

ANALISADOR DE REDES WIRELESSHART MONOCANAL

ALEXANDRE A. LORENÇATO*, IVAN MÜLLER*, JEAN M. WINTER*, GUSTAVO KUNZEL†, JOÃO NETTO‡, CARLOS E. PEREIRA*

*Departamento de Engenharia Elétrica
Universidade Federal do Rio Grande do Sul
Porto Alegre, Rio Grande do Sul, Brasil

†Departamento de Controle e Automação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul
Rio Grande do Sul, Brasil

‡Instituto de Informática
Universidade Federal do Rio Grande do Sul
Porto Alegre, Rio Grande do Sul, Brasil

Emails: alexandre.lorencato@ufrgs.br, ivan.muller@ufrgs.br, jean.winter@ufrgs.br, gkunzel@gmail.com, netto@info.ufrgs.br, cpereira@ece.ufrgs.br

Abstract— *WirelessHART* is a robust and reliable protocol for industrial environment usage because of its security mechanism, the ability to program several communication routes between network devices, and deterministic, free of collisions channel hopping media access controller. However, for increasing adoption of this technology, it is necessary to increase the amount of *WirelessHART* manufacturers to develop industrial sensors and actuators devices. This leads to the need of tools to be created in order to assist the development and debugging of new network compliant devices. The *WirelessHART* network analyzer is undoubtedly one of these tools. Various approaches are being proposed for the analysis of *WirelessHART* networks. However, all of them make use of a microcomputer as an element of the whole system and this difficult their use in real field applications. The presence of wires, lack of local data storage and other aspects such as batteries limitations must be taken into account when the users intend to use analysis systems in field. This work proposes one conceptually different proposal that meet the basic requirements for the use in the field. This approach is based on the proposed integration between a field device and an innovative method of capturing messages using only one transceiver. This proposal is implemented as proof of concept.

Keywords— *WirelessHART* Protocol, IEEE 802.15.4, Wireless network analysis, Industrial Wireless Sensor Networks, protocol analysis.

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 frequentes tornam a comunicação no protocolo *WirelessHART* 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 *WirelessHART*. Disto surge a necessidade de criação de ferramentas capazes de auxiliar o desenvolvimento e depuração destes novos dispositivos de rede. O Analisador de rede *WirelessHART* é, sem dúvida, uma delas. Diversas abordagens são propostas para a análise de redes *WirelessHART*. Entretanto, em todas elas a utilização de um microcomputador como elemento do sistema inviabiliza sua utilização em campo. A presença de cabos, falta de 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 uma alternativa aos sistemas de análise de redes atuais apresentando uma proposta conceitualmente diferente mas que cumprem os requisitos básicos para sua utilização em campo. Nesta abordagem, 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— Protocolo *WirelessHART*, IEEE 802.15.4, Análise de redes sem fio, Redes industriais de sensores sem fio, analisador de protocolos.

1 Introdução

Nos sistemas tradicionais de automação industrial, onde a interligação entre sensores, atuadores e controladores é feita por cabos, 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 fortes campos magnéticos, 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 atra-

tiva do que as soluções cabeadas existentes (Low et al., 2005).

As redes de sensores sem fio são sistemas em que cada nó sensor pertencente à 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. Estes sensores 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 mai-

oria das aplicações. Contudo, em ambientes industriais, tais falhas são inaceitáveis. Neste caso, os dispositivos sem fio 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 a confiabilidade da 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 et al., 2005), (Gungor and Hancke, 2009).

Com o objetivo de atender esta nova demanda, muitos protocolos de comunicação industrial tem sido desenvolvidos. As especificações dos protocolos ISA100.11a, Zig-Bee PRO e *WirelessHART*(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 protocolo de comunicação WH foi desenvolvido sobre a camada física do padrão IEEE 802.15.4, redefinindo o mecanismo de acesso ao meio tornando-o determinístico. Mecanismos de retransmissão de mensagens e saltos de frequência a cada comunicação foram agregados. A diversidade de rotas foi prevista através da utilização de redes em malha. A segurança da informação foi desenvolvida para permitir autenticação, integridade e criptografia utilizando algoritmos estabelecidos.

Com o surgimento do WH, tornou-se necessário o desenvolvimento 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 (Han et al., 2009). Um destes equipamento é o analisador de redes WH.

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 res-

ponsabilidade de interpretar, validar e apresentar os dados capturados.

Um analisador de redes formado a partir desta estrutura auxilia 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 de ferramenta de análise do protocolo. 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. Desta forma, 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.

Esse artigo é organizado da seguinte forma: Na seção 2 são analisados alguns trabalhos relacionados ao analisador de rede proposto. Na seção 3 é apresentada a proposta a ser desenvolvido nesse trabalho. A seção 4 apresenta a implementação e os resultados experimentais obtidos. Finalizando o artigo, a seção 5 apresenta as conclusões obtidas a partir dos resultados experimentais obtidos neste trabalho.

2 Trabalhos relacionados

O padrão de comunicação sem fio *WirelessHART* 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 o analisador de rede padrão da HCF que tem a responsabilidade de fazer a coleta de dados necessário para o processo de certificação. Internamente, o *Wi-Analys* é composto por 16 transceivers IEEE 802.15.4. Cada um sintonizado em uma canal do espectro 2.4 GHz. Todos estes rádios são conectados a uma FPGA que realiza a amostragem de cada um dos canais. Os dados então são agregados e enviados a um microcomputador através de uma porta USB. No microcomputador, um *software* trata, filtra e até permite exportar estes dados. Apesar de ser a ferramenta oficial da HCF para utilização com redes *WirelessHART*, é um equipamento para uso em labora-

tório. Pode ser utilizado durante o processo de desenvolvimento de um dispositivo *WirelessHART*, mas que não tem a robustez e a mobilidade necessária para aquisição de dados em campo com uma rede *WirelessHART* completa.

Outros analisadores de rede tem sido propostos na literatura. O analisador descrito por (Kratzig et al., 2009) propõe um analisador de redes para o padrão IEEE 802.15.4 independente das camadas superiores. A solução proposta tem 3 partes: Uma unidade RF composta por 16 rádios com splitter, uma unidade de processamento composta por um FPGA Xilinx Spartan 3A DSP e um computador que atua como unidade de controle. A unidade RF recebe, em paralelo, os 16 canais. O FPGA lê os dados através da porta SPI, coloca um *timestamp* e transfere os dados para uma FIFO que é lida pelo PC através da *Ethernet*. Assim, como no *Wi-Analys*, o processamento é feito por PC e não há armazenamento local das informações. Todos os dados são capturados independentemente de sua utilidade gerando fluxos desnecessários de informação.

Assim como na proposta de analisador de rede acima, o trabalho realizado em (Mraz et al., 2011) foca em redes padrão IEEE 802.15.4. Ele divide a solução em 2 partes: A unidade de recepção que é responsável pela obtenção dos dados e a unidade de análise dos pacotes recebidos. O *hardware* proposto para a unidade de recepção consiste de um microcontrolador Atmega1281 e uma unidade de RF AT86RFxx que sintoniza apenas um canal dos 16 possíveis do espectro 2.4 GHz. A unidade de análise dos pacotes é composta por um microcomputador e por um módulo driver capaz de ler os dados e enviá-los ao *software* WireShark que registra os pacotes de dados coletados para posterior análise. A comunicação entre a unidade de recepção e a de análise é feita através de uma porta USB. Apesar da plataforma escolhida para a unidade de análise de pacotes de dados ser adequada para a inclusão de novos protocolos, o *hardware* utilizado na unidade receptora deixa a desejar em se tratando de redes WH uma vez que não há previsão de troca de canais.

A solução proposta por (Koubaa et al., 2011), conhecida como Z-Monitor, é basicamente uma solução por *software*. Seu objetivo é prover uma solução aberta, extensível e modular para monitoração de redes IEEE 802.15.4. O *hardware* utilizado não é definido. A solução proposta permite o uso de qualquer rádio compatível com redes IEEE 802.15.4 que seja capaz de redirecionar o fluxo de dados da antena para uma interface de comunicação. Apesar da ferramenta permitir criação de módulos capazes de interpretar novos protocolos, a aplicabilidade ao WH não é totalmente coberta. Questões referentes a trocas de canais frequentes inviabilizam o uso de *dongles* IEEE 802.15.4 comumente encontrados do mercado que possuem

apenas um transceiver de RF onde o salto entre canais não é previsto.

O trabalho realizado por (Ferrari et al., 2009) propõe uma arquitetura distribuída onde diversos pontos de uma rede WH podem ser analisados. Cada um destes pontos de análise consiste de uma estrutura chamada *probe* que se liga com uma central única de monitoração através de uma rede *Ethernet*. Cada *probe* consiste de 16 rádios onde cada um sintoniza um canal do espectro de frequências de 2.4GHz. Todos estes rádios são gerenciados por uma FPGA através da porta de comunicação SPI. A central de monitoração basicamente é um microcomputador que trata os pacotes recebidos, descarta os inválidos e ignora os repetidos. A solução proposta é extremamente complexa e tem foco na visão geral da rede WH dando informações adicionais ao gerenciador da rede para auxílio no processo de manutenção e ajustes da rede. Contudo também apresenta infraestrutura complexa de dispositivos de rede, cabeamento e a necessidade de um computador conectado ao sistema o qual torna a solução inviável do ponto de vista de rearranjo espacial dos pontos da rede WH a serem analisados.

3 Analisador Proposto

A estrutura proposta nesse trabalho é apresentada na Figura 1. 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.

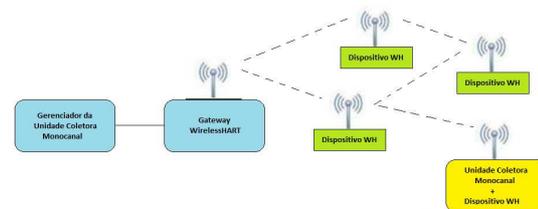


Figura 1: Estrutura do coletor de dados monocanal

A unidade coletora de dados proposta nessa abordagem realiza as funções de sintonização de canal, captura de mensagens e armazenamento de dados coletados em memória não-volátil para posterior análise. Entretanto deriva suas funções 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. 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 com o 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 na vizinhança da unidade coletora já estejam tratados, o gerenciador da unidade coletora 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 sintonizando os canais, capturando e armazenando as mensagens WH transmitidos entre os dispositivos da rede em memória não volátil.

Para realizar as atividade de interpretação e decodificação das mensagens WH capturadas, se torna essencial o desenvolvimento de uma ferramenta de análise de dados. Muitas são as abordagens observadas na literatura para desempenhar desse papel. A abordagem utilizada neste trabalho propõe a integração com a ferramenta desenvolvidas por (Kunzel, 2012).

A integração entre a unidade coletora de dados e a ferramenta proposta por (Kunzel, 2012) é feita através de um arquivo texto armazenado em um cartão SD. Esta ferramenta carrega o arquivo gerado pela unidade coletora, 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.

4 Implementação e Resultados Experimentais

Um cenário de testes precisou ser montado para a validação da proposta do coletor de dados monocanal. Cinco dispositivos de campo foram utilizados no ensaio: um transmissor de temperatura da Emerson modelo TT648, três rádio protótipos WH descritos em (Muller et al., 2010) e o namimote (Muller et al., 2012), identificado com 2003-AAL, 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 2.

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

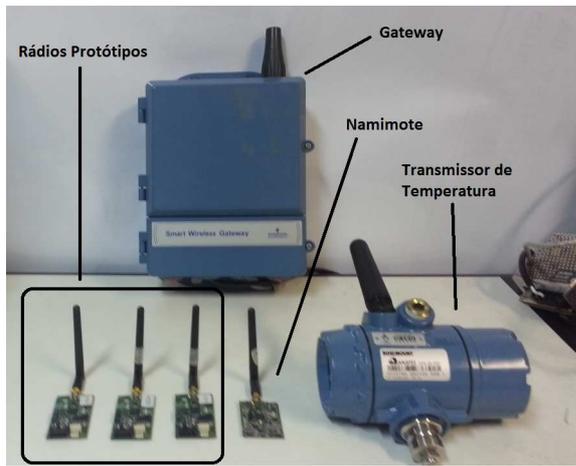


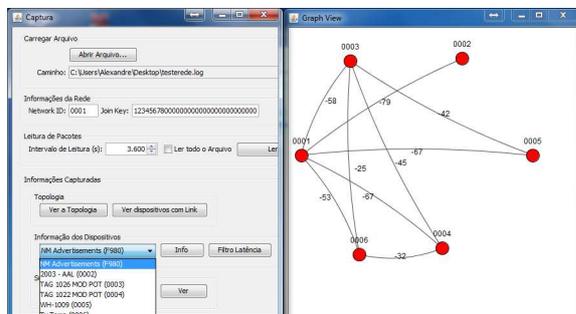
Figura 2: Equipamento utilizados nos ensaios

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 são automaticamente incluídos na lista de dispositivos ativos e seus *links* de comunicação são coletados pelo gerenciador da unidade coletora e enviados à unidade coletora monocanal.

Após o processo de geração do arquivo de integração pela unidade coletora de dados monocanal, a unidade de análise de dados foi executada para interpretar e decodificar os pacotes de dados WH coletados. A topologia da rede mostrada pelo *gateway*, na Figura 3(a), era vista pelo *software* de análise de rede, após interpretação das mensagens, conforme apresentado na Figura 3(b).

MARK Tag	Node state	Active neighbors	Neighbors	Service desired	Reliability	Missed updates	Path stability	RSSI	Joins	Join Time
0000 - AAL	ONLINE	ONLINE	1	ONLINE	100.0 %	0	92.4 %	-57 dB	7	04/26/13 20:01:53
TAG 1026 MOD POT	ONLINE	TAG 1026 MOD POT	3	ONLINE	100.0 %	0	92.1 %	-30 dB	1	04/26/13 20:08:15
TAG 1026 MOD POT	ONLINE	TAG 1026 MOD POT	4	ONLINE	100.0 %	0	100.0 %	-30 dB	1	04/26/13 20:05:18
Tx Temp	ONLINE	TAG 1022 MOD POT	3	ONLINE	100.0 %	0	99.5 %	-67 dB	1	04/26/13 20:22:56
WH-1009	ONLINE	TAG 1026 MOD POT	2	ONLINE	100.0 %	0	99.5 %	-67 dB	1	04/26/13 20:14:16

(a) Topologia apresentada pela interface gráfica do *gateway*



(b) Topologia obtida através da análise dos dados coletados

Figura 3: Topologia da rede formada

Alguns dados adicionais foram também obtidos através da ferramenta de análise. As informa-

ções de dois dispositivos de campo são apresentadas na Figura 4.

Informações	Características
LinkID: 0018 EFP82002003	Fonte Energia: POWER_LINE
LongTag: 2003 - AAL	Linear RSL: -85
Nick: 0002	Max. Vantagem: 1

Informações	Características
LinkID: 0018 EFP82001022	Fonte Energia: POWER_LINE
LongTag: TAG 1022 MOD POT	Linear RSL: -85
Nick: 0004	Max. Vantagem: 32

Figura 4: Informações dos dispositivos obtidos através da ferramenta de análise

A estrutura dos *superframes* e *links* de comunicação utilizados na rede são apresentados na Figura 5.

Dispositivo	Número do Slot	Offset Canal	Vizinho	Tipo	Opções
WH-1009 (0005)	0466	08	0001	NORMAL	TRANSMIT
Tx Temp (0006)	0482	07	0001	NORMAL	TRANSMIT
2003 - AAL (0002)	0486	08	FFFF	BROADCAST	RECEIVE
Tx Temp (0006)	0486	08	0001	NORMAL	TRANSMIT
2003 - AAL (0002)	0522	08	FFFF	BROADCAST	RECEIVE
TAG 1026 MOD POT (0003)	0522	08	0001	NORMAL	TRANSMIT
2003 - AAL (0002)	0534	08	FFFF	BROADCAST	RECEIVE
TAG 1026 MOD POT (0003)	0534	08	0005	NORMAL	TRANSMIT
WH-1009 (0005)	0534	08	0003	NORMAL	TRANSMIT
2003 - AAL (0002)	0610	09	FFFF	BROADCAST	RECEIVE
TAG 1022 MOD POT (0004)	0610	09	0001	NORMAL	TRANSMIT
2003 - AAL (0002)	0611	01	FFFF	BROADCAST	RECEIVE
Tx Temp (0006)	0611	01	FFFF	JOIN	RECEIVE
2003 - AAL (0002)	0634	00	FFFF	JOIN	RECEIVE
2003 - AAL (0002)	0646	06	0001	NORMAL	TRANSMIT
2003 - AAL (0002)	0722	08	FFFF	BROADCAST	RECEIVE
WH-1009 (0005)	0733	08	0001	NORMAL	TRANSMIT

Dispositivo	Número do Slot	Offset Canal	Vizinho	Tipo	Opções
2003 - AAL (0002)	0105	01	FFFF	JOIN	TRANSMIT
2003 - AAL (0002)	0106	01	FFFF	BROADCAST	RECEIVE
Tx Temp (0006)	0106	01	0004	BROADCAST	RECEIVE
TAG 1022 MOD POT (0004)	0106	01	FFFF	JOIN	TRANSMIT
2003 - AAL (0002)	0110	03	FFFF	BROADCAST	RECEIVE
WH-1009 (0005)	0110	03	0003	BROADCAST	RECEIVE
TAG 1026 MOD POT (0003)	0110	03	FFFF	JOIN	TRANSMIT
Tx Temp (0006)	0110	09	FFFF	JOIN	TRANSMIT
2003 - AAL (0002)	0113	04	0001	BROADCAST	RECEIVE
2003 - AAL (0002)	0129	08	FFFF	BROADCAST	RECEIVE
TAG 1026 MOD POT (0003)	0129	08	0001	BROADCAST	RECEIVE
2003 - AAL (0002)	0142	09	FFFF	BROADCAST	RECEIVE
TAG 1022 MOD POT (0004)	0142	09	0001	BROADCAST	RECEIVE
2003 - AAL (0002)	0157	10	FFFF	BROADCAST	RECEIVE
WH-1009 (0005)	0157	10	0001	BROADCAST	RECEIVE
2003 - AAL (0002)	0172	06	FFFF	BROADCAST	RECEIVE
Tx Temp (0006)	0172	06	0001	BROADCAST	RECEIVE

Figura 5: Estrutura dos *superframes* obtidos pela ferramenta de análise

5 Conclusões

O presente trabalho apresenta uma nova ferramenta para análise das redes WH. A ferramenta de análise de redes WH desenvolvida apresenta diferenças significativas quanto a estrutura de *hardware* dos tradicionais analisadores principalmente pela capacidade de monitorar todos os 16 canais deste padrão com a utilização de apenas um transceptor. São apresentadas diferentes soluções para obtenção de dados de uma rede com diferentes desafios tais como: presença de criptografia nas mensagens, sincronismo com os quadros de tempo (TDMA) e salto de canais.

A unidade coletora de dados deste trabalho foi desenvolvida de forma a integrar-se à rede WH como um tradicional dispositivo de campo, desta forma obtendo informações estratégicas para a monitoração dos dados da rede. Outras questões relevantes para sua aplicação foram implementadas como uma arquitetura de *hardware* que permite mobilidade e capacidade de transferência e armazenamento de dados.

A arquitetura utilizada neste trabalho permite que possam ser implementados filtros locais nos *firmwares* dos rádios coletores possibilitando receber apenas os dados de interesse para o caso de estudo. Ainda, através da modificação do *firmware* é possível estender o uso desta arquitetura para outros protocolos sem a necessidade de grandes alterações no sistema. A integração com uma outra ferramenta de análise de rede WH é outra possibilidade oferecida neste trabalho permitindo ampliar o escopo de análise de redes WH. Finalmente, em laboratório foram realizados ensaios com a ferramenta demonstrando sua eficiência e funcionamento adequado, no entanto, ainda foram observadas questões temporais que podem ser aprimoradas para a manutenção do sincronismo do dispositivo na rede.

Agradecimentos

Agradecemos à Capes e CNPq pela provisão de bolsas de estudo. Também somos gratos à Finep pelo financiamento do projeto E3, da qual este trabalho faz parte.

Referências

- Akyildiz, I., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002). A survey on sensor networks, *Communications Magazine, IEEE* 40(8): 102 – 114.
- Ferrari, P., Flammini, A., Marioli, D., Rinaldi, S., Sisinni, E. and Taroni, A. (2009). An innovative distributed instrument for wireless-shart testing, *Instrumentation and Measurement Technology Conference, 2009. I2MTC '09. IEEE*, pp. 1091 –1096.
- Gungor, V. and Hancke, G. (2009). Industrial wireless sensor networks: Challenges, design principles, and technical approaches, *Industrial Electronics, IEEE Transactions on* 56(10): 4258 –4265.
- Gutierrez, J., Winkel, L., Callaway, E. and Barrett, R. (2010). *Low-rate wireless personal area networks: enabling wireless sensors with IEEE 802.15.4*, third edn, Standards Information Network / IEEE Press, New York.
- Han, S., Song, J., Zhu, X., Mok, A., Chen, D., Nixon, M., Pratt, W. and Gondhalekar, V. (2009). Wi-htest: Compliance test suite for diagnosing devices in real-time wireless-shart network, *Real-Time and Embedded Technology and Applications Symposium, 2009. RTAS 2009. 15th IEEE*, pp. 327 –336.
- Koubaa, A., Chaudhry, S., Gaddour, O., Charari, R., Al-Elaiwi, N., Al-Soli, H. and Boujelben, H. (2011). Z-monitor: Monitoring and analyzing iee 802.15.4-based wireless sensor networks, *Local Computer Networks (LCN), 2011 IEEE 36th Conference on*, pp. 939 –947.
- Kratzig, M., Rauchhaupt, L., Schimschar, A. and Trikaliotis, S. (2009). 16-channel-analyser for parallel iee 802.15.4 monitoring, *Emerging Technologies Factory Automation, 2009. ETFA 2009. IEEE Conference on*, pp. 1 –4.
- Kunzel, G. (2012). *Ambiente para avaliação de estratégias de roteamento para redes wireless-shart*, Dissertação de mestrado, Programa de Pós-Graduação em Engenharia Elétrica - UFRGS.
- Low, K., Win, W. and Er, M. (2005). Wireless sensor networks for industrial environments, *Computational Intelligence for Modeling, Control and Automation, 2005 and International Conference on Intelligent Agents, Web Technologies and Internet Commerce, International Conference on*, Vol. 2, pp. 271 –276.
- Mraz, L., Komosny, D., Cervenka, V., Moravek, P. and Simek, M. (2011). Open-packet analyser platform for wireless sensor networks based on iee 802.15.4, *Telecommunications and Signal Processing (TSP), 2011 34th International Conference on*, pp. 145 –149.
- Muller, I., de Freitas, E. P., Susin, A. A. and Pereira, C. E. (2012). Namimote: A low-cost sensor node for wireless sensor networks., in S. D. Andreev, S. Balandin and Y. Koucheryavy (eds), *NEW2AN*, Vol. 7469 of *Lecture Notes in Computer Science*, Springer, pp. 391–400.
- Muller, I., Pereira, C., Netto, J., Fabris, E. and Allgayer, R. (2010). Development of a wireless-shart compatible field device, *Instrumentation and Measurement Technology Conference (I2MTC), 2010 IEEE*, pp. 1430–1434.
- Radmand, P., Talevski, A., Petersen, S. and Carlsson, S. (2010). Comparison of industrial wsn standards, *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on*, pp. 632 –637.