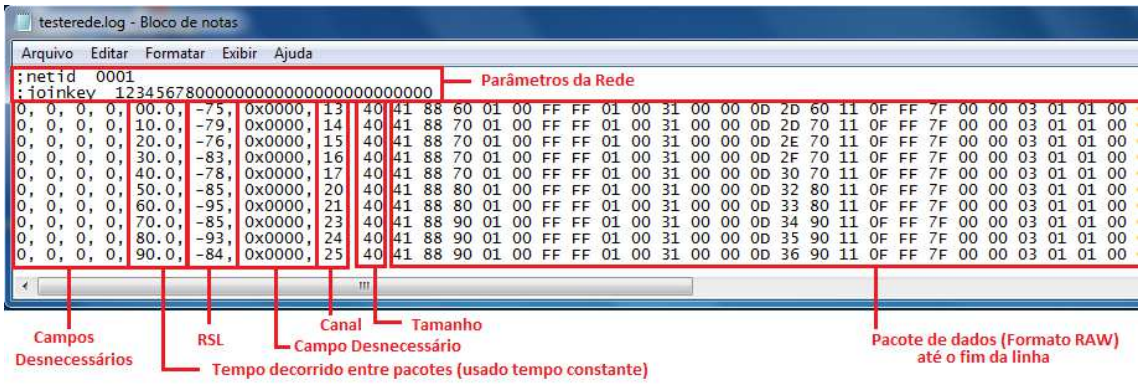


Figura 39: Estrutura do arquivo de integração

senta um dispositivo de campo e cada linha representa comunicação com um dispositivo na vizinhança.

Em um exemplo prático, o dispositivo de campo identificado pelo *nickname* 5 está conectado aos vizinho *nickname* 1 (ponto de acesso) e ao *nickname* 3. Esta informação é confirmada na última linha da Figura 40(a) que indica que o dispositivo **WH - 2009** tem apenas os dispositivos **GWEmerson** (gateway) e o dispositivo **TAG 1026 MOD POT** como vizinho. Em uma análise mais aprofundada, onde estendemos o processo de conferência realizado a todos os dispositivos de campo, vemos que a topologia de rede formada foi corretamente interpretada e decodificada pela ferramente de análise a partir dos pacotes de dados coletados pela unidade coletora monocanal.

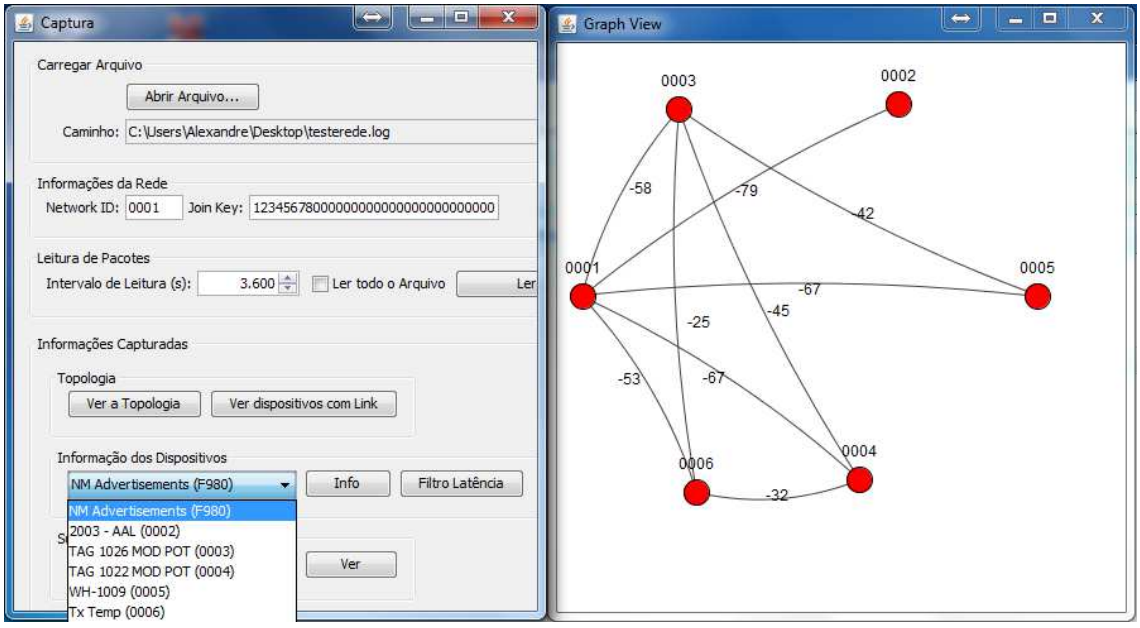
Alguns dados adicionais foram também obtidos através da ferramenta de análise. As informações de dois dispositivos de campo são apresentadas na Figura 41 e a estrutura dos *superframes* e *links* de comunicação utilizados na rede são apresentados na Figura 42.

Smart Wireless Gateway

Network Device Status factory

HART Tag	Node state	Active neighbors	Neighbors	Service denied	Reliability	Missed updates	Path stability	RSSI	Joins	Join Time
2003 - AAL	●	GWEmerson	1	●		0	92.1 %	-57 db	7	04/26/13 20:01:53
TAG 1022 MOD POT	●	GWEmerson TAG 1026 MOD POT Tx Temp	3	●	100.0 %	0	92.1 %	-30 db	1	04/26/13 20:08:53
TAG 1026 MOD POT	●	GWEmerson TAG 1022 MOD POT WH-1009 Tx Temp	4	●	100.0 %	0	100.0 %	-30 db	1	04/26/13 20:05:18
Tx Temp	●	GWEmerson TAG 1022 MOD POT TAG 1026 MOD POT	3	●	100.0 %	0			1	04/26/13 20:22:50
WH-1009	●	GWEmerson TAG 1026 MOD POT	2	●	100.0 %	0	90.5 %	-67 db	1	04/26/13 20:14:10

(a) Rede formada apresentada pelo *gateway*



(b) Rede obtida através da análise dos dados coletados

Figura 40: Rede formada durante o ensaio

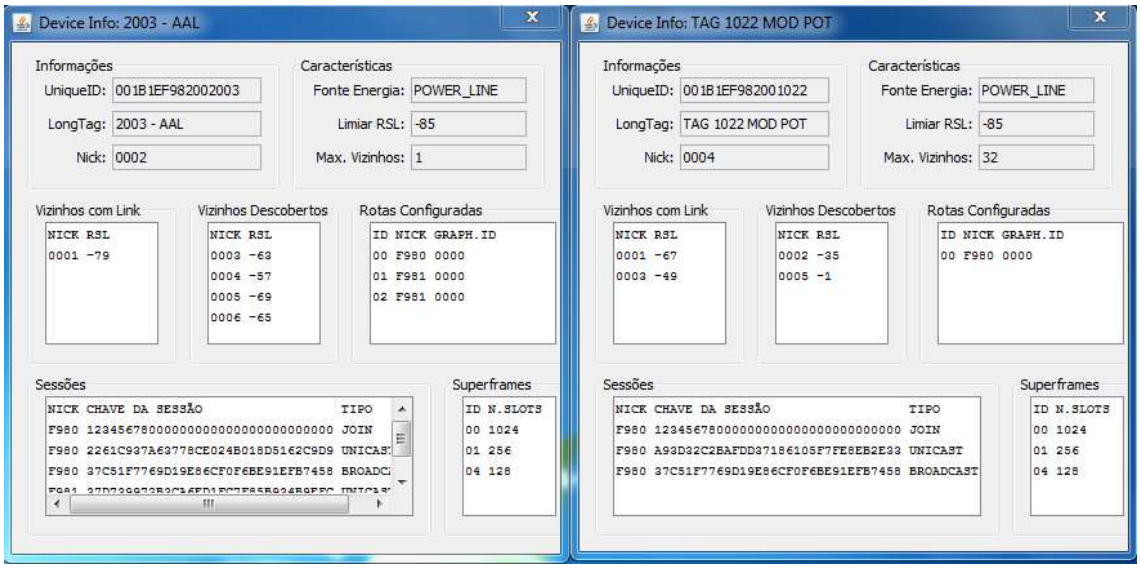


Figura 41: Informações dos dispositivos obtidos através da ferramenta de análise

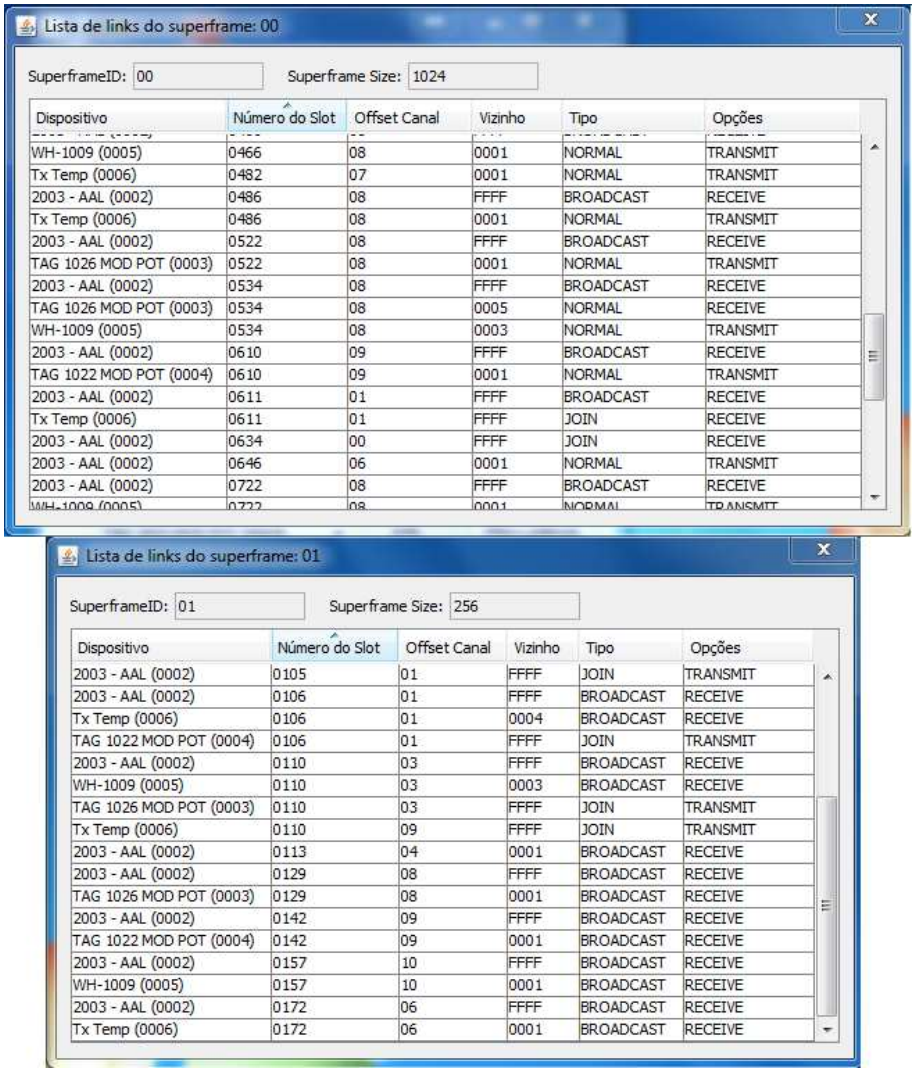


Figura 42: Estrutura dos *superframes* obtidos pela ferramenta de análise

5.4 Síntese do capítulo

Neste capítulo foi apresentada a implementação das duas unidades coletoras de dados proposta neste trabalho. Inicialmente descreveu-se a implementação da unidade coletora de dados monocanal, onde o *firmware* desenvolvido e o *hardware* utilizado foram detalhados. Em seguida, o *software* do gerenciador da unidade coletora de dados monocanal foi apresentado e cada um dos seus estados foi descrito. Na sequência do trabalho, o estado atual do projeto do *hardware* da unidade de coleta de dados multicanal é apresentado. Finalizando o capítulo, os resultados experimentais obtidos na implementação monocanal são comentados.

6 CONCLUSÕES E TRABALHOS FUTUROS

Muitos são os desafios no processo de análise de uma rede WH. A presença de criptografia na rede, o sincronismo com os *timeslots* do TDMA e os saltos de canais utilizados por esse protocolo são alguns exemplos. Os trabalhos estudadas que realizam análise de redes WH utilizam a mesma estrutura de *hardware*, baseadas em uma solução com múltiplos transceptores, onde o processo de captura dos pacotes de dados é realizado de modo simultâneo em todos os canais do espectro de frequência. Não há armazenamento temporário entre a unidade responsável pelo coletor de dados e pela unidade de análise. Esse processo, que necessita fios de intercomunicação entre os sistemas e baterias para alimentação, dificulta sua utilização em campo.

O presente trabalho propõe alternativas inovadoras no processo de coleta e análise de redes WH. A quebra temporal entre o momento da coleta de dados e o momento da análise dos dados coletados é obtido através da inclusão de uma memória não volátil na arquitetura proposta. Assim, a unidade coletora, de tamanho reduzido e alimentada por baterias, pode ser facilmente alocada em pontos do chão de fábrica onde o acesso de microcomputadores e cabos de alimentação se torna difícil.

A integração entre o dispositivo de campo e a unidade de coleta de dados também se apresenta como uma contribuição significativa neste trabalho. Algumas vantagens são obtidas com essa decisão de projeto. O envio de comandos à unidade coletora através da própria rede sem fios permite um modo simplificado de gerenciamento sobre o dispositivo. Principalmente se o mesmo está instalado em campo, coletando dados de uma rede real no chão de fábrica. A proposta de integração entre os elementos do sistema também

possibilita que a ferramenta evolua. Os dados coletados e armazenados na memória não volátil poderiam ser transmitidos pela rede WH diretamente para a unidade de análise dos dados sem que houvesse necessidade de deslocamentos para remoção dos cartões de memória dos dispositivos.

A proposta de análise de redes WH utilizando apenas um *transceptor* também apresenta ineditismo, pois é a primeira tentativa observada na literatura neste sentido. Nesta arquitetura, que utiliza dois elementos que colaboram entre si, o *transceptor* fica saltando de canal em canal seguindo a programação feita pelo gerenciador da rede. Para atingir esse objetivo, o presente trabalho apresenta os pontos e os cuidados que precisam ser alterados para que se consiga eficiência da solução.

Através dos resultados experimentais obtidos com a unidade coletora monocanal pode-se perceber que houve a necessidade de uma correção temporal maior para a manutenção do sincronismo com a rede. Esse incremento de tempo, da ordem de 75 us, era esperado e reflete o processamento adicional incluído na camada de enlace de dados para realizar as tarefas do produtor dos dados coletados. Do ponto de vista do tempos de máximo e mínimo, o impacto da alteração feito no *firmware* original foi relativamente pequena gerando apenas um deslocamento médio nos dados obtidos.

Apesar da integração da ferramenta de coleta de dados monocanal se mostrar funcional com a ferramenta de análise, algumas questões envolvendo implementação precisam ser melhor resolvidas. Durante os ensaios, percebeu-se perdas de alguns pacotes de ACK que sugerem que o processo implementado para a captura das mensagens e confirmações subsequentes deva ser melhor estudado. Ensaios mais aprofundados precisam ser feitos de modo a verificar se estas perdas são frutos de falhas no processo de implementação ou de insuficiência de poder de processamento do dispositivo para tratar o grande fluxo de mensagens trafegando no ar.

A abordagem multicanal apresentada nesse trabalho segue a lógica dos trabalhos relacionados. Entretanto, inova permitindo que os rádios coletores, entidades responsáveis por fazer a coleta em cada um dos canais, seja microprocessada. A escolha desta topologia permite que filtros locais possam ser implementados nos *firwmares* dos rádios coletores

recebendo apenas dados que realmente sejam objeto de estudo da ferramenta de análise. A modificação do *firmware* dos rádios coletores também estende o uso da tecnologia desenvolvida com a implementação de novos protocolos sem a necessidade de alterações significativas na placa base da unidade coletora de dados multicanal. Aliado a isto, o dispositivo proposto possibilita o desenvolvimento de outros equipamentos para avaliação e validação de dispositivos WH, entre eles, geradores de interferências para avaliação de coexistência.

A integração com uma ferramenta de análise de rede WH é outro ponto promissor das propostas desenvolvidas. Desta forma, o escopo da análise da rede pode ser ampliado, através da inclusão de novas funcionalidades, uma vez que se tem o domínio de toda a cadeia de coleta, armazenamento e análise de redes WH.

REFERÊNCIAS

AKYILDIZ, I. et al. A survey on sensor networks. **Communications Magazine, IEEE**, [S.l.], v.40, n.8, p.102 – 114, Aug. 2002.

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

DEPARI, A. et al. Design and performance evaluation of a distributed WirelessHART sniffer based on IEEE1588. In: PRECISION CLOCK SYNCHRONIZATION FOR MEASUREMENT, CONTROL AND COMMUNICATION, 2009. ISPCS 2009. INTERNATIONAL SYMPOSIUM ON, 2009, Brescia. **Proceedings...** [S.l.: s.n.], 2009. p.1 –6.

FERRARI, P. et al. An innovative distributed instrument for WirelessHART testing. In: INSTRUMENTATION AND MEASUREMENT TECHNOLOGY CONFERENCE, 2009. I2MTC '09. IEEE, 2009, Singapore. **Proceedings...** [S.l.: s.n.], 2009. p.1091 –1096.

FREESCALE. **Compact Integrated Antennas**: designs and applications for the mc1319x, mc1320x, and mc1321x. 2006. Disponível em: <www.freescale.com/files/rf_if/doc/app_note/AN2731.pdf>. Acesso em: 12 set. 2012.

FREESCALE. **MC1322x**: advanced zigbeetm- compliant platform-in-package (pip) for the 2.4 ghz ieee® 802.15.4 standard. 2010. Disponível em: <www.freescale.com/files/rf_if/doc/data_sheet/MC1322x.pdf>. Acesso em: 11 jul. 2012.

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

GUTIERREZ, J. et al. **Low-rate wireless personal area networks**: enabling wireless sensors with ieee 802.15.4. 3.ed. New York: Standards Information Network / IEEE Press, 2010.

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

HART COMMUNICATION FOUNDATION. **HCF SPEC-065 Rev. 1.0**: 2.4ghz dsss o-qpsk physical layer specification. Austin: HCF, 2007. Parte de norma.

HART COMMUNICATION FOUNDATION. **HCF SPEC-099 Rev. 9.0**: command summary specification. Austin: HCF, 2007. Parte de norma.

HART COMMUNICATION FOUNDATION. **HCF SPEC-075 Rev. 1.1**: tdma data link layer specification. Austin: HCF, 2008. Parte de norma.

HART COMMUNICATION FOUNDATION. **HCF SPEC-155 Rev. 1.1**: wireless command specification. Austin: HCF, 2008. Parte de norma.

HART COMMUNICATION FOUNDATION. **HCF SPEC-085 Rev. 1.2**: network management specification. Austin: HCF, 2009. Parte de norma.

HART COMMUNICATION FOUNDATION. **HCF SPEC-085 Rev. 2.0**: network management specification-preliminary d. Austin: HCF, 2011. Parte de norma.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Part 15.4**: wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (wpans). New York: IEEE Computer Society, 2006. Parte de norma.

KARAPISTOLI, E. et al. An overview of the IEEE 802.15.4a Standard. **Communications Magazine, IEEE**, [S.l.], v.48, n.1, p.47 –53, Jan. 2010.

KIM, A. et al. When HART goes wireless: understanding and implementing the wirelesshart standard. In: EMERGING TECHNOLOGIES AND FACTORY AUTOMATION, 2008. ETFA 2008. IEEE INTERNATIONAL CONFERENCE ON, 2008, Hamburg. **Proceedings...** New York: IEEE Press, 2008. p.899 –907.

KOUBAA, A. et al. Z-Monitor: monitoring and analyzing ieee 802.15.4-based wireless sensor networks. In: LOCAL COMPUTER NETWORKS (LCN), 2011 IEEE 36TH CONFERENCE ON, 2011, Bonn. **Proceedings...** [S.l.: s.n.], 2011. p.939 –947.

KRATZIG, M. et al. 16-Channel-Analyser for parallel IEEE 802.15.4 monitoring. In: EMERGING TECHNOLOGIES FACTORY AUTOMATION, 2009. ETFA 2009. IEEE CONFERENCE ON, 2009, Mallorca. **Proceedings...** [S.l.: s.n.], 2009. p.1 –4.

KUNZEL, G. **Ambiente para Avaliação de Estratégias de Roteamento Para Redes WirelessHART**. 2012. 95p. Dissertação (Mestrado em Engenharia Elétrica) — Universidade Federal do Rio Grande do Sul, Porto Alegre, 2012.

LOW, K.; WIN, W.; ER, M. Wireless Sensor Networks for Industrial Environments. In: COMPUTATIONAL INTELLIGENCE FOR MODELLING, CONTROL AND AUTOMATION, 2005 AND INTERNATIONAL CONFERENCE ON INTELLIGENT AGENTS, WEB TECHNOLOGIES AND INTERNET COMMERCE, INTERNATIONAL CONFERENCE ON, 2005, Vienna. **Proceedings...** [S.l.: s.n.], 2005. v.2, p.271 –276.

MRAZ, L. et al. Open-packet analyser platform for wireless sensor networks based on IEEE 802.15.4. In: TELECOMMUNICATIONS AND SIGNAL PROCESSING (TSP), 2011 34TH INTERNATIONAL CONFERENCE ON, 2011, Bradford. **Proceedings...** [S.l.: s.n.], 2011. p.145 –149.

MULLER, I. et al. Development of a WirelessHART compatible field device. In: INSTRUMENTATION AND MEASUREMENT TECHNOLOGY CONFERENCE (I2MTC), 2010 IEEE, 2010, Austin. **Proceedings…** New York: IEEE Press, 2010. p.1430–1434.

MULLER, I. et al. Namimote: a low-cost sensor node for wireless sensor networks. In: NEW2AN, 2012, St. Petersburg. **Proceedings…** New York: Springer, 2012. p.391–400. (Lecture Notes in Computer Science, v.7469).

PETERSEN, S.; CARLSEN, S. WirelessHART Versus ISA100.11a: the format war hits the factory floor. **Industrial Electronics Magazine, IEEE**, [S.l.], v.5, n.4, p.23 –34, Dec. 2011.

RADMAND, P. et al. Comparison of industrial WSN standards. In: DIGITAL ECOSYSTEMS AND TECHNOLOGIES (DEST), 2010 4TH IEEE INTERNATIONAL CONFERENCE ON, 2010, Dubai. **Proceedings…** [S.l.: s.n.], 2010. p.632 –637.

SONG, J. et al. WirelessHART: applying wireless technology in real-time industrial process control. In: REAL-TIME AND EMBEDDED TECHNOLOGY AND APPLICATIONS SYMPOSIUM, 2008. RTAS ’08. IEEE, 2008, St. Louis. **Proceedings…** [S.l.: s.n.], 2008. p.377 –386.

WINTER, J. **Análise de Coexistência em redes WirelessHART**. 2013. 99p. Dissertação (Mestrado em Engenharia Elétrica) — Universidade Federal do Rio Grande do Sul, Porto Alegre, 2013.

WINTER, J. et al. WirelessHART Routing Analysis Software. In: COMPUTING SYSTEM ENGINEERING (SBESC), 2011 BRAZILIAN SYMPOSIUM ON, 2011, Florianópolis. **Proceedings…** [S.l.: s.n.], 2011. p.96–98.

YOO, S.-E. et al. Guaranteeing Real-Time Services for Industrial Wireless Sensor Networks With IEEE 802.15.4. **Industrial Electronics, IEEE Transactions on**, [S.l.], v.57, n.11, p.3868 –3876, Nov. 2010.