UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE ENGENHARIA DE COMPUTAÇÃO

LEANDRO TAVARES BRUSCATO

Detecção de Energia para Rede *Wireless*HART

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharel em Engenharia de Computação.

Orientador: Prof. Dr. João Cesar Netto
Co-orientador: Jean Michel Winter

Porto Alegre
2014

AGRADECIMENTOS

AGRADECIMENTOS

Primeiramente gostaria de agradecer ao meu orientador, Prof. Dr. João Cesar Netto, que me auxiliou na escolha do tema e me guiou durante toda essa caminhada completamente desconhecida por mim. Sempre calmo e dando-me a liberdade na medida para desenvolver esta tarefa.

Gostaria de agradecer ao meu co-orientador, Jean Michel Winter, que sempre esteve ao meu lado tirando toda e qualquer dúvida, das mais simples até as mais complexas, e que muitas vezes resultaram em discussões longas, e quase filosóficas.

Gostaria de agradecer, também, ao Dr. Ivan Müller, que sempre estava disposto a ajudar, sugerindo as melhores soluções e mais simples.

Agradecer à minha família, que sempre foi compreensiva e sempre esteve ao meu lado, me dando força nos momentos mais complicados. E principalmente, à minha sobrinha Tathiana, que compreendia as muitas vezes que eu recusava algum convite por estar desenvolvendo este trabalho.

E finalmente a namorada Rafaela que sempre estava disposta a me ajudar e me acompanhou nesta jornada, passando horas estudando ao meu lado.

RESUMO

Para o setor industrial, a evolução da tecnologia sem fio representou menores custos de instalação e manutenção. Mas, como a maioria dessas tecnologias se concentram na mesma faixa de frequência, a interferência se torna um dos grandes obstáculos a serem transpostos, juntamente com a segurança e a confiabilidade. Na maioria das tecnologias sem fio, a forma de controle de colisões é simples e desta forma gera atrasos em algumas transmissões. Em aplicações industriais, com critérios de comunicações em tempo real, a perda de pacotes pode acarretar em desastres, e consequentes perdas monetárias. A primeira norma de tecnologia sem fio para a indústria a ser aceita como um padrão internacional foi a *Wireless*HART, sendo uma seção do padrão HART, que é largamente utilizado nas indústrias. Este trabalho tem como objetivo o desenvolvimento de um novo estado de detecção de energia na arquitetura *Wireless*HART para medir a interferência de cada canal, Após sua realização, através de análises e testes, foi comprovada a detecção e identificação de interferência, para que, no futuro, o gerenciador da rede se adapte e previna conflitos de dados, diminuindo assim a perda de informações.

Palavras-chave: Rede sem fio. Redes Industriais. *Wireless*HART.

ABSTRACT

For industries, the evolution of wireless technology represented a lower cost for installations and maintenance. However, most of these technologies operate in the same frequency range and the interference becomes the biggest problem to solve. There are also concerns about security and reliability. Most wireless technologies, the control of collisions is simple, and therefore causes delay in transmission. In industrial real-time, the loss of a large number of packets can cause disasters, and subsequent monetary losses. The first wireless protocol for industry that was accepted as an international standard was the WirelessHART. That is part of a standard section of HART, which is widely used in industries. This work proposes the development of a new status of energy detection in WirelessHART architecture to measure the interference of each channel. It was showed through analysis and testing, the appropriate detection and interference identification , Future work includes an analysis from the network manager, which will adapt and prevent conflicts of data, thus reducing the loss of information.

Keywords:. Wireless network. Industrial network. WirelessHART.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACK	*Acknowledge*
AES	*Advanced Encryption Standard*
ASN	*Absolute Slot Number*
CCA	*Clear Channel Assessment*
CRC	*Cyclic Redundancy Check*
CDMA	*Code Division Multiple Access*
DLPDU	*Data Link Protocol Data Unit*
ER	Entidade Relacionamento
FDMA	*Frequency Division Multiple Access*
EMI	Interferência Eletromagnética
IEC	*International Electrotechnical Commission*
ID	Identificador
IEEE	*Instituteof Electricaland Electronics Engineers*
LASCAR	Laboratório de Sistemas de Controle, Automação e Robótica
LQI	*Link Quality Indicator*
MIC	*Message Integrity Check*
P2P	*Peer-to-Peer*
RF	Rádio Frequência
RX	Recepção
SF	SupreFrame
TDMA	*Time Division Multiple Access*
TX	Transmissão
WH	WirelessHART

SUMÁRIO

1 INTRODUÇÃO

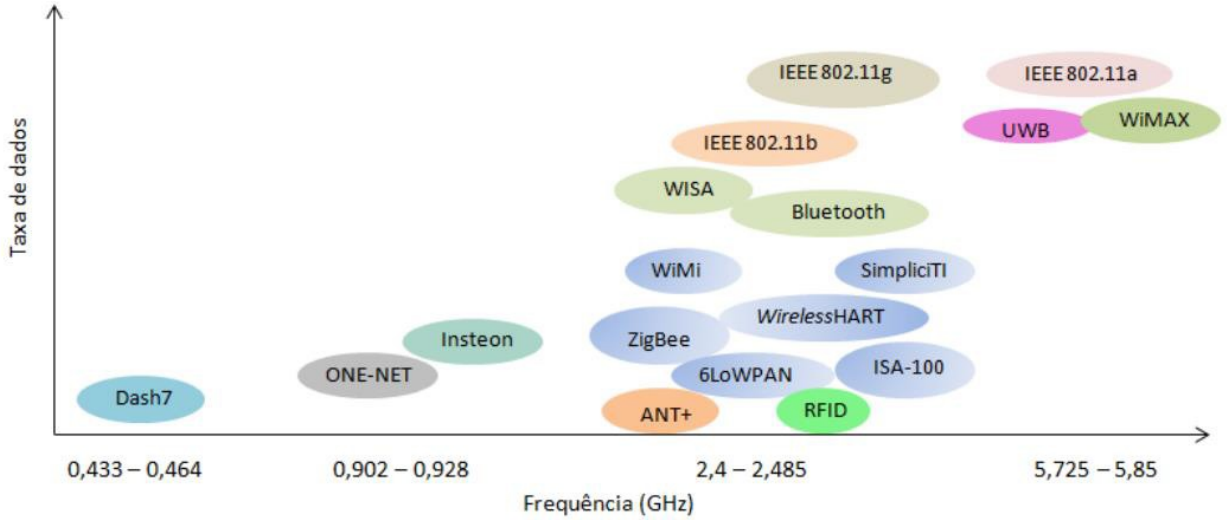
O avanço tecnológico presenciado nas últimas décadas, permitiu uma grande evolução no setor das comunicações. Não somente em função do desenvolvimento da microeletrônica, mas também para acompanhar os requisitos tecnológicos da indústria.

A comunicação se torna vital onde a presença humana é perigosa ou inacessível, como locais onde a quantidade de radiação é maior do que a suportada pelos seres. O envio de algum dispositivo que substitua a presença humana, torna todo esse processo menos perigoso e oneroso. Para esses aparelhos serem controlados de forma remota, a comunicação é fundamental. Outro local em que, nas últimas décadas, os dispositivos controlados remotamente estão sendo utilizados é na indústria.

Os sistemas de comunicação sem fio têm passado por melhorias tecnológicas durante as últimas décadas, e em muitas aplicações se tornado a melhor escolha. Ela apresenta diversas soluções para o chão de fábrica, ambientes agropecuários e diversos outros locais, e resolvem tradicionais problemas provenientes destes ambientes, em comparação aos sistemas cabeados. Os principais benefícios, comparativamente com o cabo, são custos menores de instalação e manutenção, ganhos em flexibilidade e confiabilidade. Todavia, aparecem novos obstáculos a serem transpostos, tais como o aumentando a vida útil dos dispositivos, visando o baixo consumo de energia, e a preocupação com a interferência na comunicação. ISA-100, 6LoWPAN, WirelessHART e ZigBee são exemplos desse tipo de tecnologia (MULLER, 2011).

Nos últimos anos, diversas tecnologias sem fio foram desenvolvidas e a maioria dessas não está preparada para coexistir com as outras. Uma faixa de frequência largamente utilizada é a faixa de 2,4 GHz, conforme apresentado na Figura 1.1, deixando o problema da interferência ainda mais agravado.

Figura 1.1: - Protocolos de comunicação e faixas não licenciadas do espectro de frequência



Fonte: Winter (2014).

Produzir um dispositivo que seja capaz de organizar e se adaptar a diversas interferências é de grande importância. Visto isso, este trabalho, desenvolvido no Laboratório de Sistemas de Controle, Automação e Robótica (LASCAR) da Universidade Federal do Rio Grande do Sul, apresenta a implementação da proposta de um modelo de análise de energia dentro do protocolo *WirelessHART* (WH), com o objetivo de obter mais métricas na ocupação do ambiente, a fim de melhorar o uso dos recursos da rede de comunicação sem fio, assim como a organização do envio de dados. Mais especificamente, este estudo se propõe a fazer uma análise da frequência 2,4 GHz, na qual o protocolo WirelessHART é baseado.

O desafio deste trabalho é agregar ao dispositivo WH atual, a característica de medição de energia, e mantê-lo na rede desempenhando suas outras tarefas. Desta forma, não haveria custo monetário adicional para incluir esta característica na rede WH, apenas o consumo de energia que este novo estado despenderá.

2 WIRELESSHART

O protocolo WirelessHART é uma parte da norma HART , atualmente na sua versão 7, na qual a seção “sem fio” foi inserida, assegurando assim a compatibilidade com componentes HART mais antigos. Esta parte da norma HART visa contemplar estruturas onde a inserção de cabos seja inviável, ou simplesmente indesejado. Outro atrativo da norma HART é a aceitação de umas das principais comissões internacionais eletrotécnicas, a IEC (*International Electrotechnical Commission*), afirmando a qualidade da tecnologia e propiciando interoperabilidade entre dispositivos de diferentes fabricantes. O *WirelessHART* apresenta características que configuram este protocolo com alta confiabilidade, podendo estar presente em todas as fases da planta industrial (Nixon, 2010).

2.1 Elementos

A arquitetura do *WirelessHART* é composta por diversos dispositivos, que vão desde dispositivos de campo ao computador que recebe os dados(Nixon, 2010).

O Gateway possibilita a integração do *host WirelessHART* com os principais protocolos de *host* existentes (Modbus, Profibus, Ethernet). O Gateway pode, também, gerenciar a segurança e a rede (Nixon, 2010).

O gerente de rede é responsável pela criação e a manutenção da malha de rede, sempre identificando a melhor rota, além da distribuição dos recursos da rede entre os dispositivos (Nixon, 2010). O gerente de segurança distribui as chaves de criptografia, e também é responsável por manter a lista de dispositivos autorizados a estarem na rede (Nixon, 2010).

O Processo inclui os instrumentos de medição e as instrumentações habilitadas para HART (Nixon, 2010).

O repetidor é um equipamento com a função de repassar a mensagem a fim de aumentar a distância entre dois dispositivos, ou simplesmente contornar um obstáculo. Caso o aparelho de campo não esteja ao alcance de outro rádio, seja por distância ou por obstáculo, o sinal poderá ser roteado para outro dispositivo. Na arquitetura *WirelessHART* todos os dispositivos são possíveis repetidores. Porém, com a função apenas de repetidor, ele não pode gerar novas mensagens (Nixon, 2010).

O Adaptador, como já foi mencionado, a arquitetura WH é compatível com o protocolo HART. Com o adaptador é possível inserir na rede *WirelessHART* um dispositivo HART que não possua conexão sem fio. O adaptador juntamente com o dispositivo HART

será tratado apenas com um aparelho *WirelessHART* (Nixon, 2010).

O terminal portátil tem a função de verificar e calibrar os dispositivos de campo, sendo utilizados em manutenção de rotina e também o terminal portátil é utilizado para introduzir um novo dispositivos em uma rede *WirelessHART* que já existente. (Nixon, 2010).

O aparelho de campo, do inglês *field device*, é o comunicador final, o que obtém os dados da planta via sensor e os transmite (Nixon, 2010).

2.2 Camada OSI

O modelo OSI tem como objetivo ser uma padrão para os protocolos de comunicação fim-a-fim, permitindo a comunicação em uma rede heterogênea. Este modelo é um conjunto de sete camadas que pode analisar cada camada separadamente e abstrair as demais. Esta arquitetura é dividida em: Física, Rede, Enlace, Transporte, Sessão, Apresentação e Aplicação. A arquitetura WH é compatível com o modelo OSI, respeitando todas as divisões destas camadas, facilitando, assim, qualquer conexão com outros dispositivos que também sejam compatíveis a este modelo. Nesta seção serão apresentadas as camadas Física, de Enlace, de Rede, Transporte e Aplicação, conforme Tabela 2.1. As camadas de Sessão e Apresentação serão abstraídas, pois no protocolo WH não há equivalência com elas (Nixon, 2010).

Tabela 2.1 -Camada OSI do WirelessHART

Camada OSI	Descrição
Aplicação	WirelessHART procedimentos de aplicação, comandos orientados, tipo de dados pré-definidos
Transporte	Transferência de um conjunto de dados, segmentação dos pacotes
Rede	Otimização de energia, redundância de caminho e auto-organização da rede
Enlace	Tempo de sincronização TDMA/CSMA , segurança e confiabilidade
Física	Wireless 2.4 GHz baseado em IEEE 802.15.4, 10 dBm

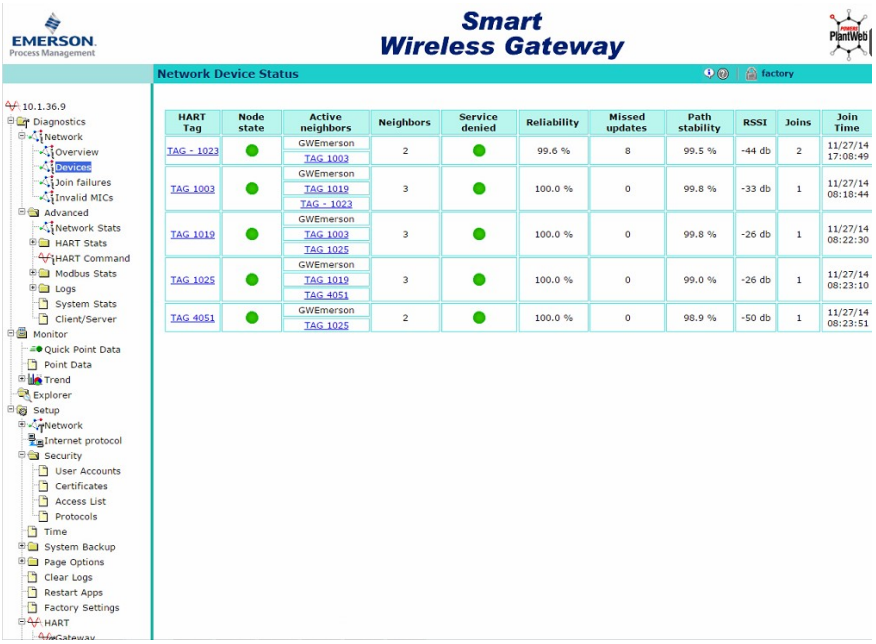
Fonte: HFC (2007).

2.2.1. Camada de aplicação

Na camada de aplicação é onde os programas de alto nível são alocados, como browser de Internet, gerenciador de P2P, compartilhador de vídeos e muitos outros (Kurose, 2014). No caso da arquitetura WH, a camada de aplicação segue as mesmas especificações do HART. O protocolo WH obedece a mesma tabela de comandos, e com esses é possível obter informações de um determinado rádio ou da rede como um todo. Neste trabalho foi utilizado o Smart Wireless Gateway 1420 que possui a aplicação de controle da comunicação dos dispositivos na rede.

A Figura 2.1 representa as opções de gerenciamento da rede que o Gateway proporciona, com essa interface é possível remover dispositivos, consultá-los, ou verificar as estatísticas para determinar se um dispositivo está funcionado de forma esperada.

Figura 2.1: - Aplicação do Gateway 1420



HART Tag	Node state	Active neighbors	Neighbors	Service denied	Reliability	Missed updates	Path stability	RSSI	Joins	Join Time
TAG - 1023	●	GWEmerson TAG 1003	2	●	99.6 %	8	99.5 %	-44 db	2	11/27/14 17:08:49
TAG 1003	●	GWEmerson TAG 1019 TAG - 1023	3	●	100.0 %	0	99.8 %	-33 db	1	11/27/14 08:18:44
TAG 1019	●	GWEmerson TAG 1003 TAG 1025	3	●	100.0 %	0	99.8 %	-26 db	1	11/27/14 08:22:30
TAG 1025	●	GWEmerson TAG 1019 TAG 4051	3	●	100.0 %	0	99.0 %	-26 db	1	11/27/14 08:23:10
TAG 4051	●	GWEmerson TAG 1025	2	●	100.0 %	0	98.9 %	-50 db	1	11/27/14 08:23:51

Fonte: Elaborado pelo autor

2.2.2 Camada de transporte

A camada de transporte é responsável por fazer a ligação entre a camada de rede e a camada de aplicação, tendo como objetivo fornecer um serviço de comunicação diretamente aos processos de aplicação que rodam em servidores distintos. A camada de aplicação determina quais pacotes serão enviados pela rede, caso o pacote seja perdido ou corrompido, esta camada, no dispositivo de origem, pode retransmiti-lo e pois isso, esse transporte é considerado confiável. A camada de transporte também pode ser responsável por fragmentar uma mensagem da camada de aplicação para enviar para a camada de rede. Desta forma a mensagem é dividida e são enviadas separadamente pela camada de rede até o dispositivo destino. Quando estas mensagens chegarem na camada de transporte do destino elas são remontadas, e a camada de aplicação acaba não tomando ciência do fato. (Kurose, 2014). No caso da arquitetura WH, com a redundância de caminhos por diversos motivos, a mensagem pode percorrer caminhos distintos. Para esta camada é indiferente se o dispositivo de campo tem um enlace direto com o Gateway ou se tem diversos dispositivos entre eles, o pacote é tratado da mesma forma (Nixon, 2010).

2.2.3 Rede

A camada de rede é responsável por garantir que o pacote chegará ao destino, escolhendo o melhor caminho, esta camada ainda faz o controle de congestionamento, utilizando rotas auxiliares caso o melhor caminho esteja sobrecarregado, desta forma é possível duas partes da mesma mensagem tomarem rotas distintas (Kurose, 2014). Na arquitetura *WirelessHART* cada dispositivo tem seu ID e com isso é possível determinar quem é a fonte e quem o destino. Quando o dispositivo de campo tenta se conectar à rede desta arquitetura recebe uma chave de segurança fornecido pelo gerenciador da rede. O gerenciador de rede, tendo a relação de todos os dispositivos da rede, calcula o melhor caminho para o envio dos pacotes e, com a chave de segurança, somente os aparelhos fonte e destino poderão decodificar a mensagem, tornando a rede segura (Nixon, 2010). Diferentemente da camada de transporte, se um pacote for fragmentado, a camada de rede garantirá que cada fragmento chegue ao seu destino. Outros recursos muito importantes são as tabelas de rotas e tabelas de tempo. Tabelas de rotas são usadas para encaminhar comunicações ao longo da rede. Tabelas de tempo são usadas para alocar a largura de banda de comunicação para serviços específicos, tais como publicação de dados e blocos de transferência de dados. A segurança garante privacidade e integridade na rede sem fio, assegurando que cada dispositivo tenha um identificador único e este não seja violado.

2.2.4 Enlace

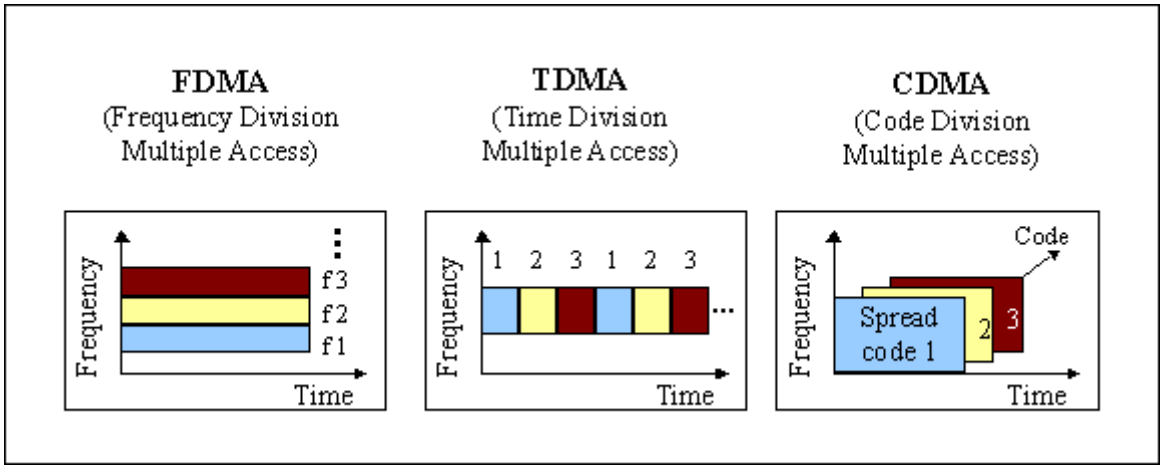
O enlace é a conexão entre dois dispositivos adjacentes, independentemente do meio físico. Compete a camada de enlace garantir que o mensagem chegue ao próximo dispositivo e que haja integridade dos dados. Para um computador se comunicar com um outro computador da mesma rede, ligados por um *switch* são necessários dois enlaces, do primeiro computador até o *switch* e do *switch* até o segundo computador. No caso do *WirelessHART*, cada conexão entre os dispositivos de campo é um enlace. Como são muitos nodos e estamos lidando com tecnologia sem fio, é imprescindível que haja uma forma de gerenciar o compartilhamento deste meio físico. Existem diferentes mecanismos de compartilhamento, tais como FDMA, TDMA e CDMA (Kurose, 2014). A Figura 2.2 ilustra estes métodos.

FDMA é a divisão do meio por frequência, ou seja, a amplitude de frequência é menor para cada dispositivo, diminuindo assim a quantidade de bits por segundo, mas com todo tempo dedicado.

TDMA é a divisão do meio por tempo, ou seja, cada dispositivo pode transmitir uma maior quantidade de bits por segundo, mas em apenas um intervalo de tempo. Esta divisão é utilizada na arquitetura WirelessHART, pois desta forma há maior economia de energia e proporciona uma rede determinística.

CDMA é a divisão do meio por código, sendo que cada dispositivo tem uma codificação específica.

Figura 2.2: - Representação das três formas de compartilhamento de meio



Fonte: Committedto connecting_the world (2005)

O protocolo WirelessHART, como já foi explicado, utiliza o TDMA como forma de compartilhamento do meio. Este protocolo tem algumas peculiaridades sobre o TDMA, ele utiliza o que é chamado SuperFrame, que é composto por um conjunto de *slots*, e também utiliza saltos de canais. Os *slots* são compartilhados em pares para os dispositivos, sendo um como transmissor e outro como receptor. Cabe ao gerenciador da rede determinar qual *slot* será alocado para qual dispositivo, e também em qual canal será utilizado.

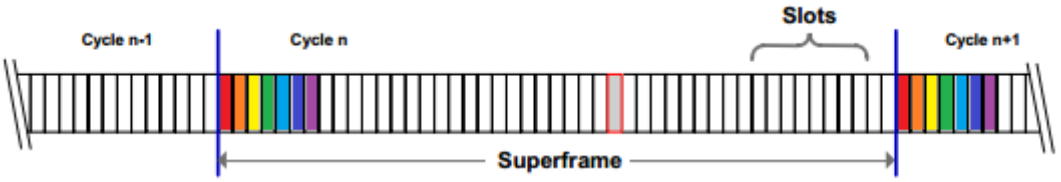
Quando ocorre a transmissão de um DLPDU (*Data Link Protocol Data Unit* – Unidade de Dados do Protocolo da Camada de Enlace), o dispositivo transmissor aguarda a confirmação do recebimento, chamada de ACK (*Acknowledgment*- Confirmação). Caso a mensagem seja do tipo *broadcast* (Todos receptores), não ocorrerá ACK (Kurose, 2014).

2.2.4.1 Superframes

O SuperFrame é a denominação que recebe o intervalo de tempo que contém um conjunto de *slots* (HCF, 2007).

A Figura 2.3 ilustra o SuperFrame (SF), o qual se repete de forma contínua, ou seja quando o SF *n* acaba, o SF *n+1* é iniciado, seguindo a sequência anterior.

Figura 2.3: - SuperFrame



Fonte: HCF (2007) modificado.

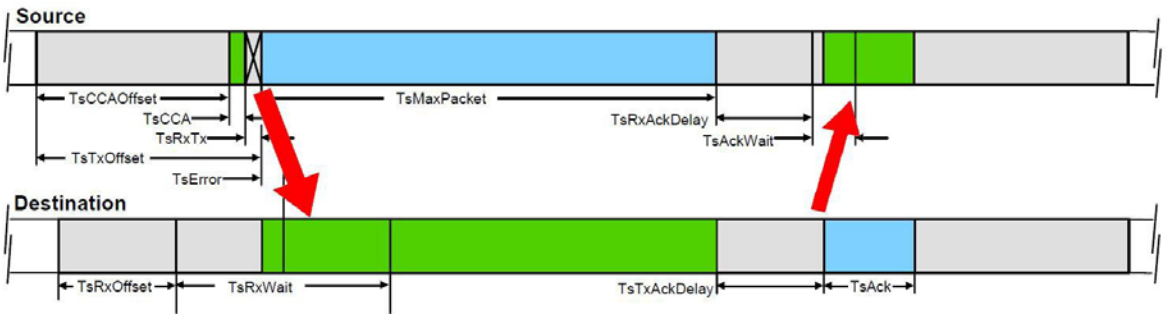
2.2.4.2 ASN

Cada *Slot* tem seu identificador que determina a ordem dentro do SuperFrame. O *Absolut Slot Number* (ASN), identifica o *slot* ao longo do tempo transcendendo o SF.

2.2.4.3 Slot

Slot é uma subdivisão do SuperFrame, e neste intervalo de tempo é possível fazer a transmissão do DLPDU e a conformação do mesmo pelo ACK. Então, o mesmo *slot* é compartilhado entre dois dispositivo; contudo um será para transmissão e outro para recepção. O *slot* tem o tamanho de 10 ms, sendo que deste intervalo de tempo, apenas 4256 µs é para transmissão (HCF, 2007).

Figura 2.4: Temporização do *Slot*



Fonte: TDMA Data Link Specification (2007) modificado

A Figura 2.4 representa a transmissão que ocorre em um *slot*. A barra superior é a do transmissor e a barra inferior é a do receptor. O *time slot* do transmissor se inicia com os preparativos para a transmissão, calculando o Cyclic Reduncancy Check (CRC) e encapsulando os pacotes. Todas essas atividades ocorrem no intervalo de tempo TsCCAOffset. Ao término deste processo, ocorre o CCA, período conhecido como TsCCA, e a ativação do modo de transmissão ocorre no TsRxTx. Se no CCA for verificado que o canal está ocupado, o processo de transmissão cessa imediatamente e o DLPDU é realocado para o próximo *slot*; caso contrário, após o TsRxTx ocorre o TsAckWait, que é o período de confirmação da entrega dos dados (HCF, 2007).

Com o dispositivo receptor, o processo se inicia no TsRxOffset. O rádio fica "escutando", esperando receber a mensagem no intervalo TsRxWait, e se vale da função *drift*, que ressincroniza o *time slot.* Ao receber o sinal, o rádio verifica se o endereço destino é o seu, e, se confirmado o destinatário, ocorre a verificação do DLPDU. Se este estiver integro, é transmitido o ACK, porém essa verificação demora alguns microssegundos e este tempo é conhecido como TsTxAckDelay, conforme Tabela 2.2 (HCF, 2007).

Tabela 2.2- 2450MHz IEEE 802.15.4-2006 Temporização e especificação.

TsTxOffset	Tempo entre o início do time *slot* e o início da transmissão da mensagem	2120 µs ± 100 µs
TsRxOffset	Tempo entre o início do time *slot* e o início da escuta por comunicação	1120 µs ± 100 µs
TsRxWait	Tempo de espera pelo início da mensagem	2200 µs ± 100 µs
TsMaxPacket	Comprimento máximo do pacote (inclui cabeçalho, ou seja, 133 bytes)	4256 µs
TsTxAckDelay	Tempo entre fim da recepção e início da transmissão do ACK	1000 µs ± 100 µs
TsRxAckDelay	Tempo entre o fim da transmissão e início da escuta pelo ACK	900 µs ± 100 µs
TsAckWait	Mínimo tempo de espera do início do ACK	400 µs ± 100 µs
TsAck	ACK (26 bytes)	832 µs
TsCCAOffset	Tempo entre o início do time *slot* e o início do CCA	1800 µs ± 100 µs
TsCCA	Tempo de execução do CCA	128 µs
TsRxTx	Tempo de comutação entre transmissão e recepção	192 µs

Fonte: HCF (2008)

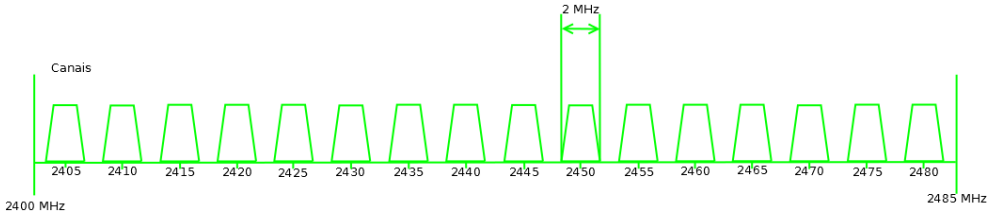
2.2.5 Camada física

A camada física é o meio que conecta cada dispositivo, ligando cada par

separadamente, gerando assim a transmissão entre dispositivos (Kurose, 2014). No caso do protocolo *WirelessHART* utiliza-se o ar como meio e baseia-se no padrão IEEE 802.15.4, com uma frequência de 2.4 GHz, conjunto de 16 canais e taxa de transferência de 250 kbit/s. Este padrão do *Instituteof Electricaland Electronics Engineers* (IEEE) é utilizada por diversas tecnologias, como ZigBee, ISA100.11a,WirelessHART, e MiW.

Os 16 canais do WH são definidos de 11 a 26, contudo o canal 26 é empregado em outros sistemas RF, sendo assim o WH utiliza apenas do canal 11 ao 25. Cada canal possui uma largura de banda de 2MHz e a distância entre os canais adjacentes é de 5MHz. A Figura 2.5 representa todos os canais do IEEE 802.15.4 (HCF, 2008).

Figura 2.5: - Canais do Protocolos WirelessHART

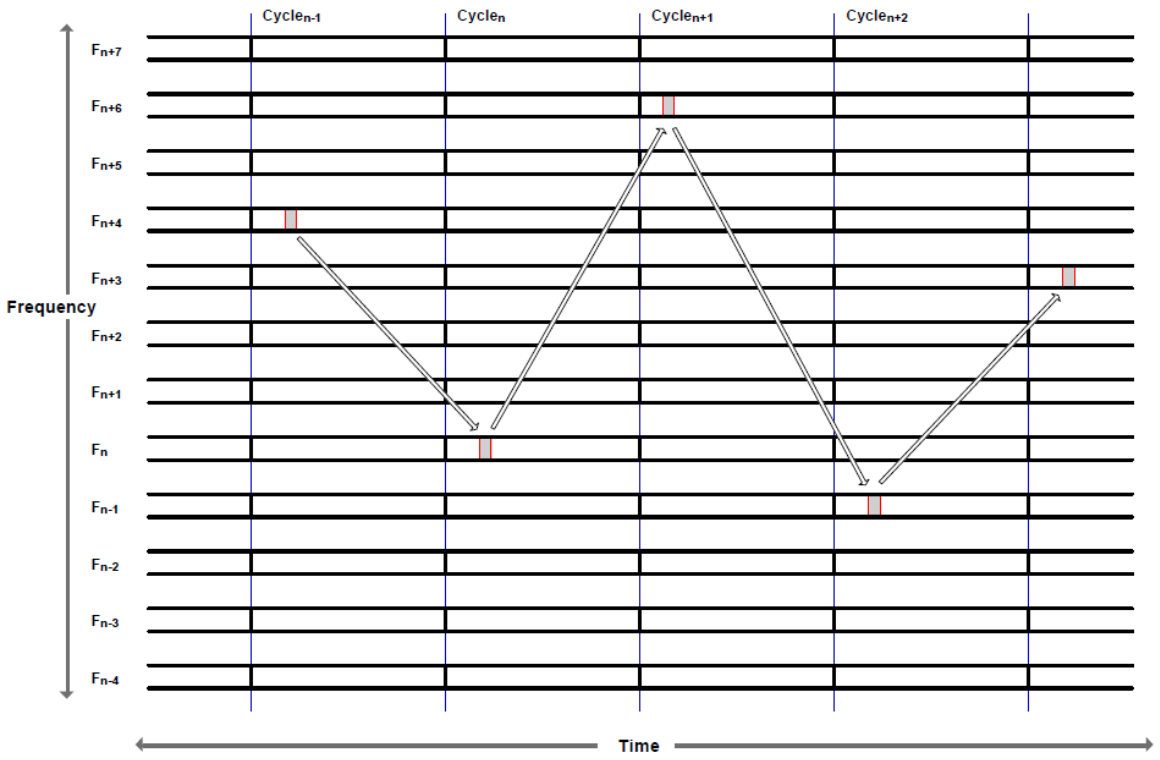


FONTE **:** WirelessHART: The first wireless standard for industrial applications (2013) Modificado

2.2.5.1 Saltos de canais

Com o objetivo de deixar a rede mais segura e confiável, o protocolo WH utiliza saltos de canais, desta forma fica mais difícil para algum dispositivo mal intencionado obter informações sobre a rede, uma vez que este não tem a informação dos canais a serem utilizados. Essa troca de frequência ocorre independente de qualquer condição do ambiente, os canais a serem utilizados são determinados através de uma equação que relaciona o ASN, o offset do link e os canais atribuídos para a rede. O rádio receptor e o transmissor conhecem o canal a ser utilizado nos seus *slots*, *slot* de transmissão (TX) e *slot* de recepção (RX). A Figura 2.6 representa o chaveamento entre canais, mostrando que ao longo do tempo o mesmo enlace recebe diferentes canais para a comunicação (HCF, 2007).

Figura 2.6: - Salto de Canal



Fonte: TDMA Data Link Layer Specification

2.2.5.2 Funcionalidades da camada Física

ED – *Energy Detection*, detecção de energia.

Um valor medido do meio físico, que mede a potência de sinal recebido dentro da largura de banda de um determinado canal. O período de mensuração é de 128µs (HCF, 2007).

CCA – *Clear Channel Assessment*, avaliação do canal utilizado.

Avalia o uso do canal, ou seja, determina se o mesmo está ocupado, prevenindo assim possíveis perdas de pacote (HCF, 2007).

LQI – *Link Quality Indicator*, indicador de qualidade do link.

Apresenta a intensidade e/ou qualidade do pacote recebido. Essa medida pode ser obtida a partir do ED, uma estimativa do sinal-ruído ou uma combinação de ambos (HCF, 2007).

2.3 Características do *WirelessHART*

O protocolo WH é robusto, confiável, seguro e de simples implementação. Ele disponibiliza as vantagens da tecnologia sem fio de maneira rápida e fácil ao usuário (Nixon, 2010).

2.3.1 Confiabilidade

Além do salto de canais, a rede WH possui diversos caminhos redundantes que aumentam a chance de que a mensagem chegue ao seu destino antes do *timeout*. Como a faixa de frequência desta arquitetura é muito utilizada, há também a preocupação que a rede coexista com outras redes, sendo assim é possível que o usuário selecione os canais a serem transmitido, evitando os já utilizados. A otimização da largura de banda e a sincronização para envio de mensagens no tempo determinado também contribuem para garantir 99.9% de confiabilidade desta tecnologia (Nixon, 2010).

2.3.2 Segurança

A arquitetura WH possui um conjunto de ferramenta para a segurança da rede que são divididas em dois tipos:

2.3.2.1 Proteção da rede sem fio

O protocolo tem o nível de potência de transmissão ajustável que reduz o alcance da rede, diminuindo assim os locais que um *sniffer* possa monitorar a rede WH.

Os múltiplos níveis de chaves de segurança de acesso fazem com que um dispositivo mal intencionado, que tenha entrado na rede de forma autêntica, não se comporte como um dispositivo gerenciador, como no caso do Gateway (Nixon, 2010).

A indicação de tentativas de acesso fracassadas, notificação de falhas na integridade de mensagens e notificação de falhas de autenticação, também auxiliam a detectar possíveis intrusos na rede (Nixon, 2010).

2.3.2.2 Proteção de informação

Como proteção de informação existem diversas ferramentas, como: chave de

segurança em múltiplos níveis, criptografia *Advanced Encryption Standard* (AES) de 128 bits padrão, chave de criptografia exclusiva para cada mensagem, integridade de dados, autenticação de dispositivos e alternância de chaves de criptografia. Tornando o WirelessHART uma arquitetura segura (Nixon, 2010).

2.3.3 Distância de alcance

A norma HART estabelece duas estimativas de distâncias, para ambientes *outdoor* (com linha de visada direta) e ambientes *indoor* (sem linha de visada direta), que são apresentadas na Tabela 2.3.(Nixon, 2010).

Tabela 2.3 - Distância de comunicação entre dispositivos WH

Ambientes *indoor*		Ambientes *outdoor*	
Potência de transmissão (dBm)	Distância (m)	Potência de transmissão (dBm)	Distância (m)
0	35	0	100
10	75	10	250

Fonte: HCF (2007)

2.3.4 Tipos de Mensagens no WirelessHART

A norma WH define 5 tipos de mensagens, as quais são apresentadas abaixo:

Advertisement: para um dispositivo conseguir se juntar a rede esta mensagem é utilizada. Quando um dispositivo deseja unir-se à rede, ele fica “escutando-a” e esperando por estes pacotes, e se vale das informações contidas nele para sincronizar-se com a rede, e desta forma iniciar o processo de agregação (*Join*) (Nixon, 2010).

Data: são as DLPDUs que contém informações dos dispositivos e da rede (Nixon, 2010).

Keep-Alive: são usados para garantir que ainda há conexão entre dispositivos vizinhos. O *payload* destas mensagens é vazio e em muitas vezes são usados para sincronizar a rede, dado que o ajuste de tempo será retornado pelo ACK correspondente.(Nixon, 2010).

Disconnect: é gerado por dispositivos que estão deixando a rede, ou seja, o dispositivo não estará mais disponível para comunicação, e deve ser removido da lista de dispositivos, assim como todos os links envolvidos (Nixon, 2010).

ACK (*Acknowledgment*): é transmitido pelo rádio receptor para confirmar a recepção de um DLPDU, todavia se este pacote se tratar de *broadcast*, o ACK não ocorre. A transmissão só acontece após o dispositivo receber e confirmar a integridade dos dados (Nixon, 2010).

3 TRABALHO DESENVOLVIDO

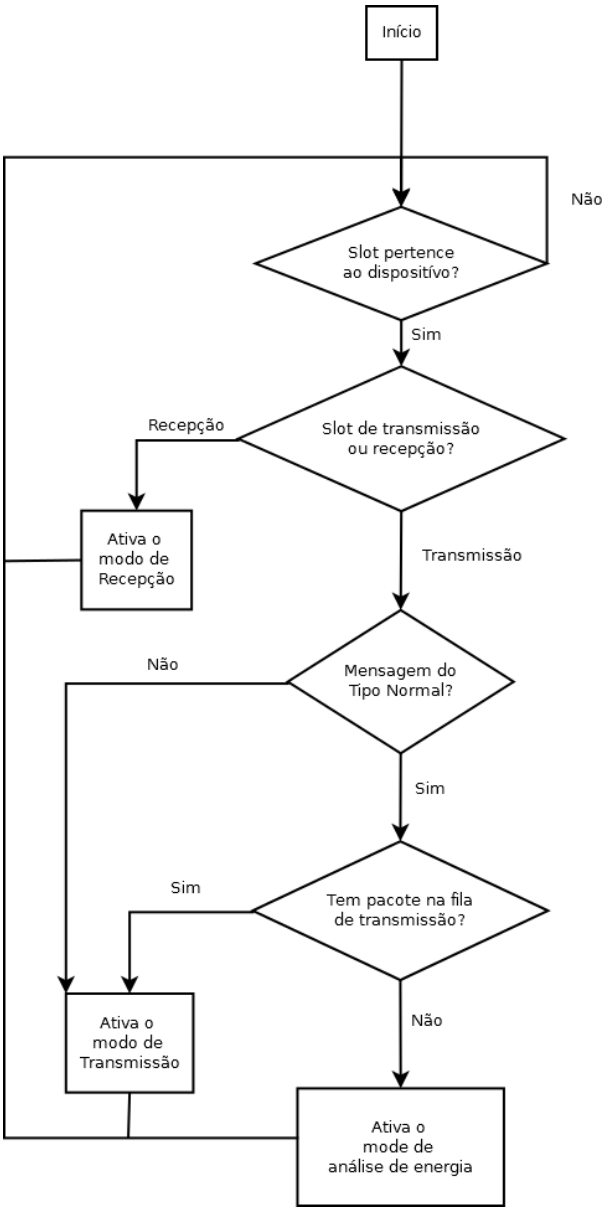
3.1 Projeto

Este trabalho propõe a inserção de um novo mecanismo de sensoriamento de espectro dentro do protocolo WH, com o objetivo de buscar novas métricas para avaliar o uso do espectro de frequência. A literatura descreve diversos métodos para o sensoriamento do espectro como: filtros combinados, detecção de energia, ciclo estacionário e forma da onda (Cabric, 2004). Como a tecnologia utilizada é calcada em temporização e se quer fazer o sensoriamento de espectro em um intervalo de tempo bem definido e com baixo processamento de informação o método utilizado é a detecção de energia.

O trabalho faz parte da proposta apresentada em (Winter, 2014), onde é proposto o desenvolvimento de métodos para o melhor uso dos recursos dentro de uma rede WH (Winter 2014). No trabalho desenvolvido por (Machado, 2011), a detecção de energia ocorria de forma a analisar uma grande parte do espectro do *slot*, todavia o dispositivo utilizado era dedicado a esta função e utilizava uma biblioteca que, ao juntar ao programa já desenvolvido, tornava-se muito grande para as especificações do dispositivo.

Atualmente, o dispositivo torna ao estado *idle*, esperando o próximo *slot*, se no *slot* reservado para que haja a transmissão de algum dado, a fila de pacotes a serem transmitidos estiver vazia. O trabalho desenvolvido visa aproveitar este momento em que os rádios estejam ociosos para estudar o comportamento do ambiente. A proposta é que ao invés deste rádio ir para o estado de baixo consumo, vá para o estado de detecção de energia (ED), como é ilustrado na Figura 3.1. Visto que a transmissão de dados não é cíclica, e o rádio opera nos canais WH disponíveis, cada dispositivo cobrirá esses canais da rede.

Figura3.1: - Fluxograma para o estado de detecção de energia



Fonte: Elaborado pelo autor.

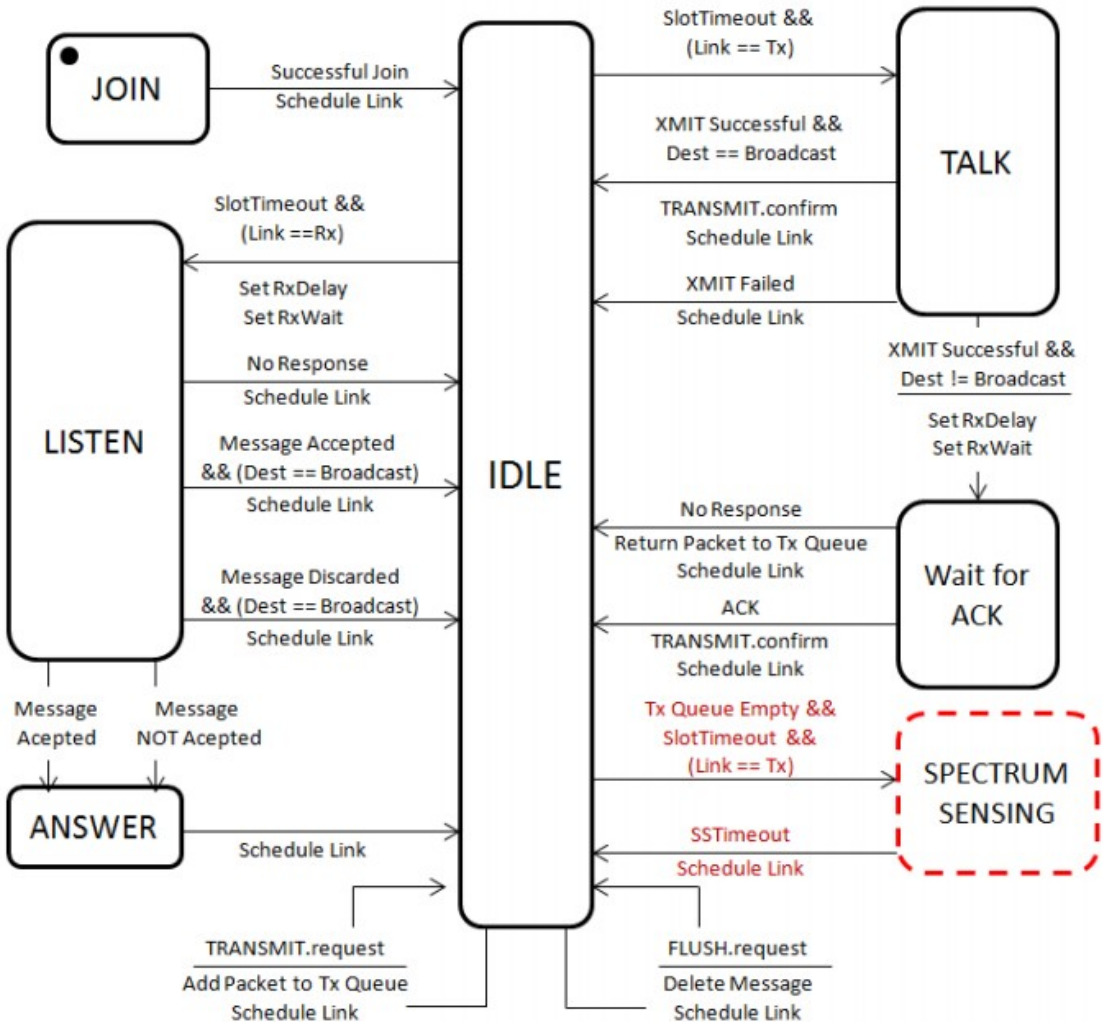
Atualmente, o WH já utiliza o CCA que, antes de enviar o DLPDU, verifica se o canal está ocupado. Contudo, esta informação não é enviada para o gerenciador de rede. Para que seja possível a adaptação da rede, perante o ambiente, apenas a informação de canal ocupado não é suficiente. Identificar qual a magnitude da interferência, qual canal, em qual *slot* e qual o vizinho compartilha o mesmo *slot* são informações cruciais para a adaptação da rede.

Como a coleta dessas informações utilizarão um *slot* de transmissão, o envio delas não ocorrerá no mesmo instante da sua detecção, para isso um buffer foi desenvolvido para armazenar os dados e, quando solicitado, o dispositivo enviará para o gerenciador estas informações.

3.2 Estados da Rede WirelessHART

A arquitetura WH foi projetada com seis estados no *firmware*, estes estado auxiliam o funcionamento dos dispositivos e a capacidade de entrar e se comunicar na rede WH. No trabalho de (Winter, 2014), o sétimo estado é inserida, para possibilitar a detecção de energia, conforme pode ser observado na Figura 3.2. Abaixo desta, estão descritos os estados representados na mesma, se iniciando pelo *Join*.

Figura 3.2: - Máquina de estados WirelessHART



Fonte: Winter (2014)

Join; o processo de *Join* é feito quando um determinado rádio entra na rede WH. O dispositivo fica “escutando” os canais do protocolo, recebendo assim as informações de SuperFrame, *graphs* e *links* (HCF, 2009).

Talk; após o dispositivo entrar na rede WH, e ele estiver em seu *slot* de TX, o mesmo pode transmitir seus dados, sendo este estado conhecido como *Talk*. Ao término deste envio, o dispositivo entra no estado de *Wait for* ACK (HCF, 2009).

Wait for ACK; após a transmissão, o dispositivo precisa se certificar de que a informação foi recebida de forma correta. Esta confirmação é o ACK, que é enviado pelo receptor logo que confirmada a integridade do dado. Caso o destinatário não receba os dados, não será gerado o ACK (HCF, 2009).

Listen; após o dispositivo entrar na rede WH, e ele estiver em seu *slot* de RX, o mesmo pode receber os dados, estado conhecido como *Listen*. Ao final do recebimento, este dispositivo entra no estado *Answer* (HCF, 2009).

Answer; ao final do recebimento do pacote, este estado é ativado para informar se os dados foram recebidos de forma correta, transmitindo ou não o ACK, estado conhecido como Answer (HCF, 2009).

Idle; quando o dispositivo não está em outro estado, este é habilitado. O *Idle* também é ativado na troca de estados ou em eventos, como *Timeout Slot, Flush, Transmit, Request* e eventos para agendar novos *links* e SuperFrame (HCF, 2009).

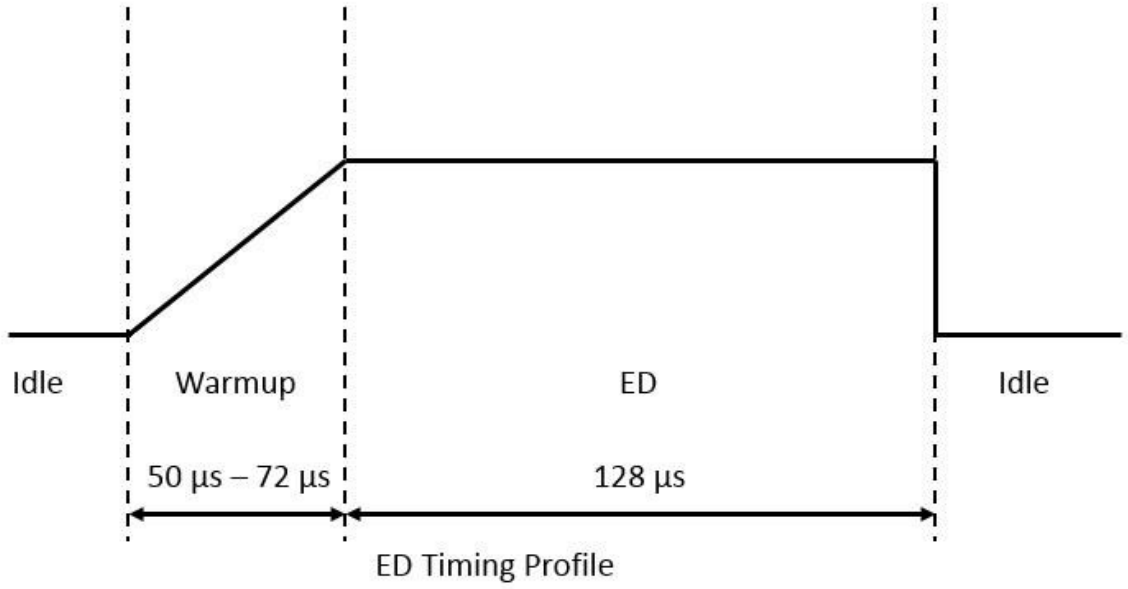
Spectrum Sensing; neste estado é proposta a realização da análise de energia durante o período do *slot* de transmissão dos links do tipo normal, dentro da condição de que a fila de pacotes a serem enviados esteja vazia. No momento em que o dispositivo estiver inativo, nas situações já citadas, este estado se tornará ativo (Winter 2014).

Então este trabalho visa o desenvolvimento deste estado, a validação do método utilizado para detecção de energia e também o armazenamento e envio dos dados ao gerenciador de rede.

5.3 Análise de energia

A energia é detectada pelas antenas dos dispositivos, podendo provir de diversas fontes. O processo de detecção de energia é empregado no CCA, que faz a verificação do canal antes da transmissão, para reduzir as colisões (HART COMMUNICATION FOUNDATION 2008). Todavia este trabalho se propõem a utilizá-lo de forma diferenciada, fazendo uma detecção mais prolongada no *slot* de transmissão. A função de detecção de energia no CCA é documentada na norma do WH, e, segundo a sua arquitetura, antes da detecção de energia (ED), o dispositivo passa por um intervalo de transição (Warmup) de 50 µs a 72 µs, e o tempo para se obter a energia é de 128 µs, como a Figura 3.3 apresenta.

Figura 3.3: Tempo de ED

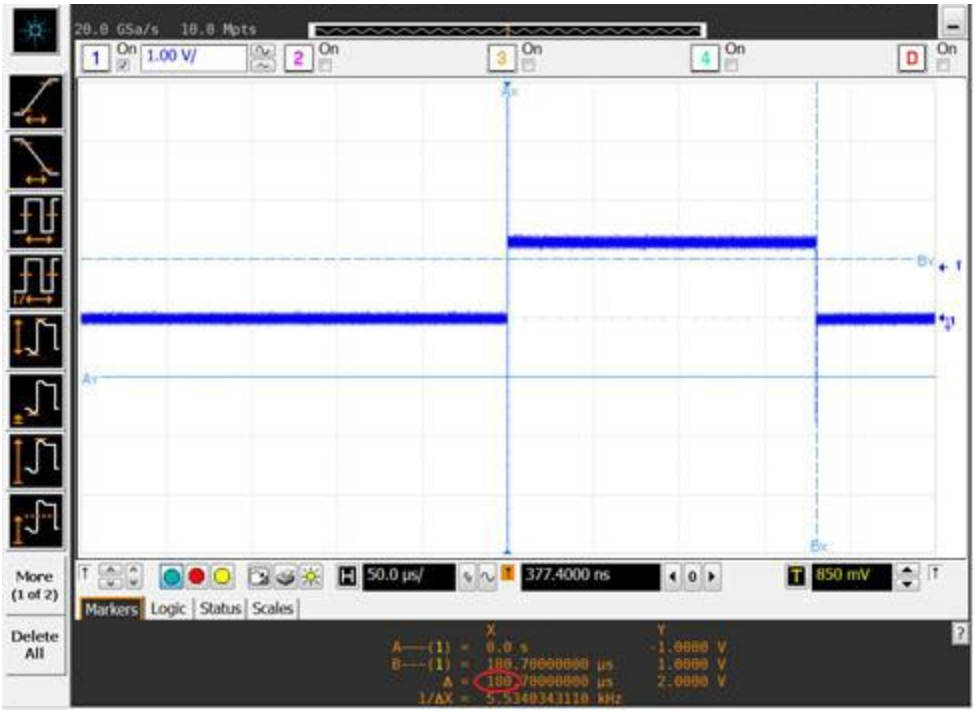


Fonte: HCF (2008) Modificado

3.3 Aferimento do ED

Como já foi informado, o período de medição do ED é de 128 µs, com uma espera de 50 µs de Warmup, sendo o intervalo de aferição de 178 µs.

Figura 3.4: - Intervalo de detecção de energia



Fonte: Elaborado pelo autor.

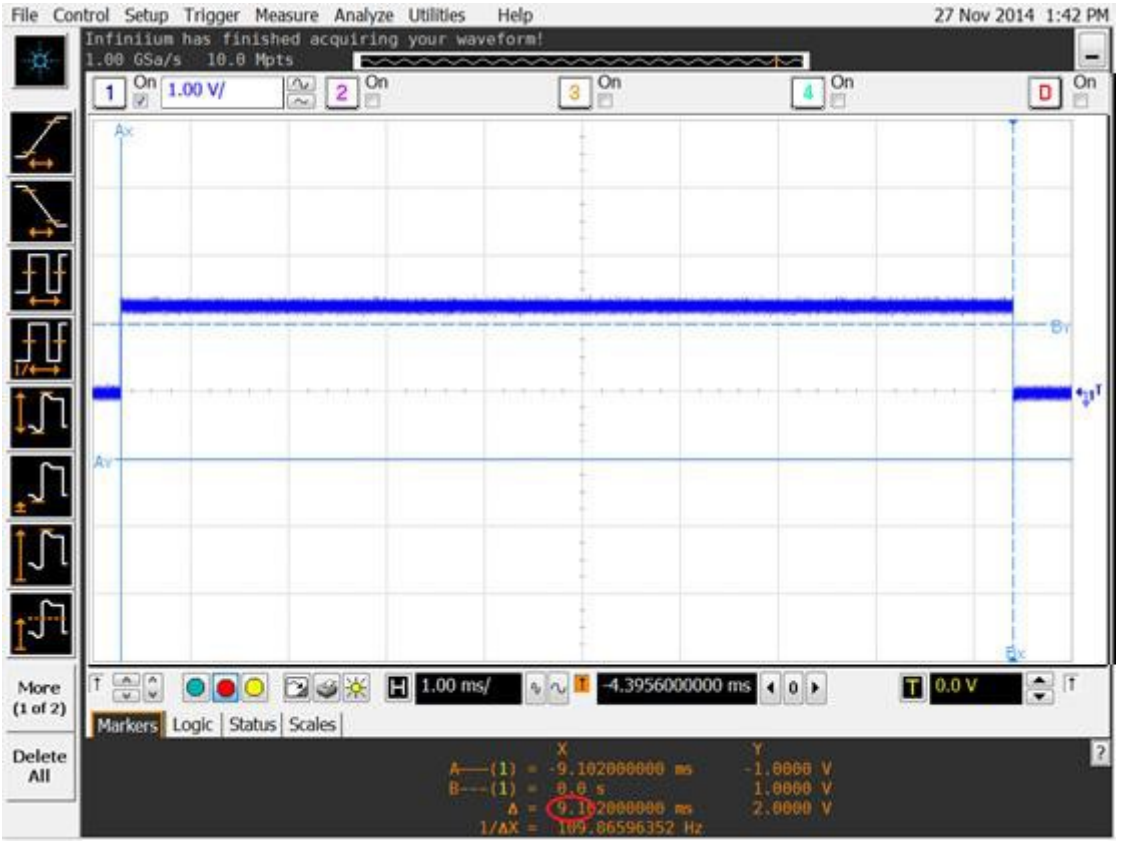
A Figura 3.4 Ilustra a medida feita em um osciloscópio em nível de hardware, ativando um pulso em uma porta de saída quando a função ED e desligando este pulso quando esta função cessa. É possível identificar a diferença entre o começo e o final do pulso, que ocorre durante a chamada da função de detecção. Nesta figura, o intervalo é de 180 µs e, a diferença de 2 µs deve-se ao cálculo do ED e iterações de controle.

O valor de 180 µs é muito inferior ao tempo do *slot*, que é de 10 ms. Desta forma foi feito um laço para fazer diversas medições e, após este, é calculada uma média entre elas, pois armazenar o histórico de cada medida ocuparia muita memória e como o WH é fundado em temporização um método que dispendesse muito tempo ou processamento do dispositivo poderia dessincronizá-lo, e desta forma, ele poderia sair da rede.

Atualmente, com o laço executando diversas aferições do ED, o tempo total de medição é de mais de 9 ms, conforme observado na Figura 3.5 de um osciloscópio, que gera

um pulso que se inicia e se encerra junto da função ED. Durante este intervalo ocorrem 42 aferições, podendo-se concluir que o tempo real de mensuração é de 5,376 ms (42 x 128 µ$\square$ = 5,376 $\square\square$), porém, desta forma, temos 2,1 ms de *Warmup e 1,26 ms de Idle*. Então, no intervalo de 10 ms, é possível medir por volta de 53% deste tempo.

Figura 3.5: Intervalo de tempo de detecção de energia



Fonte: Elaborado pelo autor.

Com este tempo de 9 ms é possível medir quase toda fração do *slot* destinada a comunicação, pois, no pior dos casos, quando são somados os maiores tempos referentes a transmissão, visualizados na Tabela 2.2 (TsCCAOffSet, TsCCA, TsRxTx, TsTxOffset, TsMaxPacket, TsRxAckDalay e TsAckWait), tem-se o tempo total necessário para completar uma transmissão e confirmá-la, sendo este de 9796 µs (2120 µs + 128 µs + 192 µs + 1800 µs + 4256 µs + 900 µs + 400 µs).

De acordo com (IEEE, 2011), os valores máximos e mínimos de detecção de energia são 0xFF e 0x00, respectivamente. Esses valores são associados à quantidade de energia detectada pelo receptor com no máximo -15 dBm e no mínimo -100 dBm. Para chegar neste

valor é utilizada a seguinte equação.

$$\text{[illegible]}_{\text{[illegible]}m} = \frac{\text{[illegible]}_{\text{[illegible]}}}{3} - 100 \quad (1)$$

Fonte: HART Communication Foundation (2008)

3.4 Validação do Projeto

Para a validação do projeto foram propostas quatro verificações:

1) Comprovar que o *slot* pertence a um *slot* TX, e a mensagem é do tipo normal;

2) Se assegurar de que a fila de pacotes esteja vazia;

3) Analisar o comportamento do dispositivo na rede WirelessHART;

4) Checar a medida de energia em diferentes circunstâncias.

3.4.1 Verificação *Slot* TX e tipo Normal

Na camada de aplicação do protocolo WH, o comando 784 (*Read List Link* – Ler a Lista de Links) retorna como informação todos os links de um determinado dispositivo, como pode ser verificado na Tabela 3.1.

Tabela 3.1 - Dados de resposta do comando 748

Byte	Formato	Descrição
0-1	Unsigned-16	Índice do link
2	Unsigned-8	Número de links lidos
3-4	Unsigned-16	Número de links ativos
5	Unsigned-8	SuperFrame ID
6-7	Unsigned-16	Número do *slot* no SuperFame deste link
8	Unsigned-8	ChannelOffset deste link
9-10	Unsigned-16	Nickname do vizinho deste link, se broadcast o valor será 0xFFFF
11	Bits-8	LinkOptions, define se o link é de Transmissão, recepção ou compartilhamento, ver tabela LinkOptions
12	Enum-8	LinkType, ver define se o link é do tipo normal, de descobrimento broadcast e join, ver tabela LinkType
13-...		Volta para o *byte* 5 e o processo se repete até o *byte* 12

Fonte: Wireless Command Spefication (2008).

Através do comando 784 foi realizada a leitura dos links utilizados pelo dispositivo, com estes dados as informações foram separadas e interpretadas, gerando a Figura 3.6. A linha em azul refere-se ao número do *slot* no SuperFrame, em decimal. Com os dados obtidos é possível determinar o LinkOption (Tabela 3.2) e o LinkType (Tabela 3.3) e, desta forma, verificar que o *slot* selecionado está na tabela de links, e é do tipo normal e de transmissão.

Figura 3.6: - Representação da resposta do comando 784 já pré-processada.

Response Data Bytes										
0-1	Link index	00 00								
2	Number of links to read	0A								
3-4	Number of active links	00 0B								
5	Superframe ID	1	0	0	0	4	1	1	0	0	0
6-7	Slot Numberin the superfreme	00F1	219	1	19	001A	001E	00F5	110	119	319
8	ChannelOffset for this link	0	1	0	0	3	1	0	1	2	0
9-10	Nickname of neighbor	FFFF	1	1	1	FFFF	FFFF	F980	F980	1	1
11	linkOptimos tabela 46	2	1	3	1	1	2	1	2	1	1
12	linkType	2	0	1	0	2	2	3	3	0	0
		241	537	1	25	26	30	245	272	281	793

Fonte: Elaborado pelo autor

Tabela 3.2 -LinkOptions

Valor	Nome
0x01	Transmite
0x02	Recebe
0x03	Compartilha

Fonte: Wireless Command Spefication (2008).

Tabela 3.3 -LinkType

Valor	Nome
0	Normal
1	Discovery
2	Broadcast
3	Join

Fonte: Wireless Command Spefication (2008).

Na Figura 3.6, cada coluna representa um link e seus atributos. Os links de transmissão do tipo normal são identificados pela cor verde, e os valores dos *slots* no SuperFrame, em decimal, estão circulados com a cor vermelha. Em contra partida, no dispositivo, o programa foi modificado para apresentar o seu ASN atual, caso fossem obedecidas as condições de ser um *slot* de transmissão e de ser um *slot* do tipo normal. Valendo-se as seguinte fórmula:

$$\text{\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond} \text{ \textdiamond\textdiamond } \text{\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond}a\text{\textdiamond\textdiamond} = (\text{\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond}) \,\%\, \text{\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond} \text{ \textdiamond\textdiamond } \text{\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond} \text{ \textdiamond\textdiamond}$$

$$\text{\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond}a\text{\textdiamond\textdiamond} \qquad (2)$$

Fonte: HCF (2008)

é possível determinar a qual *slot* o ASN pertence.

O modelo de Gateway utilizado neste trabalho coloca todos os *slots* de transmissão no SuperFrame 0, o qual é dividido em 1024 *slots*, sendo assim a equação (2) fica da seguinte forma:

$$\text{\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond} \text{ \textdiamond\textdiamond } \text{\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond}a\text{\textdiamond\textdiamond} = (\text{\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond\textdiamond}) \,\%\, 1024 \qquad (3)$$

A partir da equação (3), a Figura 3.7 foi gerada, e nela pode ser identificada a sequência de *slots* de transmissão do tipo normal. Pode-se observar que, quando comparada à Figura 3.6, as mesmas sequências de *slots* são mantidas, mesmo que a análise comece no meio do SuperFrame, sendo o primeiro *slot* 537 e o segundo 793. Após isso, o ciclo recomeça

a partir do *slot* 25 e segue a sequência 281, 537, e 793. Desta forma fica comprovado que apenas os *slots* do TX e os *slots* do tipo Normal estão sendo verificados.

Figura 3.7: - *Slot* analisados

ASN	1024	ASN	1024
190583321	537	190585881	25
190583577	793	190586137	281
190583833	25	190586393	537
190584089	281	190586649	793
190584345	537	190586905	25
190584601	793	190587161	281
190584857	25	190587417	537
190585113	281	190587673	793
190585369	537	190587929	25
190585625	793	190588185	281

Fonte: Elaborado pelo autor

3.4.2 Verificação de Fila Vazia

No programa, antes do dispositivo entrar no estado de transmissão, a fila de pacotes é verificada. Se não houver dados a serem transmitidos, o dispositivo torna ao estado de *idle* e retorna no próximo *slot*. Essa característica, aumenta a vida útil dos dispositivos, pois reduz o consumo de energia. A função que determina qual será o próximo pacote a ser transmitido, no caso de não haver pacotes, retorna “-1”, tornando a verificação simples.

Figura 3.8: - Representação da resposta do comando 748 já pré-processada.

Response Data Bytes										
0-1	Link index	00 00								
2	Number of links to read	0A								
3-4	Number of active links	00 0A								
5	Superframe ID	1	0	0	4	1	1	0	0	0	0
6-7	Slot Numberin the superfreme	00BA	005E	1	000B	00C3	00C9	015E	025E	031D	035E
8	ChannelOffset for this link	5	6	0	0D	0B	9	6	5	8	0B
9-10	Nickname of neighbor	FFFF	1	1	FFFF	F980	FFFF	1	1	F980	1
11	linkOptimos tabela 46	2	1	3	1	1	2	1	1	2	1
12	linkType	2	0	1	2	3	2	0	0	3	0
		186	94	1	11	195	201	350	606	797	862

Fonte: Elaborado pelo autor

Porém com o objetivo de comprovar que de fato as condições de *slot* TX, *slot* do tipo normal e fila de pacotes vazia foram atendidas foi refeito o teste com o comando 784, em momentos distintos. Novamente os dados foram classificados e interpretados, gerando a Figura 3.8. A linha em azul representa o valor do *slot* no SuperFrame, em decimal, e esta linha

será comparada com a Figura 3.9.

Mais uma vez o programa do dispositivo foi modificado, para apresentar o seu ASN, caso obedecesse às condições de: ser um *slot* de transmissão, de ser um *slot* do tipo normal e a fila de pacotes estiver vazia. Através da equação 3, a Figura 3.9 foi elaborada. Diferentemente da Figura 3.7, a Figura 3.9 apresenta a diferença temporal entre o ASN atual e o ASN detectado anteriormente.

Figura 3.9: - *Slot* analisados e a diferença em milissegundos entre os *slots* analisados

ASN	1024	diferença
103892830	862	
103893086	94	256
103894110	94	1024
103894366	350	256
103894494	478	128
103894878	862	384
103895390	350	512
103895518	478	128
103895646	606	128

Fonte: Elaborado pelo autor

Na Figura 3.9 foram alisados todos os *slot* que estavam ociosos. Diferentemente da Figura 3.7, os resultados obtidos foram não sequenciais. Isto é, não obedecera a ordem dos *slots* de transmissão e dos *slots* do tipo normal. Demonstra-se assim que nem todos os *slots* de transmissão e do tipo normal estão ociosos. O melhor exemplo são os *slots* circulados na cor vermelha, ambos representam o *slot* 94, porém em SuperFrame distintos, ou seja, ocorreu a análise de energia no primeiro *slot* possível, e apenas no próximo SF foi possível fazer outra análise de energia.

3.4.3 Comportamento do dispositivo junto à rede WirelessHART

Juntamente de todos os testes propostos, foi analisado o comportamento do dispositivo na rede WH, com a rede estável, em pleno funcionamento. Nesta verificação, o dispositivo manteve estabilidade na rede, alcançando 100% de confiabilidade com zero perdas pacotes, como verificado na Figura 3.10. Essa verificação foi realizada com uma taxa de publicação de 4 segundos, e ficou em análise durante aproximadamente 12 horas.

Taxa de publicação é o intervalo de tempo em que o dispositivo de campo transmite os dados de medição para o Gateway testes (Emerson Process Management, 2012). Ainda foi constatado que, para tempos inferiores, ocorrem perdas de mensagens, inclusive em

dispositivos comerciais que foram utilizados como referência nos.

Figura 3.10: - Comportamento das aparelhor na rede WH

HART Tag	Node state	Active neighbors	Neighbors	Service denied	Reliability	Missed updates	Path stability	RSSI	Joins	Join Time
TAG - 1015	●	GWEmerson TAG 1003	2	●	100.0 %	0	97.8 %	-44 db	1	11/24/14 17:08:00
TAG 1003	●	GWEmerson TAG - 1015	2	●	100.0 %	0	97.8 %	-72 db	1	11/23/14 20:01:41

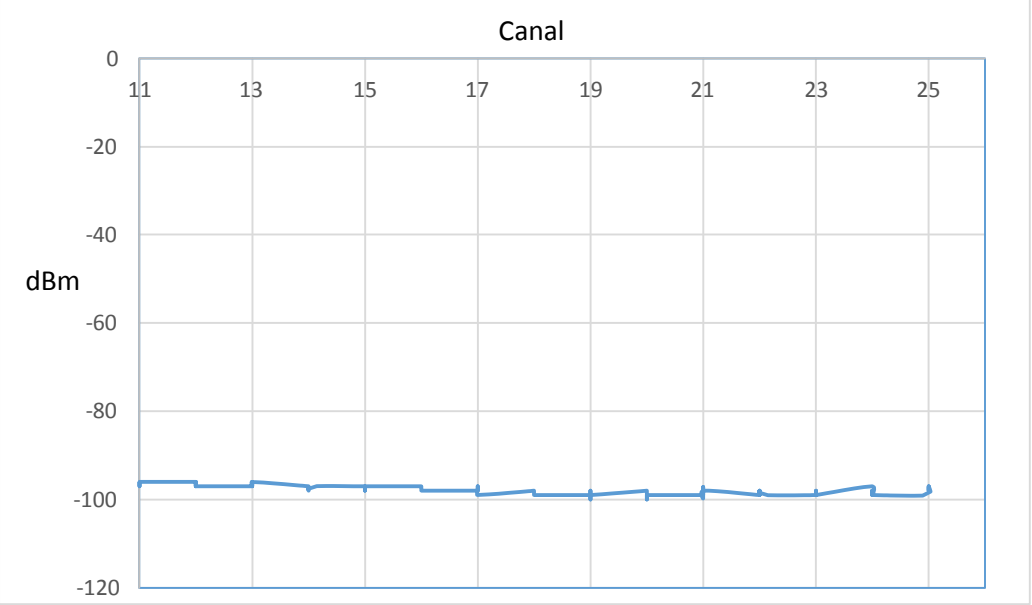
Fonte: Elaborado pelo autor.

3.4.4 Testes com diferentes sinais

Para testar se a função de detecção de energia se comporta de forma correta foram realizados diversos testes.

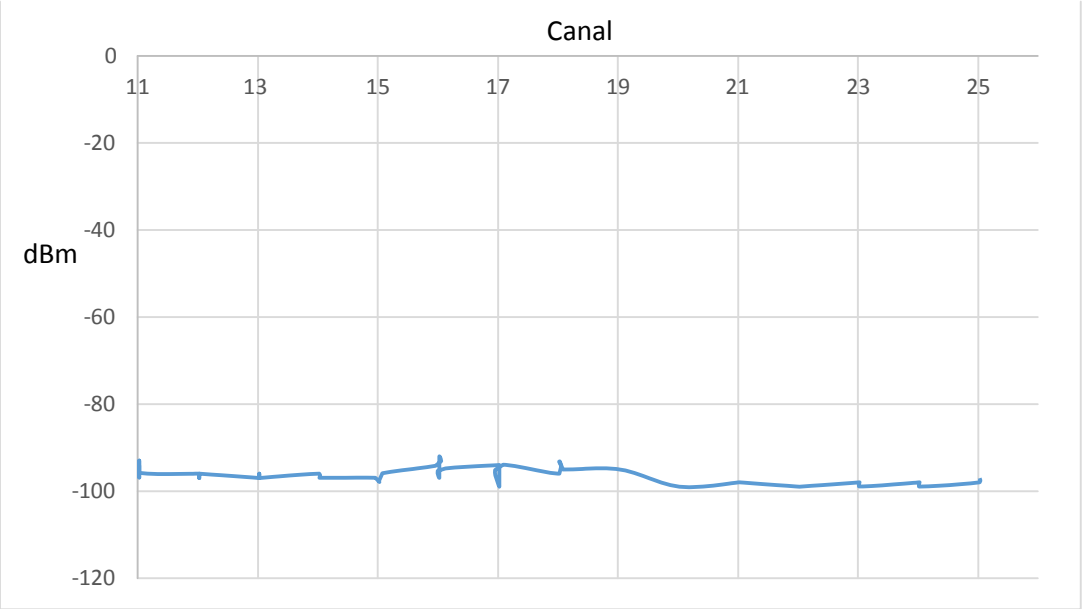
A Figura 3.11 apresenta a análise de energia com pouca interferência tendo a média das amostras dos canais em -98 dBm. Já a Figura 3.12 apresenta interferência dos canais 15 até o 19, com média de -95 dBm entre estes canais, provenientes do sinal de WiFi presente no teste.

Figura 3.11: - Analise de energia sem interferência WiFi e do gerador de interferência.



Fonte: Elaborado pelo autor.

Figura 3.12: -Analise de energia somente com interferência WiFi.



Fonte: Elaborado pelo autor.

Apenas a detecção do sensor a uma variação de energia, não demonstra que a análise de energia apresenta os valores corretos de detecção de energia do espectro, sendo que o próximo teste visa contemplar esta lacuna.

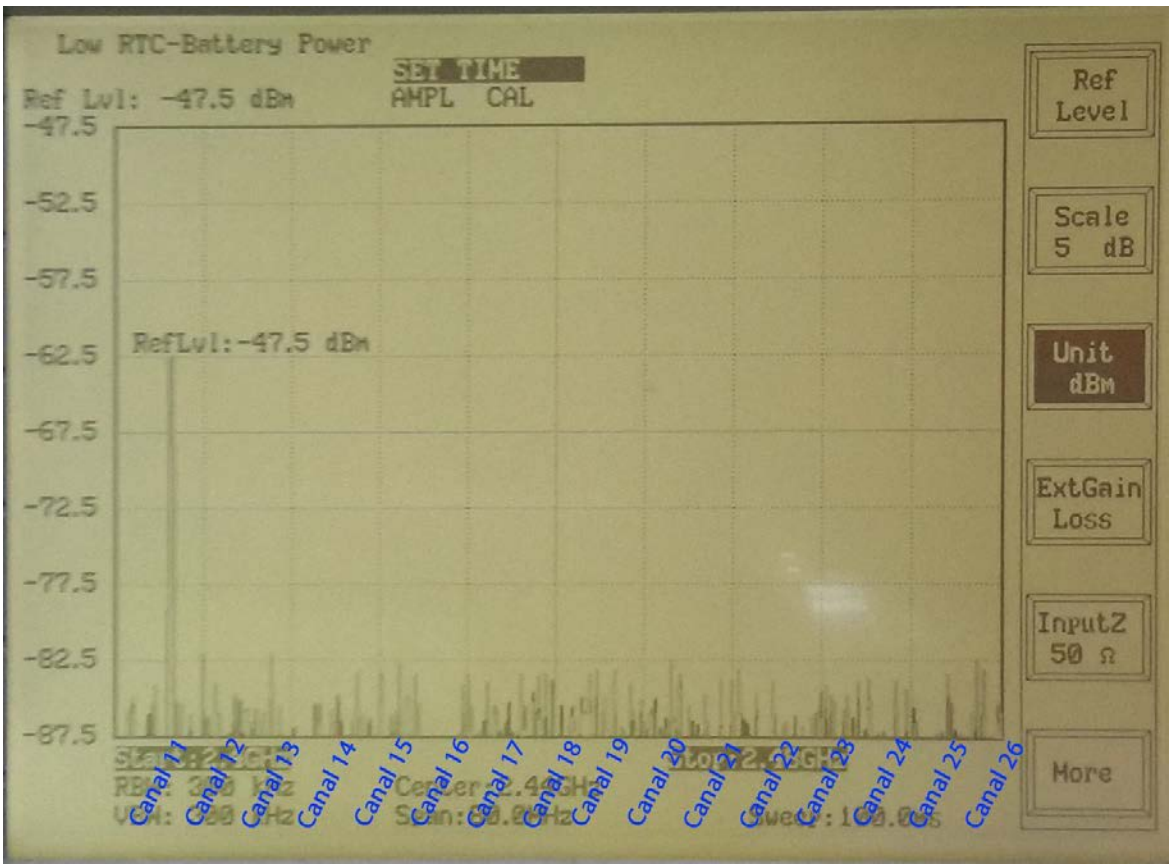
3.4.4.1 Teste comparativo

Além das verificações já realizadas para garantir a entrada no estado proposto, é preciso comprovar que a quantidade de energia que o programa apresenta como resposta são valores aceitáveis e condizentes com o esperado.

Para isto, o teste proposto consiste em utilizar o dispositivo Agilent Technologies Fieldfox N9912a como uma fonte de interferência, e para analisar os resultados foram, utilizados o Instek Spectrum Analyzergps 827 e o rádio da família MC13224, desenvolvido em (Muller, 2010).

A fim de diminuir as diferenças de recepção do sinal para os dispositivos ambos os dispositivos receptores de interferência foram posicionados de forma equidistantes da antena do dispositivo transmissor de interferência, gerando desta forma um triangulo isósceles. Para esta verificação foi produzido uma interferência no canal 11 do WH (2,405 GHz) .

Figura3.13: - Analisador de frequência Instek



Fonte: Elaborado pelo autor

3.4.4.2 Dados obtidos

Como a Figura 3.13 demonstra, no eixo x a unidade é em dBm e começa em -87,5 indo até -47,5, e a unidade do eixo y é de frequência em GHz, com uma faixa de 2,400 até 2,480. Para facilitar, já estão apontados os 16 canais, sendo que o canal 26 não é bem representado, visto que nesta arquitetura ele é de uso exclusivo. Vendo este gráfico, o valor que se destaca é no canal 11, com potência detectada de -62,5 dBm, enquanto o valor médio dos outros canais é de -85,0 dBm.

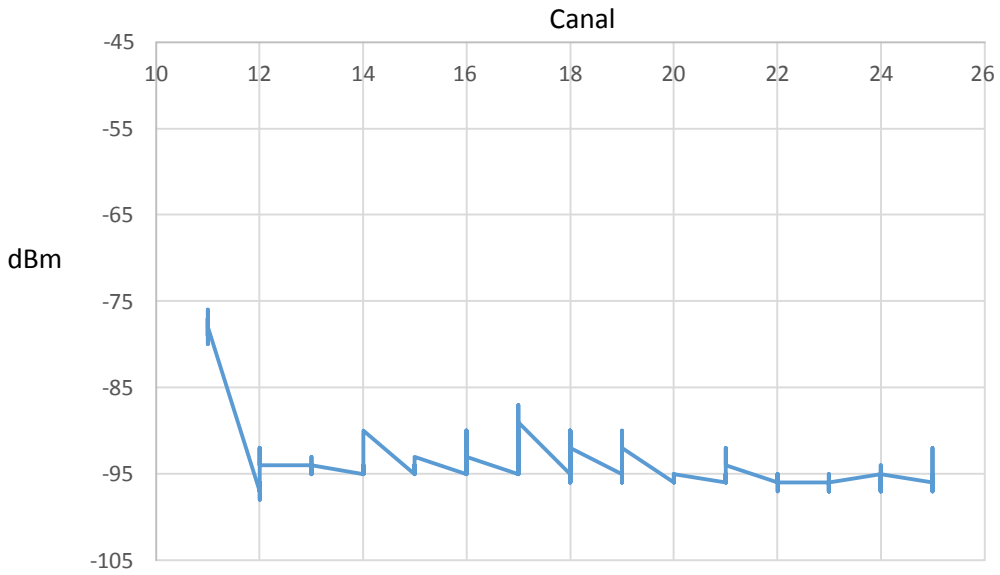
Como o cálculo da potência é

$$\mathrm{dBm} = 10 \log_{10} \left(\frac{\mathrm{PmW}}{1\mathrm{mW}}\right) \quad (4),$$

podemos concluir que a cada 3 dBm, a potência duplica. Então, o sinal detectado no canal 11 é 181 vezes maior que o detectado nos demais canais.

A Figura 3.14 representa as medidas do dispositivo da família MC13224 desenvolvido no LASCAR

Figura 3.14: - Energia detectada pelo Rádio MC13224



Fonte: Elaborado pelo autor.

Como demonstrado na Figura 3.14, a unidade utilizada no eixo x é dBm, com intensidade máxima de -45 e mínima de -105, e o eixo y representa os canais do protocolo WirelessHART. Foram feitas 312 medições em todos os canais, lembrando que essa média não ocorre de forma linear, pois a sequência de análises não é determinística, com média de 20,8 análises por canal. Neste gráfico, o canal 11 apresenta uma média de -78,6 dBm e os demais canais -97,7 dBm, e fazendo o mesmo cálculo da potência, de que para cada 3 dBm a potência duplica, concluímos que a diferença do canal 11 para os demais canais é de 80 vezes maior.

3.4.4.3 Análise dos resultados

Visivelmente o valor da diferença do canal que recebe a interferência para os demais canais, aferido pelo aparelho Instek Spectrum, é muito maior do que o medido no dispositivo do LASCAR. Contudo, diversos fatores devem ser levados em conta, como o tipo da antena e o seu tamanho, que influenciam na análise, assim como as outras interferências presentes e o método de medição. A forma que o aparelho Instek faz a medição é por pico, procurando assim o maior sinal e apresentando-o. É ideal para sinais EMI (2.7GHz Spectrum Analyzer, 2001), alterando assim a comparação com o dispositivo trabalhado, que opera com médias. No laboratório onde foram realizados os experimentos, há diversas redes WiFi , e dentre elas a

do próprio laboratório, que opera no canal 6 do WiFi (2.437 GHz). O dispositivo analisado detectou uma pequena interferência no canal 17 do WH (2.435 GHz), frequência muito próxima a utilizada pela rede WiFi. Contudo o Instek Spectrum não detectou esta interferência. Este fato corrobora para a influência dos tipos e tamanhos das antenas, e também aumenta a média do sinal dos demais canais no dispositivo MC13224.

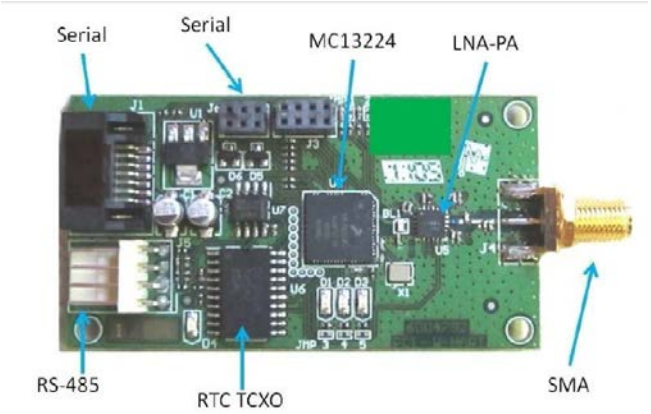
3.5 Rádios utilizados no trabalho

Os aparelhos utilizados para este projeto foram o rádio com o SOC (*System On Chip*) da empresa Freescale, família 1322x. Duas versões do dispositivo foram utilizados, primeiramente um kit de desenvolvimento produzido pela empresa Fresscale (Figura 3.15) e após foi utilizado o dispositivo desenvolvido no trabalho de (MULLER, 2012) (Figura 3.16).

Figura 3.15: - Kit de desenvolvimento Freescale

Fonte Elaborado pelo autor

Figura 3.16: - MC13224v produzido no Development of a WirelessHART Compatible Field Device



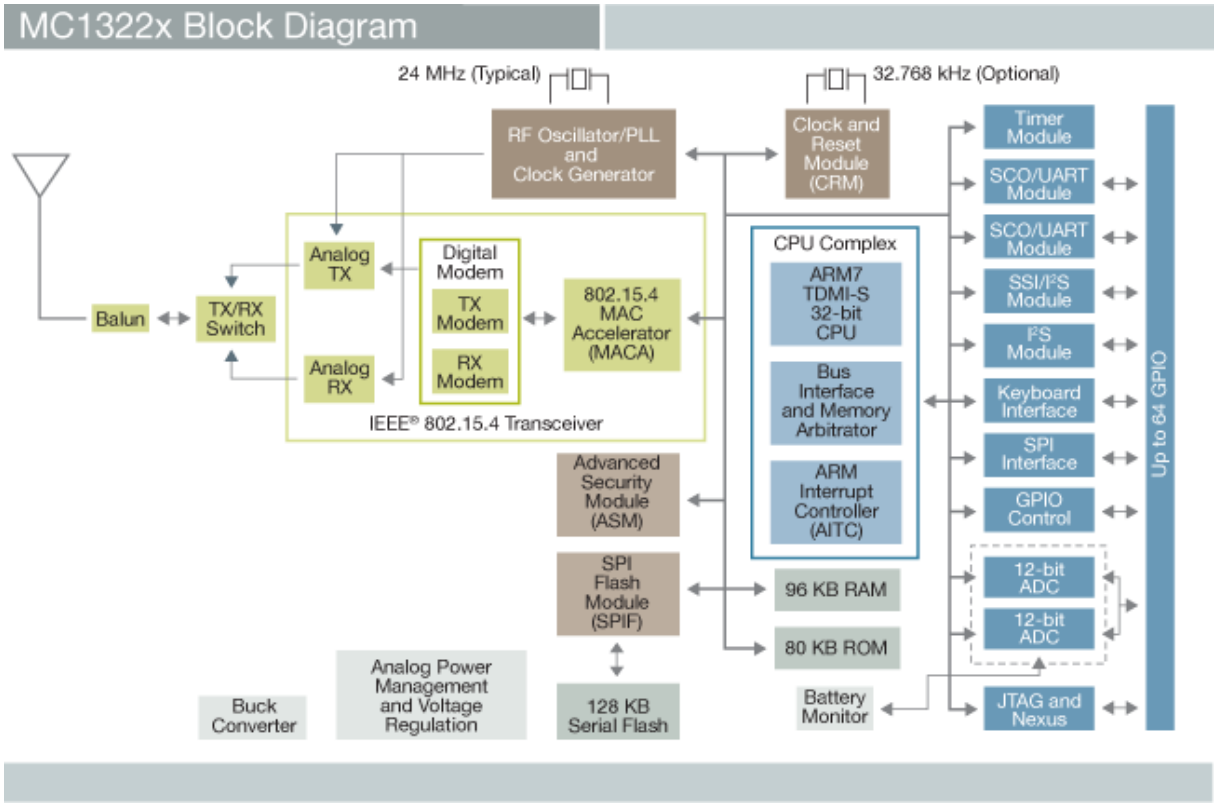
Fonte: Muller (2012).

Em ambos os testes o projeto foi aprovado, conseguindo manter-se na rede de forma estável e com poucas perdas de pacotes.

3.5.1 Diagrama de bloco do SOC MC1322x

Abaixo é ilustrado, pela Figura 3.17, o diagrama de blocos que contém todas as funcionalidades do SOC utilizado

Figura 3.17: -:Diagrama de Bloco da Família MC1322x



Fonte: FREESCALE SEMICONDUCTOR (2012)

Este aparelho tem um processador ARM7 de 32 bits. O diagrama de blocos acima apresenta as seguintes características:(FREESCALE SEMICONDUCTOR ,2012):

Cristal oscilador de referência de clock;

21 mA consumo de corrente típica no modo RX com MCU ativo;

29 mA Consumo de corrente típica no modo TX com MCU ativ;.

128 KB serial flash;

RAM de 96 KB de memória;

ROM 80KB de memória contendo *bootcode*, todos os drivers de dispositivo e

compatível com IEEE 802.15.4 MAC;

MAC acelerador (sequenciador e de interface DMA);

AES 128-bit hardware de encriptação / desencriptação com gerador de números aleatórios;

Porta JTAG para *debug;*

Nexus funcionalidade estendida porta de depuração;

Não necessita de componentes RF externos;

Componentes correspondentes ao RF e *balun* estão dentro do encapsulamento;

Monitorador de Bateria (FREESCALE SEMICONDUCTOR ,2012).

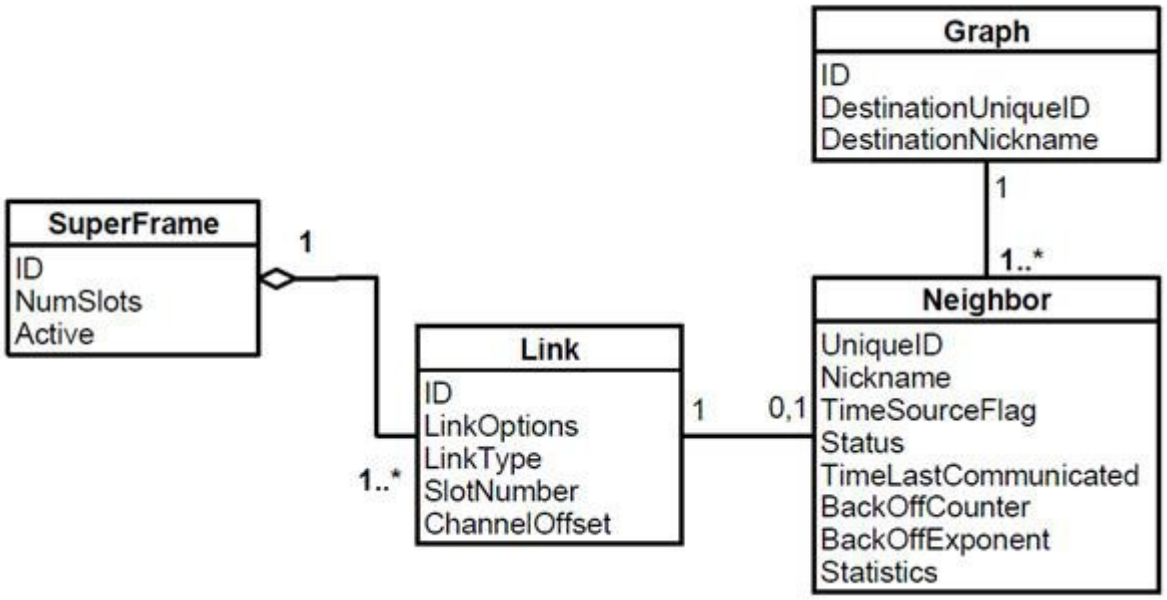
Destas diversas características, o cristal oscilador, compatibilidade com IEEE 802.15.4, o MAC AES 128-bit e porta JTAG para *debug*, se destacam como as principais. O Cristal Oscilador é fundamental, visto que o algoritmo de multiplexação da arquitetura WirelessHART é fundado em *slot*, que devem estar sincronizados no tempo. Então, ter uma precisão e sincronismo entre os *clocks* dos dispositivos é fundamental para uma boa relação entre eles. Compatibilidade com o protocolo IEEE 802.15.4,o qual é o protocolo utilizado pelo WH. O AES 128-bit torna a rede mais segura e é uma das formas adotadas pela rede WH para garantir a segurança desta. E, a porta JTAG para *debug* é utilizada para fazer testes passo-a-passo.

Desta forma, a escolha do dispositivo Freescale da família MC1322x é uma boa escolha a ser feita, pois todos as necessidades do protocolo WirelessHART são atendidas.

3.6 Estruturas de dados e informações a serem enviadas

A detecção de energia tem por objetivo reunir o máximo de informações sobre o ambiente da rede WH. Para o gerenciador de rede poder detectar as interferências no meio é preciso que os dados sejam armazenados e, posteriormente, enviados a ele. As informações escolhidas para análise posterior são: ID do SuperFrame, ID do Link, Canal, UniqueID do vizinho e o ED detecção de energia (HCF, 2007). Todas as outras informações são provenientes do diagrama entidade relacionamento (ER) Data-link, representados na Figura 3.18, exceto o ED, que é coletado na sua função específica.

Figura 3.18: - Diagrama ER da camada de enlace.



Fonte: TDMA Data Link LayerSpecification (2008).

Como pode ser visto nesta figura, tendo a informação do link, é possível determinar as informações acima solicitadas, ID do SuperFrame, ID do Link, Canal e UniqueID do vizinho.

A estrutura desenvolvida para isto foi a seguinte:

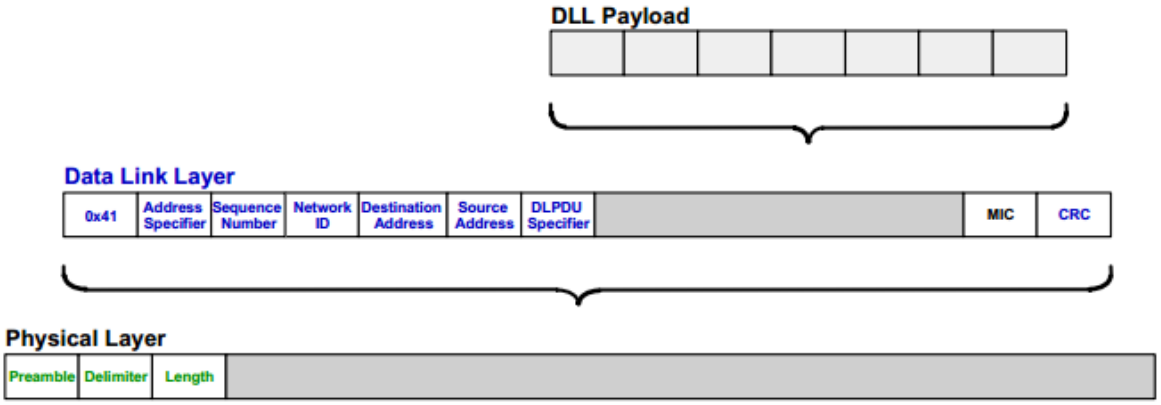
```
typedefstruct
{
  uint8_t   NeighboarId:6;  (usando 2 bytes para transmissão)
    uint8_t     SuperFrameID: 4;(usando 2 bytes para transmissão)
    uint8_t     Channel: 4;(usando 2 bytes para transmissão)
    uint8_t     ED:8;(usando 2 bytes para transmissão)
    uint64_t    ASN: 64;(usando 8 bytes para transmissão)

} DLL_ed_coletion_nodo;
```

Foi desenvolvido um comando especial que informa os dados coletadas, contudo somando todos os bytes necessários serão16 bytes. Como a aplicação limita em 85 bytes a transmitir, cada requisição transmitirá no máximo 5 coletas de ED do tipo DLL_ed_coletion_nodo. Então, para recolher todas as informações quando o *buffer* estiver cheio, seria necessário executar este comando 11 vezes, sem levar em conta que este *buffer*

pode ser realimentado nos intervalos das consultas. Outro problema é a falta de memória, visto que o dispositivo apresenta 128 kbytes e nesse espaço de memória também está incluido o código. O armazenamento de um grande número de coletas se torna inviável, e por este motivo foi criado um vetor com esta estrutura. Como a questão temporal também é considerada, o vetor proposto é circular de 64 células, sobrescrevendo as informações mais antigas por novas, e desta forma não ocupando um grande espaço da memória. Utilizando 64 nodos, com cada nodo sendo de 86 bits ou 11 bytes, apenas essa estrutura já consome 704 bytes dos 128 kbytes disponíveis.

Para o envio das informações citadas é preciso que elas sejam encapsuladas. Como apresentado na Figura 3.19, o dado do DLPDU é primeiramente encapsulado pela camada de enlace; e, os dados de endereço específico, número de sequência, identificador de rede, endereço destino, endereço origem DLPDU específico, MIC e CRC, formando o datagrama da camada de enlace, são encapsulados para codificação da camada física.

Figura 3.19: - Encapsulamento da estrutura do DLPDU



Fonte: TDMA Data Link Layes (2008).

O tamanho máximo do payload da norma IEEE 802.15.4 de uma mensagem é de 133 bytes. Desse valor 6 bytes são do cabeçalho da camada física, sobrando assim 127 bytes. O tamanho do cabeçalho da camada de enlace varia entre 25 bytes e 9 bytes. De qualquer forma a norma IEEE 802.15.4, estabelece como padrão 25 bytes de cabeçalho, e tem como resultado apenas 102 bytes de payload (Nixon, 2010).

4 CONCLUSÃO

O protocolo *Wireless*HART tem sido a tecnologia mais adequada atualmente de comunicação sem fio em aplicações industrias, porém como esta arquitetura necessita de um gerenciador de rede, que é um ponto único de falha, e a rede não suporta outros dispositivos que não possuam elementos com conectividade à arquitetura WH, então algumas fábricas podem utilizar mais de uma rede no mesmo ambiente, tornando o sistema mais seguro, na maioria das vezes. Com diversas redes competindo pelo mesmo espaço, a preocupação em se conhecer o seu ambiente através de uma análise constante da rede, é de suma importância.

Este trabalho apresentou resultados positivos nessa área. Mesmo que ao comparar com dispositivos estabelecidos no mercado, o resultado obtido não tenha sido o esperado, e atualmente o processo de detecção de energia meça aproximadamente 53% do *slot* de transmissão, os resultados obtidos já conseguem determinar pontos de interferência, utilizando-se dos *slots* que ficariam ocioso, também foi desenvolvido um comando especial na camada de aplicação que retorna as últimas coletas de detecção de energia. Em contrapartida, o programa utiliza um método do WH já validado e, na primeira versão da documentação do protocolo WH, foi documentado um endereço de memória que é possível alterar os intervalos do ED. Desta forma podendo-se ter uma fração maior do *slot* para análise. Em trabalhos futuros seria interessante modificar o tempo de ED e encontrar um dispositivo para comparação mais similar ao utilizado pelo projeto, com a mesma forma de medição de energia e antenas similares, em contra partida, a função de detecção de energia tem o custo do consumo de energia. Futuramente formas equilibrar a quantidade de *slot* analisados com o gasto energético.

A rede ainda não evita os canais com interferência, mas está caminhando nessa direção. Tendo as amostras dos *slot* vagos, caberá ao gerenciador da rede decidir qual o melhor canal e intervalo de tempo de cada dispositivo para sua comunicação. Futuramente, formas de balancear o consumo, juntamente com a análise de energia, deverão ser implementadas, visto que uma das principais virtudes desta arquitetura é o baixo consumo. Opções de redução do tamanho dos dados das amostras também estão sendo planejadas para reduzir o número de transmissões e, desta forma ,auxiliar na economia da energia.

REFERÊNCIAS

Axell, Erik, et al. "Spectrum sensing for cognitive radio: **State-of-the-art and recent advances**." Signal Processing Magazine, IEEE 29.3 (2012)
Committed to connectingthe world Access Technologies (FDMA, TDMA, CDMA) . ITU 2005 Disponível em: < http://www.itu.int >. Acesso em: 29 nov. 2014.

Cabric, D.; Mishra, S.M.; Brodersen, R.W., "**Implementation issues in spectrum sensing for cognitive radios**," Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on , vol.1, Nov. 2004

Emerson Process Management . Smart Wireless Gateway User Interface Terminology Guide Manual Supplement, Rev AA, jul. 2012.Disponível em: <http://www2.emersonprocess.com/siteadmincenter/PM%20Rosemount%20Documents/00809-0600-4420.pdf>. Acesso em: 20 nov. 2014.

FREESCALE SEMICONDUCTOR. MC1322x: Advanced ZigBee Compliant SoCPlatformfor the 2.4 GHz IEEE 802.15.4 Standard: Reference Manual. 2012. 532 p. Disponível em:<www.freescale.com/files/rf_if/doc/ref_manual C1322 R .pdf>. Acesso em: 18 nov. 2014.

HART COMMUNICATION FOUNDATION (HCF). HCF_SPEC-065: 2.4GHz DSSS OQPSK Physical Layer Specification. Austin, 2007, 20 p.

HART COMMUNICATION FOUNDATION (HCF). HCF_SPEC-075: TDMA Data Link Layer Specification. Austin, 2008, 76 p.

HART COMMUNICATION FOUNDATION (HCF).HCF_SPEC-085: Network Management Specification. Austin, 2009, 98 p.

HART COMMUNICATION FOUNDATION.HCF_SPEC-155.Rev. 1.1. Austin: HCF,2008. Parte da norma.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE). **IEEE Standard for Local and Metropolitan Area Networks - Part 15.4**: Low-Rate Wireless Personal Area Networks (LR-WPANs). New York, 2011.

KUROSE, J. F .**Redes de Computadores e a Internet: Uma Abordagem Top-down**. 5. ed. São Paulo : Pearson, 2010.

LINDAU, M., MÜLLER, I., WINTER, J., PEREIRA,C., NETTO, J., BECKER,L. **Low cost wireless site survey system for WirelessHART network deployment** Simpósio Brasileiro de Automação Inteligente out 2013.Disponível em: <http://www.sba.org.br/SBAI/pdfs/6288.pdf >. Acesso em: 25 nov. 2014.

MACHADO, T. M. **Analisador de redes *wireless*Hart com capacidade de detecção de coexistência**. 2014. 82 p. Dissertação (Mestrado em Engenharia Elétrica) – Programa de Pós-Graduação em Engenharia Elétrica, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

MULLER, I.Netto**,** J**.;** Pereira, C; Allgayer, R.; Fabris, E. **Development of a WirelessHART Compatible Field Device**.In: IEEE 2010

MULLER, I.; PEREIRA C.E.; NETTO, J. *Wireless*HART Field Devices**. IEEE Instrumentation and Measurement Magazine**, Dec. 2011.

Nixon, M. ,Mok, A. WirelessHART™: **Real-Time Mesh Network for Industrial Automation** 1. ed. Springer, 2010

Winter, J. Muller, I. Pereira C., Netto, J. **Towards a WirelessHART Network with Spectrum Sensing** 19th World Congress The International Federation of Automatic Control Cape Town, South Africa. Aug, 2014

WirelessHART: The first wireless standard for industrial applications 2013 Disponível em: < http://www.phoenixcontact.net/microsites/wireless-hart/895.htm>. Acesso em: 29 nov. 2014.

2.7GHz Spectrum Analyzer Model: GSP-827 Operation Manual. 2001