SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL
CENTRO INTEGRADO DE MANUFATURA E TECNOLOGIA
FACULDADE DE TECNOLOGIA SENAI/CIMATEC
Especialização em Automação, Controle e Robótica.

FLÁVIO AUGUSTO BRITO DO NASCIMENTO

UM ESTUDO EM SEGURANÇA WIRELESS NO CHÃO DE FÁBRICA

SALVADOR/BA

2008

FLÁVIO AUGUSTO BRITO DO NASCIMENTO

UM ESTUDO EM SEGURANÇA WIRELESS NO CHÃO DE FÁBRICA

Monografia apresentada à Faculdade de Tecnologia SENAI – CIMATEC para obtenção do título de Especialista no curso de Especialização em Automação, Controle e Robótica.

Orientador: Prof. Pedro Ivo de Oliveira Rodrigues.

SALVADOR/BA

2008

SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL
CENTRO INTEGRADO DE MANUFATURA E TECNOLOGIA
FACULDADE DE TECNOLOGIA SENAI/CIMATEC
Especialização em Automação, Controle e Robótica.

Prof. Pedro Ivo de Oliveira Rodrigues
Mestrando em Modelagem Computacional
Componente da Banca Examinadora

Dr. Edmárcio Antônio Belati
Pós-Doutor em Sistemas Elétricos de Potência
Componente da Banca Examinadora

Prof. MSC Milton Bastos de Souza
Mestre em Engenharia Elétrica
Componente da Banca Examinadora

SALVADOR/BA
2008

AGRADECIMENTOS

Agradeço aos professores e colegas que me acompanharam durante o decorrer do curso dentro e fora das salas de aula.

Agradeço principalmente aos meus pais por estarem sempre dispostos a me proporcionar oportunidades de crescer pessoalmente e profissionalmente.

LISTA DE FIGURAS

Figura 1: Projeto ALOHA 3
Figura 2: Narrowband versus Spread Spectrum 5
Figura 3: Frequency and Direct Sequence Spread Spectrum 6
Figura 4: Sistema *wireless* básico 6
Figura 5: Operação em Modo *Root* 7
Figura 6: Operação em Modo Ponte 8
Figura 7: Operação em Modo Repetidor 8
Figura 8: Tipos de rede *wireless*. 10
Figura 9: Relação entre o modelo OSI e o 802.11. 12
Figura 10: (a) Modo Estruturado; (b) Modo Ad Hoc. 12
Figura 11: Piconets. 14
Figura 12: Camadas do ZigBee. 16
Figura 13: Topologias de rede do ZigBee 17
Figura 14: ISA 100 Timeline. 19
Figura 15: ISA 100 Universal Gateway. 20
Figura 16: Solução ISA 100 para compartilhamento do espectro. 21
Figura 17: Tecnologia *Wireless* no Chão de Fábrica. 27
Figura 18: Exemplo de processo de autenticação – *Shared Key*. 28
Figura 19: Metodologia Proposta de Projetos de Redes Locais Sem Fio 32
Figura 20: RTD da Sensicast 36
Figura 21: Modelo de referência OSI 48

LISTA DE QUADROS

Quadro 1: Alguns padrões IEEE..... 9
Quadro 2: Funcionalidades dos dispositivos ZigBee..... 18

LISTA DE ABREVIAÇÕES

AP - *Access Point* ou Ponto de Acesso

DSSS - *Direct Sequence Spread Specrtum*

EAP - *Extensible Authentication Protocol*

IEEE - *Institute of Electrical and Electronics Engineers*

IP – *Internet Protocol*

IPSEC – *Internet Security Protocol*

ISM - *Industrial, Scientific, and Medical*

LAN – *Local Area Network*

MAC - *Media Access Control*

PDA - *Personal Digital Assistants*

RTD - *Resistance Temperature Detector*

SSID - *Service Set Identification*

VPN - *Virtual Private Network*

WEP - *Wired Equivalent Privacy*

WI-FI – *Wireless Fidelity*

WLAN – *Wireless Local Area Network* - Rede Local Sem Fio

WMAN – *Wireless Metropolitan Area Network* - Rede Metropolitana Sem Fio

WPAN – *Wireless Personal Area Network* - Rede Pessoal Sem Fio

WWAN - *Wireless Wide Area Network* - Rede Geograficamente distribuída Sem Fio

WPA - *Wired Protected Acess*

RESUMO

O objetivo desse trabalho é mostrar que é possível e pode ser segura a utilização de redes de comunicação *wireless* (sem fio) no chão de fábrica das empresas para aplicações não críticas ou no sensoreamento, apresentando conceitos, tipos de tecnologia que podem ser utilizadas e características de seu funcionamento, o que é permitido pela Legislação Brasileira, as vantagens e desvantagens na sua utilização, os recursos e procedimentos de segurança das tecnologias disponíveis e apresentação de uma aplicação que caracterize de forma satisfatória a operação de um sistema *wireless* no chão de fábrica.

Palavras-Chave: Redes de comunicação sem fio, *Wireless*, Chão de fábrica.

SUMÁRIO

LISTA DE FIGURAS V
LISTA DE QUADROS VI
LISTA DE ABREVIAÇÕES VII
RESUMO VIII
1. INTRODUÇÃO 1
2. HISTÓRICO 3
3. PRINCÍPIOS DAS REDES *WIRELESS* 5
3.1 Técnica de transmissão 5
3.2 Componentes dos sistemas *Wireless* 6
3.2.1 Acces Points 7
3.2.2 Estações Cliente 9
3.3 Padrões de Redes *Wireless* 9
3.3.1 802.11 e 802.11 a/b/g 10
3.3.2 Bluetooth 13
3.3.2.1 Características Técnicas 14
3.3.3 ZigBee 15
3.3.3.1 Características técnicas 16
3.3.3.2 Topologias de rede 17
3.3.4 ISA100 18
4. NORMATIZAÇÃO. 22
4.1 FCC 22
4.2 ETSI 22
4.3 IEEE 22
4.4 Agência Nacional de Telecomunicações - ANATEL 22
5. VANTAGENS E DESVANTAGENS DA COMUNICAÇÃO SEM FIO 24
6. SEGURANÇA EM REDES DE COMUNICAÇÃO *WIRELESS* 26
7. EXEMPLO DE APLICAÇÃO DE UM SISTEMA WIRELESS NO CHÃO DE FÁBRICA. 35
8. CONCLUSÕES 38

8.1 CONSIDERAÇÕES FINAIS 38
8.2 PROPOSTA PARA ESTUDOS FUTUROS 39
REFERÊNCIA BIBLIOGRAFICA 40
ANEXOS 44
Anexo 1 - Equipamentos *wireless* para indústria 44
Anexo 2 - Definições 46

1. INTRODUÇÃO

O avanço tecnológico nas telecomunicações trouxe os equipamentos sem fio para o convívio doméstico da população. Telefones sem fio, celulares, PDAs (*Personal Digital Assistants*), *notebooks*, etc. são exemplos de equipamentos que trazem facilidade de comunicação entre as pessoas. Mesmo com a discordância do inventor da *Ethernet*, Bob Metcalfe, que escreveu: "Os computadores móveis sem fio são como banheiros móveis sem tubulação – verdadeiros penicos portáteis – Eles serão comuns em veículos, construções e em shows de rock. Meu conselho é que as pessoas instalem fiação em suas casas e fiquem lá" (Metcalfe, 1995), esses equipamentos estão invadindo os lares, os escritórios, os shoppings, etc. E na indústria será que utilização de equipamentos sem fio não poderia trazer grandes benefícios?

Serão apresentadas características dos sistemas de comunicação sem fio, suas vantagens, desvantagens e mostrado que podem ser implementados como complementação ou como alternativa para as tradicionais redes com fio utilizadas no chão de fábrica.

Os termos WWAN - *Wireless Wide Area Network*, WMAN - *Wireless Metropolitan Area Network*, WLAN – *Wireless Local Area Network* e WPAN - *Wireless Personal Area Network* são os nomes dados às redes w*ireless*, de acordo com o alcance, que interligam suas estações, sem utilização de cabos (par trançado, cabo coaxial ou fibra óptica). Serão abordados neste trabalho os tipos de tecnologia que podem ser utilizadas para comunicação de equipamentos no chão de fabrica mostrando que é viável o investimento nesse segmento para aplicações não críticas e no sensoreamento dos processos industriais.

As soluções *wireless* têm sua aplicação em ambientes com dificuldades de interligação via cabo, estruturas que não suportam uma ampliação na rede cabeada existente ou que a reestruturação teria um alto custo financeiro, em construções antigas onde não são permitidas alterações na estrutura física ou locais de difícil acesso e de risco a vida. A mobilidade tornaria o serviço mais ágil, pois a aquisição de dados e a comunicação seriam feitas com ferramentas móveis (*notebooks*, PDAs, celulares e etc.), seguro pois não teria

contato direto com locais de risco, traria redução de custos e tempo na implantação em comparação com redes cabeadas.

Este trabalho mostra no segundo capítulo um pouco do histórico das comunicações sem fio, citando pontos importantes, começando coma primeira comunicação com um telégrafo sem fio e terminando com o desenvolvimento de um padrão para LANs - *Local Area Networks* sem fio.

No terceiro capítulo são apresentados os princípios das redes de comunicação *wireless*, a técnica de transmissão, os principais componentes das redes, alguns dos padrões existentes que podem ser utilizados no chão de fábrica de empresas e um padrão que está em desenvolvimento para a mesma utilização.

No quarto capítulo são citadas as instituições que normatizam e padronizam os sistemas de comunicação ao redor do mundo, sem esquecer de citar a instituição brasileira responsável pelo assunto.

No quinto capítulo são apresentadas as vantagens e desvantagens da utilização de sistemas de comunicação *wireless*.

No sexto capítulo se inicia o estudo sobre o maior problema da utilização de sistemas de comunicação *wireless*: Falta de segurança, com a apresentação dos principais problemas de segurança da tecnologia e procedimentos para minimizá-los ao máximo.

No sétimo capítulo é mostrada a aplicação de um sistema de comunicação *wireless* em uma usina nuclear, afirmando, assim, que é viável a utilização no chão de fábrica.

No oitavo são feitas as considerações finais e uma proposta de estudo para implantação de uma rede de comunicação *wireless* na planta modelo do SENAI/CIMATEC, com o intuito de desenvolver o conhecimento no assunto.

2. HISTÓRICO

A história da comunicação sem fio não é tão recente quanto se imagina. No início do século XX foi demonstrado, pelo físico italiano Guglielmo Marconi, o funcionamento de um telégrafo sem fio, localizado no litoral, que se comunicava com navios utilizando o código Morse. Comparado com os sistemas atuais é um sistema de comunicação simples, mas que basicamente tem o mesmo funcionamento dos atualmente utilizados (Tanembaum, 2003).

Outra fase da comunicação sem fio foi o Projeto ALOHANET que teve início em 1971 e foi desenvolvido pela Universidade do Havaí. Foi implementada uma rede, que utilizava comunicação via satélite, em topologia estrela, com sistemas computacionais distribuídos por quatro ilhas, figura 1, que se comunicavam com um sistema central localizado na ilha de Oahu.

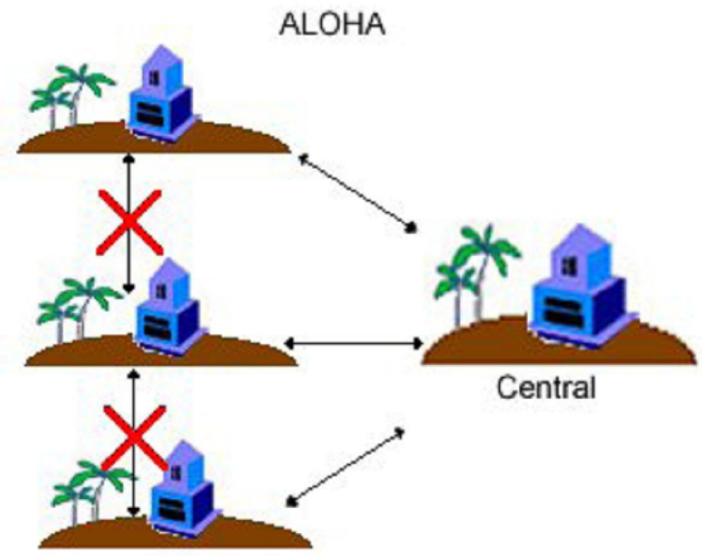

Figura 1: Projeto ALOHA

Fonte: Estudo sobre redes AdHoc – Autor: *Fernando Richter Vidal*

Segundo Farias (2003), as redes sem fio surgiram no meio militar, como muitas outras tecnologias (a exemplo da tecnologia dos sistemas móveis celulares), onde a necessidade de métodos simples e seguros de comunicação em ambientes de combate é suma importância. Com a evolução, a tecnologia passou a ser de uso público.

Já Tanembaum (2003), afirma que as LANs sem fio começaram a se tornar realidade quase na mesma época do surgimento dos *notebooks*, na década de 90, com o sonho dos seus usuários em conectar seus equipamentos a internet imediatamente ao entrar em seu ambiente de trabalho. Foram criados grupos de estudo para descobrir meios de concretizar esse sonho. A partir disso surgiram várias idéias, a primeira era equipar o ambiente de trabalho e os *notebooks* com dispositivos transmissores e receptores de ondas curtas para permitir a comunicação. Essa idéia levou a comercialização de LANs sem fio em várias empresas e trouxe um problema a incompatibilidade dos equipamentos. Daí as indústrias decidiram que padronizar seria a única solução para o problema e o IEEE - *Institute of Electrical and Electronics Engineers* recebeu essa função, condensando as tecnologias criadas nos padrões que estão disponíveis atualmente.

3. PRINCÍPIOS DAS REDES *WIRELESS*

3.1 Técnica de transmissão

Existem diversos padrões operacionais para utilização de redes sem fio que podem ser utilizados para WLANs e WPANs, e os mesmos utilizam a mesma técnica de transmissão conhecida com difusão espectral (*Spread Spectrum)* que é caracterizada por possuir uma ampla banda de transmissão utilizando baixa potência de sinal, distribuindo o sinal de modo uniforme na banda, o que garante maior integridade ao tráfego das informações e menor sujeição a ruídos e interferências. É muito diferente da transmissão em banda estreita (*narrow band*) que se caracteriza por sinais de alta potência, transmitidos em um tamanho de banda suficiente para carregar a informação. A comparação entre as técnicas de transmissão, citadas anteriormente, pode ser vista na figura 2 (Farias, 2006).

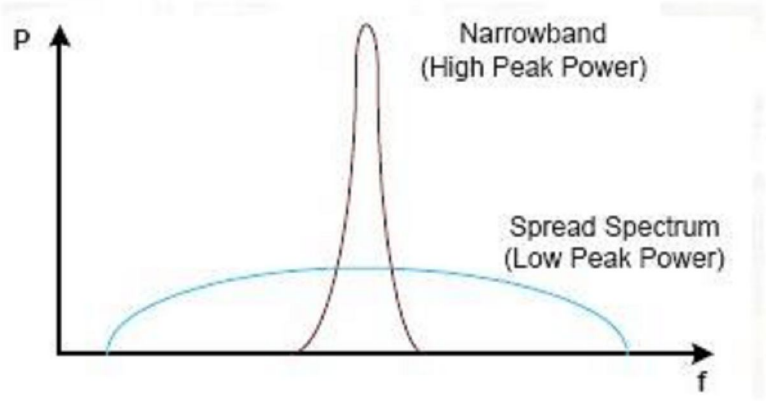

Figura 2: Narrowband versus Spread Spectrum
Fonte:http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless006.asp

Existem diversas implementações técnica de transmissão por difusão espectral, mas apenas dois tipos são regulamentados pela FCC (*Federal Communications Commission)*: o FHSS (*Frequency Hope Spread Spectrum*) e o DSSS (*Direct Sequence Spread Spectrum*), mostradas na figura 3 e conceituadas no Anexo 2.

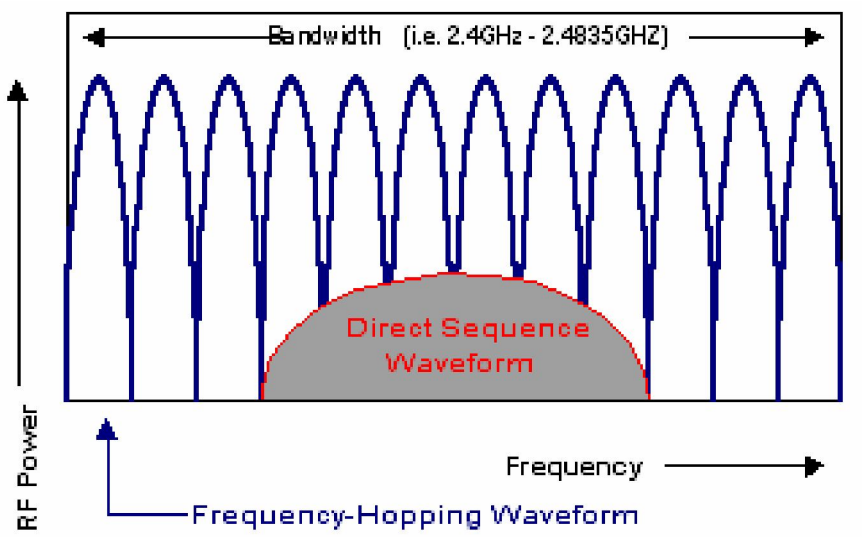

Figura 3: Frequency and Direct Sequence Spread Spectrum

Fonte: *Prosoft Technology*

3.2 Componentes dos sistemas *Wireless*

Basicamente os sistemas *wireless* são compostos por dois componentes principais *Access Points* (APs) e Estações Cliente, estações móveis que podem ser qualquer tipo de sistema computacional munido de um dispositivo que possa manter comunicação via rádio com os *Access Points* ou entre si, conforme a figura 4 abaixo:

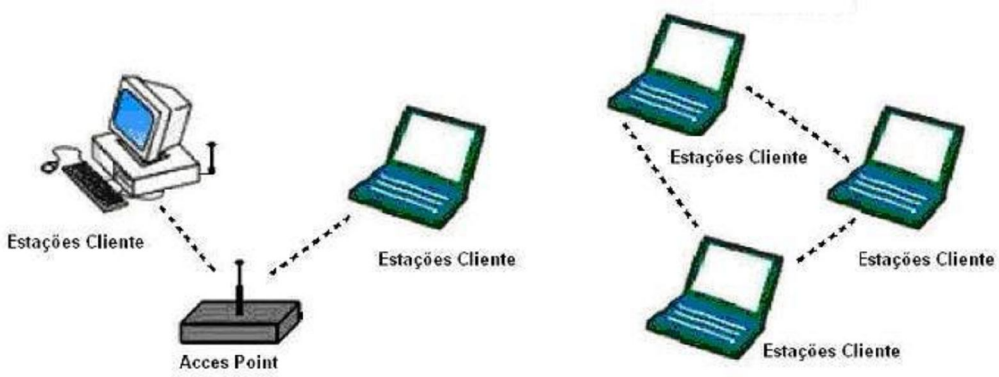

Figura 4: Sistemas *wireless* básicos

Fonte: Confeccionada pelo autor baseada em Montebeller, 2006

3.2.1 Acces Points

Os *Access Points* funcionam como pontos de entrada de uma rede para as estações cliente. Eles operam em transmissão *duplex* e possui funcionalidades semelhantes à de *switches* Ethernet, mas com a vantagem de não necessitar de fios.

Segundo Farias (2003), os *Access Points* podem se comunicar entre si, com estações cliente e com redes cabeadas em três modos de operação:

- Modo *Root*;
- Modo Ponte;
- Modo Repetidor.

O modo *Root* é utilizado para conexão do *Access Point* a uma rede cabeada. Os *Access Points* conectados a um mesmo segmento da rede podem de comunicar utilizando a rede e as Estações clientes, localizadas em células diferentes, podem através de seus *Access Points* através da rede cabeada também. Neste modo as estações cliente não se associam ao *Access Point*.

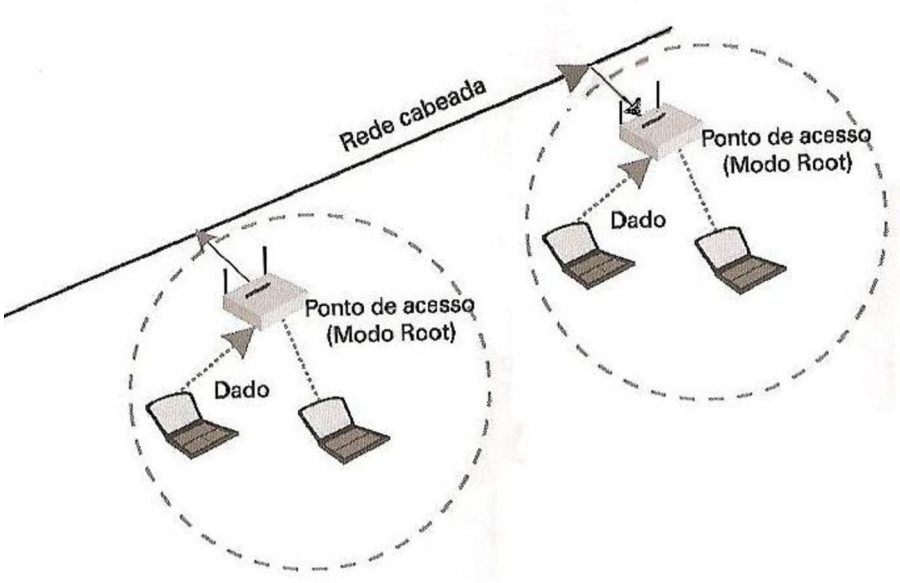

Figura 5: Operação em Modo *Root*.

Fonte: Farias, 2003

O Modo Ponte é utilizado para unir dois segmentos de rede cabeada distintos sem a utilização de fios. Essa configuração tem a função de isolar os dois segmentos de modo a impedir que o tráfego de um segmento influencie no do outro.

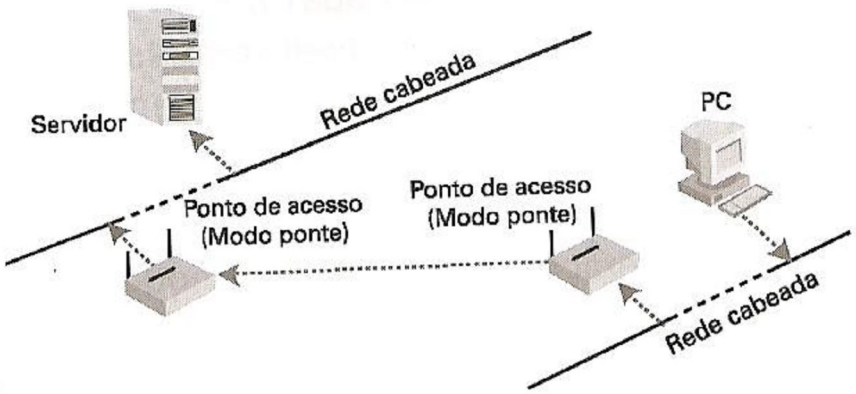

Figura 6: Operação em Modo Ponte

Fonte: Farias, 2003

O Modo Repetidor um *Access Point* é utilizado do modo *Root* e outro *Access Point* é utilizado no modo Ponte. Nesse modo as Estações Cliente se interligam ao *Access Point* repetidor que se associa a um *Access Point root* formando um link dentro de uma rede cabeada.

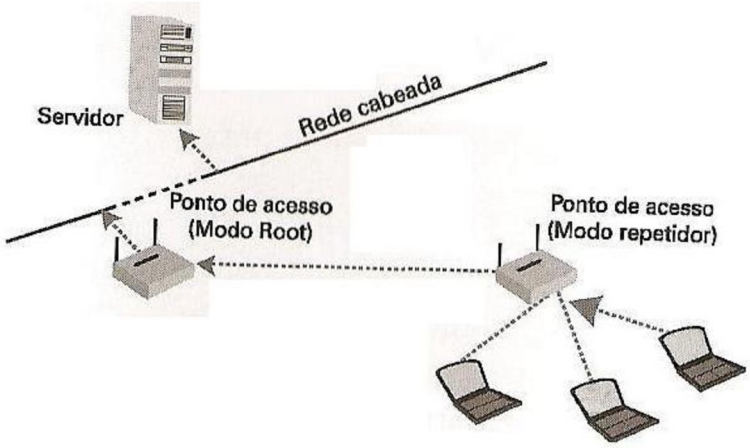

Figura 7: Operação em Modo Repetidor

Fonte: Farias, 2003

3.2.2 Estações Cliente

As Estações Cliente podem ser qualquer tipo de sistema computacional (*Notebooks*, PDAs, *desktops*, eletrodomésticos, sensores e etc.) que possua um dispositivo que possa se comunicar via rádio com os *Access Points* ou que possam comunicar-se entre si formando as redes de comunicação sem fio e atender as necessidades dos usuários.

3.3 Padrões de Redes *Wireless*

Os padrões do IEEE, para redes *wireless*, especificam as camadas física (PHY – Physical Layer) e de acesso ao meio (MAC – *Medium Acces Control*), sendo as demais camadas, de rede e de aplicação, implementadas pelos usuários.

Existem diversos padrões para tecnologia *wireless* conforme a tabela abaixo:

Padrão IEEE	Freqüência	Alcance	Taxa
802.15.1 (Bluetooth)	2.4GHz	<10m	723 Kbps
802.15.3 (UWB)	2.4GHz	30-50m	10-55Mbps
802.15.3a	3.1-10.6 GHz	<10m	110-480Mbps
802.15.4 (Zig Bee)	868 M, 915 M, 2.4 G	10-75m	20-250Kbps
802.11a	5GHz	< 50m	6-54Mbps
802.11b	2.4GHz	<100m	2-11Mbps
802.11g	2.4GHz	<100m	20-54Mbps
802.16 (WiMAX)	10-66GHz	≈10km	60-100Mbps
802.16e (150km/h)	2-6GHz	≈10km	70 Mbps

Quadro 1: Alguns padrões IEEE.
Fonte: http://www.redes.usp.br/conteudo/documentos/2-Introducao.pdf

As freqüências de operação são de uso compartilhado, isto é, os canais não são de uso exclusivo de usuários específicos e, portanto mais susceptíveis a interferências. A proteção das informações transmitidas fica a cargo do usuário. Foram determinadas pela FCC - *Federal Communications Commission* e alocadas para aplicações ISM - *Industrial, Scientific and Medical*.

Na figura 8 é mostrado como estão divididos os tipos de redes de comunicação *wireless*, de acordo com a distância em que podem operar e com a indicação do padrão que se enquadra em cada tipo.

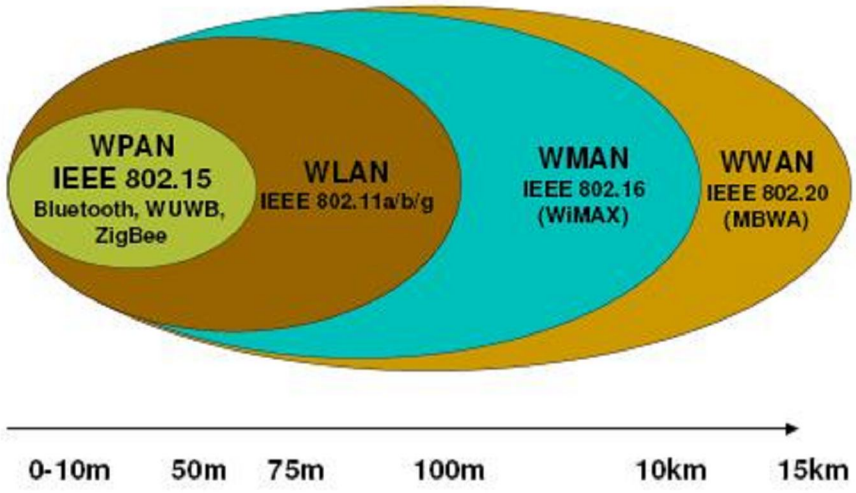

Figura 8: Tipos de rede *wireless.*
Fonte: http://www.redes.usp.br/conteudo/documentos/2-Introducao.pdf

Os padrões utilizados na WLAN e na WPAN são os mais indicados para utilização do chão de fábrica já que se trata de implantação em áreas restritas em que não é necessário um grande alcance (cobertura) para transmissão de dados. A seguir são apresentados alguns dos padrões.

3.3.1 802.11 e 802.11 a/b/g

O primeiro dos padrões a ser utilizado foi o 802.11, denominados de WI-FI, operando na faixa de 2.4 GHz operando a 2 Mbps. Logo em seguida foi criado o padrão 802.11b, com uma taxa de transmissão chegando a 11Mbps, operando na mesma faixa do 802.11, se tornando uma das mais populares devido ao seu baixo custo (Farias, 2003).

O padrão 802.11a opera na faixa de 5,0 GHz alcançando taxas de 54 Mbps, mas é incompatível com os demais padrões 802.11 por causa da faixa de operação e por isso tem pouca aceitação no mercado.

Já o padrão 802.11g surgiu como uma “fusão” dos padrões a e b, em que houve a união da alta taxa de transmissão do padrão 802.11a, com a compatibilidade, alcance e baixo custo do padrão 802.11b. Opera em 2.4 GHz com uma taxa de até 54 Mbps. Uma característica interessante é que se pode utilizar os padrões 802.11b e 802.11g conjuntamente, porém com a redução na taxa de transmissão.

De acordo com Vidal (2004), o IEEE 802.11 é um padrão internacional para WLAN aprovado pelo IEEE em 1997, que fornece especificações MAC e PHY para comunicação sem fio entre estações fixas e móveis, e, entre dispositivos portáteis dentro de uma área local específica. Na figura 9 é mostrada a relação entre o modelo OSI e o padrão 802.11.

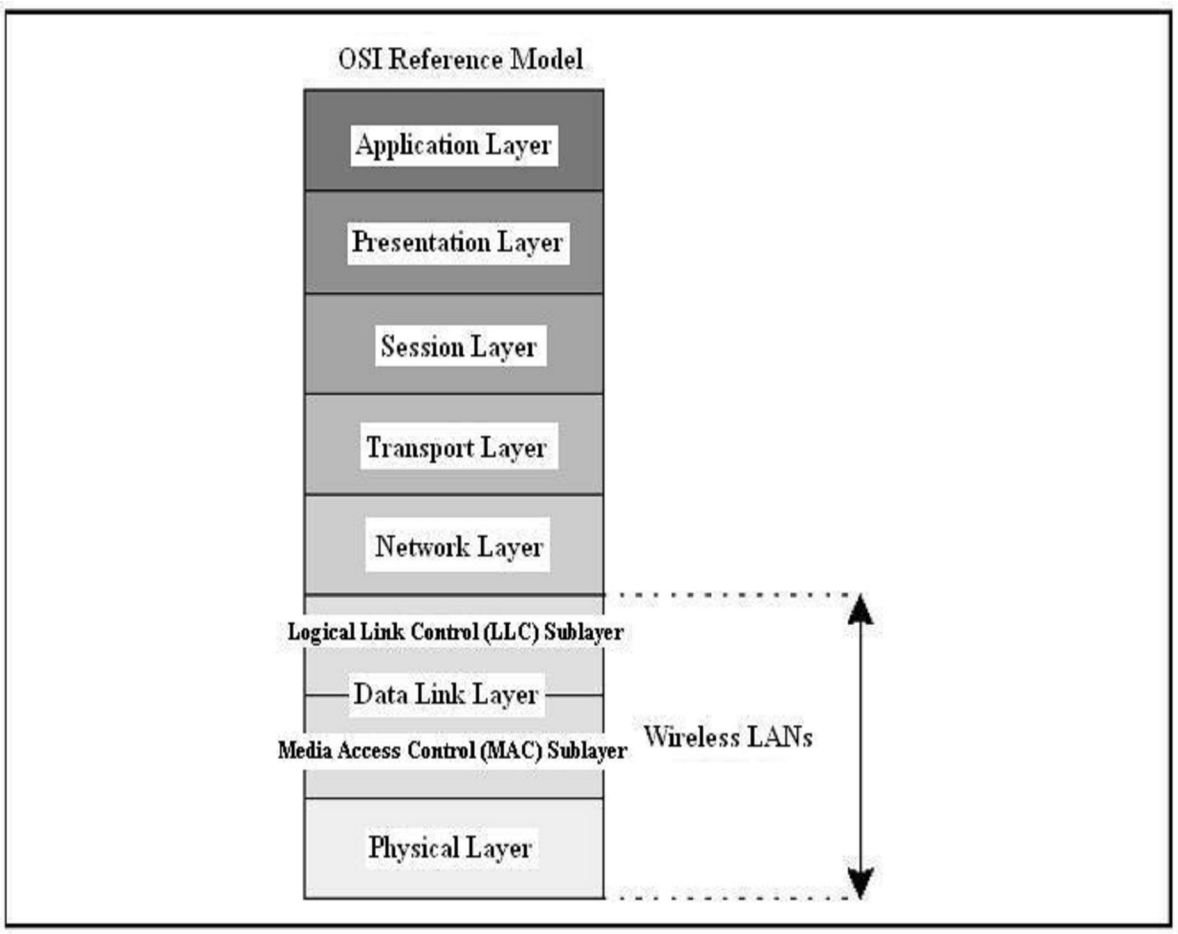

Figura 9: Relação entre o modelo OSI e o 802.11.

Fonte: Confeccionada pelo autor baseado em: http://www.lisha.ufsc.br/~guto/teaching/theses/ono.pdf.

Quando foi proposto o padrão 802.11, ele deveria operar em dois modos, com a presença de um ponto de acesso e sem a presença de um ponto de acesso, modos atualmente chamados de estruturado, figura 10(a) e *ad hoc*, figura 10(b) (Tanembaum, 2003).

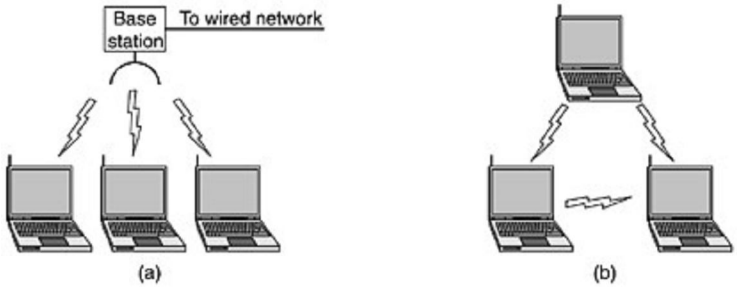

Figura 10: (a) Modo Estruturado; (b) Modo Ad Hoc.

Fonte: Tanembaum, 2003

Essa era a primeira das premissas para a operacionalidade do padrão. Além disso, tinham a resolução de possíveis interferências por obstáculos, a garantia da mobilidade e a garantia de funcionamento na mudança de células numa rede com vários pontos de acesso. Após o atendimento dessas premissas o padrão foi aprovado em 1997 e a partir daí surgiram as derivações a, b (criados em 1999) e g (criado em 2003).

3.3.2 Bluetooth

Bluetooth é uma tecnologia para comunicação sem fio de baixo custo e curto alcance, cuja transmissão de dados se dá através de sinais de rádio de alta freqüência, e através da qual os usuários poderão se conectar a uma variedade de sistemas computacionais (PCs, *notebooks*, PDAs, eletrodomésticos, etc) de forma simples, sem a necessidade de utilização de cabos (*Bluetooth Basics*).

O objetivo é facilitar transmissões de voz e dados em tempo real, permitindo que quaisquer dispositivos eletrônicos fixos ou móveis se conectem, automaticamente e de forma transparente, desde que sejam compatíveis com essa tecnologia.

Foi a Ericsson que iniciou, na década de 90, os estudos para na tentativa de viabilizar uma interface de rádio entre celulares e seus acessórios de baixo custo e consumo. A premissa era eliminação dos cabos.

No início do ano de 1997, a Ericsson buscou outros fabricantes de dispositivos portáteis na tentativa de vender a idéia, após já ter iniciado os trabalhos no desenvolvimento do microchip. O intuito era ter um número aceitável de equipamentos usando essa tecnologia, obedecendo a uma padronização e com isso chegar ao sucesso. Em 1998 foi formado um grupo chamado de SIG (*Special Interest Group*) do *bluetooth*, inicialmente formado pela empresas Ericsson, Nokia, IBM, Toshiba e Intel, unindo empresas de computação e indústria de telecomunicações e logo em seguida surgiu a tecnologia *bluetooth*.

Para o ano de 2008, está sendo esperado o lançamento de dispositivos com consumo de bateria muito mais baixo que os atualmente disponíveis.

De acordo com as informações contidas no sítio www.bluetooth.com, o IEEE homologou o *bluetooth* com a padronização 802.15.1. Nela são definidas as especificações de camada física e da subcamada de controle de acesso ao meio para a conexão de dispositivos que podem ser móveis ou fixos num alcance de 10 (dez) metros. O objetivo da padronização foi de garantir que houvesse interoperabilidade, permitindo transferência de dados, entre os dispositivos com a tecnologia *bluetooth* e com o padrão 802.11.

Os dispositivos *bluetooth* podem se conectar com outros dispositivos *bluetooth* que estejam nas proximidades, formando as redes de transmissão chamadas de *piconets*. As *piconets* são redes locais com cobertura limitada e sem a necessidade de uma infraestrutura (redes *ad hoc*). Cada dispositivo pode se comunicar com mais sete dispositivos por *piconet* e pode operar em várias *piconets* simultaneamente, conforme mostrado na figura 11. As conexões e desconexões são feitas automaticamente com a aproximação ou afastamento das redes.

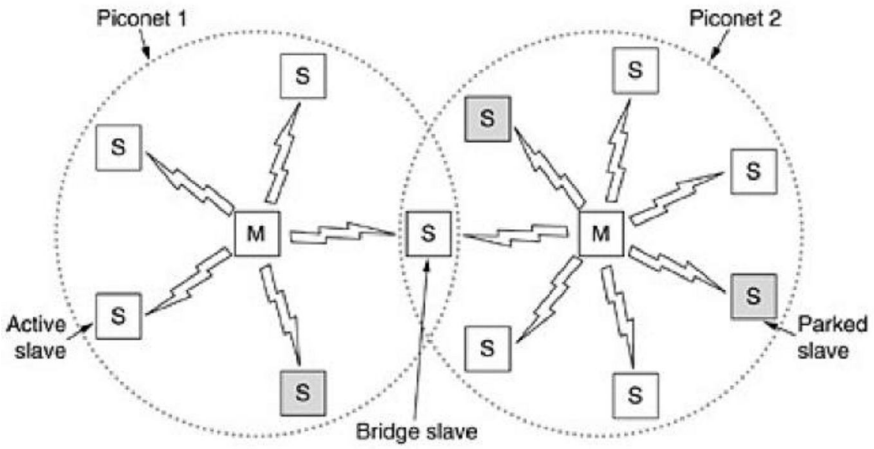

Figura 11: Piconets.
Fonte: Tanembaum, 2003

3.3.2.1 Características Técnicas

O *bluetooth* utiliza a freqüência de operação na faixa de 2,4 GHz, . O modo de transmissão é por espalhamento espectral (*spread spectrum*). O sinal pode ser espalhado acima de uma grande cadeia de freqüências, mas instantaneamente somente uma pequena banda é ocupada, impedindo a maioria das interferências na banda ISM (*Industry, Scientific,*

Medical). As freqüências de transmissão são mudadas de um modo pseudo-aleatório (cada fabricante determina como será feita essa mudança) a uma taxa de 1600 saltos por segundo. Técnica de saltos em freqüência, como a utilizada no padrão 802.11. Essa técnica dificulta as escutas por equipamentos que não fazem parte de rede, mas não as impedem. Por isso foram implementados três modos de segurança descritos abaixo (Karygiannis, 2002):

- Sem segurança (*Non secure*): Este modo é usado com dispositivos que não necessitam de nenhum nível de segurança. Transmissão de dados sem importância.
- Segurança no nível de serviço (*Service level security*): Ocorre o início dos procedimentos de segurança do dispositivo.
- Segurança no nível de link (*Link level security*): É o modo mais seguro. Neste modo o nível de segurança é o mesmo para todas as aplicações e se inicia antes de cada conexão, com o uso de chaves de código, autenticação e criptografia dos dados.

3.3.3 ZigBee

A tecnologia ZigBee utiliza o padrão IEEE 802.15.4 como referência e segue todas as orientações do mesmo para garantir sua sustentação e confiabilidade operacional. Foi desenvolvida para suprir o mercado com mais uma solução para redes sem fio com baixo custo e baixo consumo de energia e que podem ser aplicadas desde uma simples residência até numa indústria.

Oferece diversos tipos de recursos de segurança de dados. É muito bem adaptada para várias aplicações em toda a indústria. Essencialmente naquelas em que poderia se beneficiar da interoperabilidade entre dispositivos, uma das características mais marcantes, que possuem as características fundamentais padronizadas pelo IEEE 802.15.4. A utilização seria independente de uma solução proprietária desde que obedecesse a padronização.

A seguir é mostrada uma figura com as camadas da tecnologia ZigBee mostrando o que foi descrito acima.

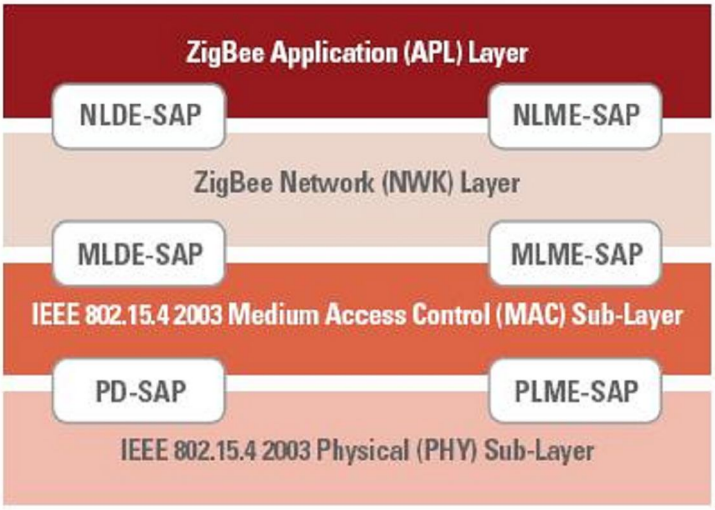

Figura 12: Camadas do ZigBee.

Fonte: *ZigBee and Wireless Frequency Coexistence | ZigBee White Paper - June 2007*

A tecnologia ZigBee, surgiu em 2004 e a entidade que se apresenta responsável por esta tecnologia intitula-se ZigBee Alliance que no sítio www.zigbee.org informa: "*The ZigBee Alliance is an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard*". A ZigBee *Alliance* é uma grupo constituído por mais de 225 empresas que investem bastante no desenvolvimento de produtos e aplicações *wireless*. As aplicações vão de segurança doméstica a controle e automação industrial e predial, entre outras.

Um fato histórico interessante é o da atribuição do nome da tecnologia que é derivado do movimento em ziguezague que as abelhas fazem para informar as outras à distância, direção e localização das fontes de alimento que foram descobertas. Movimento que é semelhante aos múltiplos percursos possíveis da informação entre os dispositivos da tecnologia, utilizados para eliminar possíveis falhas na transmissão dos dados, quando configurados na topologia em malha.

3.3.3.1 Características técnicas

O ZigBee opera em três bandas de rádio denominadas de ISM, 2.4GHz (uso global), 915MHz (América do Norte, Austrália, e alguns outros países) e 868 MHz (Europa).

Utiliza 27 canais, sendo 16 para faixa de 2,4 GHZ, 10 para faixa de 915 MHz e 1 para faixa de 868 MHz, com um taxa de transmissão máxima de 250 Kbps operando em 2,4 GHz e adota a tecnologia DSSS – *Direct Sequence Spread Spectrum* como a melhor maneira de reduzir a taxa de ocupação do canal e garantir a coexistência com outros sistemas que operam na mesma faixa de freqüências.

3.3.3.2 Topologias de rede

Existem três tipos de topologia de rede para a tecnologia ZigBee, conforme figura 13. Nas redes encontramos três tipos de dispositivos chamados de *coordinator*, *router* e *end point.* Eles são implementados com base em dispositivos físicos de classe FFD - *Full Function Device* (Dispositivo com funções completas) ou RFD - *Reduced Function Device* (Dispositivo com funções reduzidas). Na topologia em malha tem-se um dispositivo *coordinator* que se comunica com dispositivos *router* que podem comunicar-se entre si e dispositivos *end point* que só podem comunicar-se utilizando um dispositivo *router*. Na topologia em estrela tem-se um dispositivo *coordinator* central que se comunica com dispositivos *router* ou *end point* e estes só se comunicam entre si utilizando o dispositivo *coordinator* como ponte e na topologia em árvore tem-se uma variação da topologia estrela onde um dispositivo *coordinator* central se liga apenas a dispositivos *router* e os dispositivos *end point* se ligam apenas a dispositivos *router* para estabelecer comunicação.

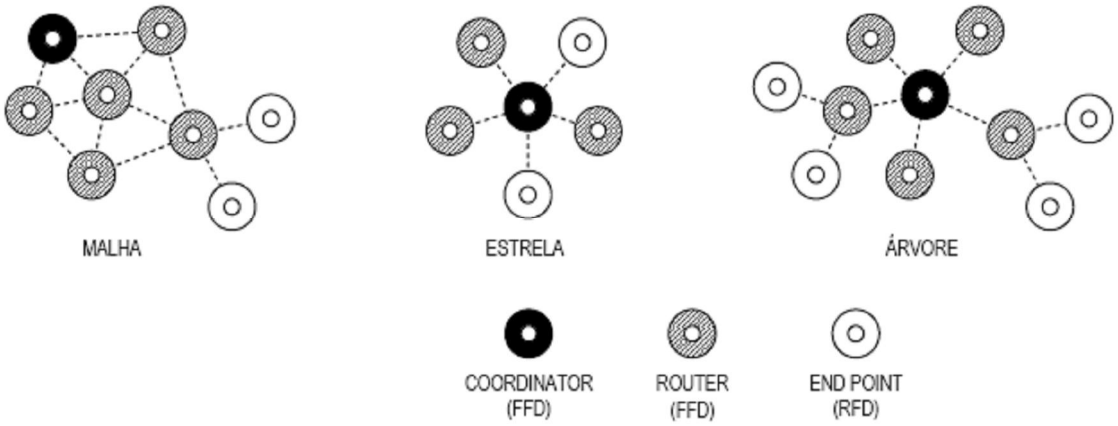

Figura 13: Topologias de rede do ZigBee

Fonte: www.cin.ufpe.br/~meso/sem%20fio/G15_Monografia.pdf .

Os dispositivos físicos citados possuem funcionalidades bem distintas. Os de classe FFD podem funcionar em todas as topologias apresentadas acima e tem a função de coordenar a rede e ter acesso a todos os outros dispositivos. Tem grande complexidade exatamente devido à função de coordenação da rede. Os de classe RFD por serem dispositivos bem simples. Não podem coordenar a rede e para se comunicar têm que estar ligados a um dispositivo FFD. Abaixo são mostradas as funcionalidades dos dispositivos citados.

Coordenador da Rede - FFD	Nó da Rede - RFD
Ajustes de parâmetros da rede	Função passiva na rede
Transmite informações pela rede	Efetua buscas por redes disponíveis
Gerencia os nós da rede	Transferência de dados da aplicação
Armazena informações dos nós de rede	Determina o status dos dados
Distribui mensagens entre nós de rede	Solicita dados ao coordenador da rede
Opera tipicamente no estado "active"	Pode permanecer no estado "sleep" por longos períodos

Quadro 2: Funcionalidades dos dispositivos ZigBee.
Fonte: www.cin.ufpe.br/~meso/sem%20fio/G15_Monografia.pdf

3.3.4 ISA100

O padrão ISA100 que está em desenvolvimento e se baseia no padrão IEEE 802.15.4, tem foco na monitoração sem fio e de todo tipo de ocorrências nos processos industriais. Este pretende garantir confiabilidade e segurança em monitoramento de processos não críticos, em alertas, controle supervisório e aplicações de controle em malha aberta e controle em malha fechada. O padrão define a pilha de protocolos, o sistema de gerenciamento, as especificações de acesso e segurança para conexão *wireless* de baixa velocidade com dispositivos fixos, portáteis e móveis sem a utilização de baterias ou com consumo de baterias muito baixos. Na figura 14 são mostradas as etapas do desenvolvimento do padrão, destacando a situação atual, bem como as principais características do mesmo.

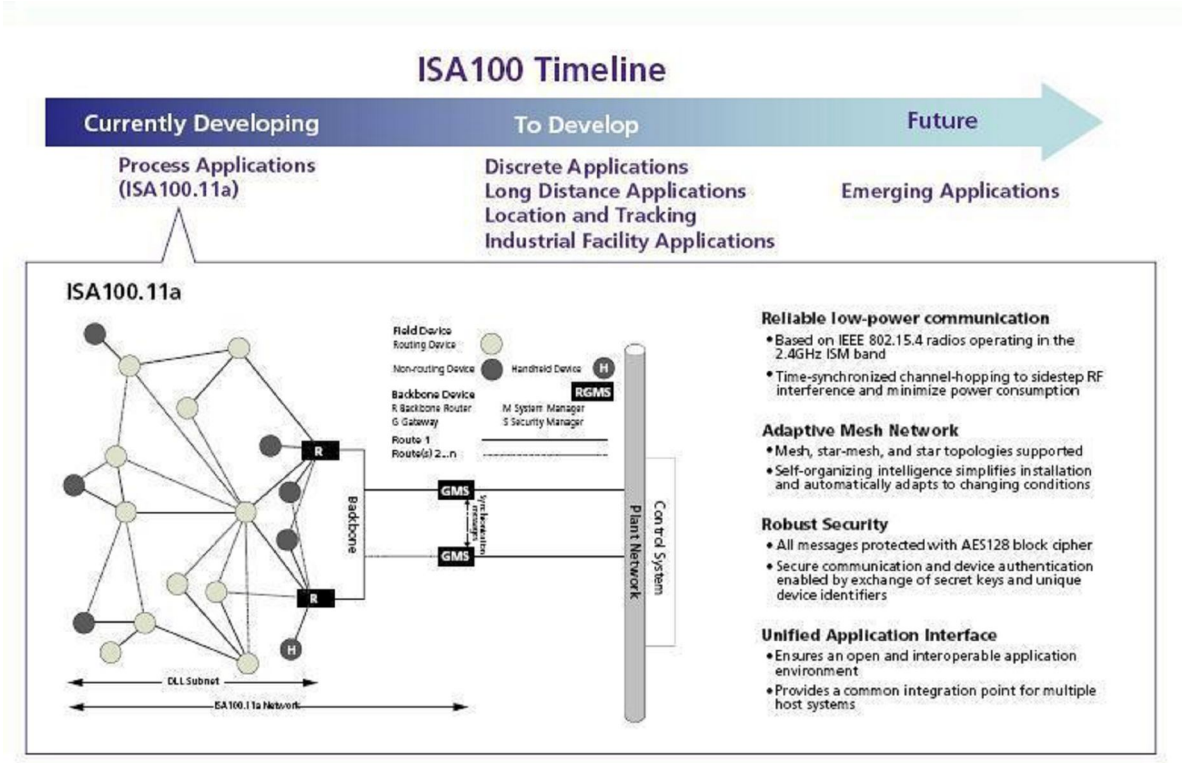

Figura 14: ISA 100 Timeline.

Fonte: www.isa.org/source/ISA100_Big_Picture.pdf

De acordo as informações constantes no sítio www.isa.org, o grupo ISA100 foi formado em 2005 com o objetivo de estabelecer padrões e procedimentos para implementação de sistemas *wireless* para automatização e controle do chão de fábrica. O grupo é formado por mais de 400 profissionais na área de automação e aproximadamente 250 empresas que disponibilizam seus conhecimentos na área para desenvolvimento dos padrões. Para o desenvolvimento da tecnologia o grupo buscou reunir os melhores em sistemas sem fio, instrumentação e segurança de modo a garantir aos usuários confiabilidade na sua utilização no meio industrial.

A família ISA100 está sendo projetada para ser compatível e se integrar a qualquer tipo de processo industrial de modo universal, conforme mostrado na figura 15. O padrão visa permitir a utilização de apenas uma solução sem fio para integrar protocolos como HART, FIELDBUS, MODBUS, PROFIBUS e etc. Ele está sendo aperfeiçoado para enviar informações desses protocolos sem a utilização de fios, preservando todo e qualquer

investimento já feito numa planta industrial. Com isso o a indústria terá apenas uma única tecnologia para aprender, operar, fazer manutenção e um único sistema de segurança para administrar.

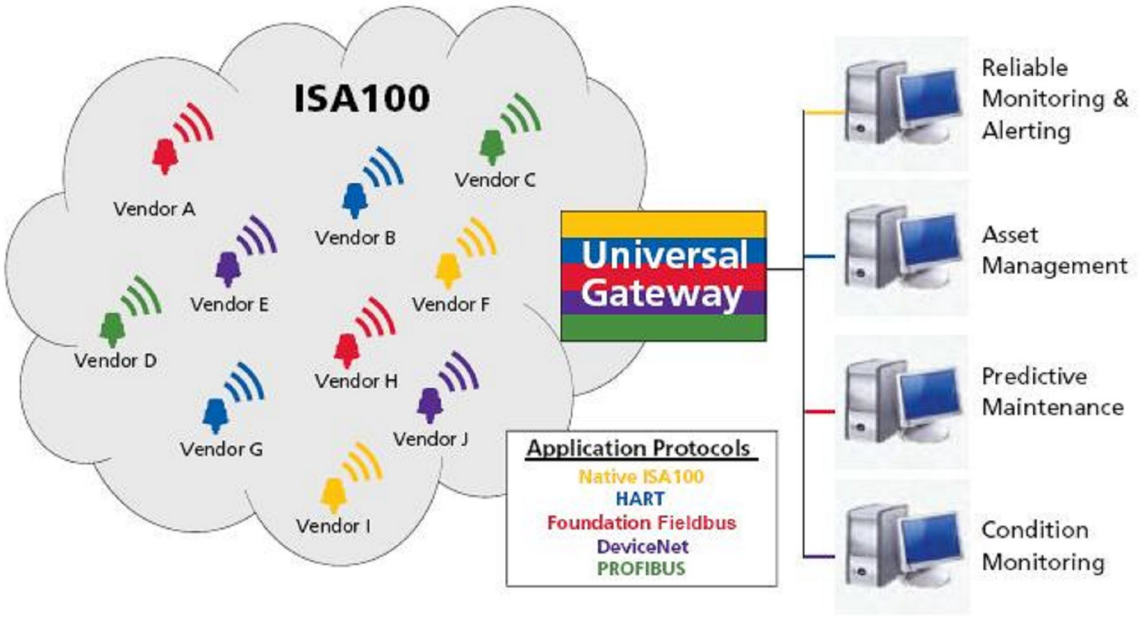

Figura 15: ISA 100 Universal Gateway.
Fonte: www.isa.org/source/ISA100_Big_Picture.pdf

Uma das grandes preocupações para quem pretende utilizar sistemas *wireless* é o "compartilhamento" das freqüências e a possibilidade de congestionamento e interferências na transmissão de dados. O padrão ISA100 já prevê uma solução para estes problemas com o monitoramento do espectro e gerenciamento dos dispositivos escolhendo os canais que estejam livres e forçando a sua utilização na comunicação entre os equipamentos, conforme figura 16.

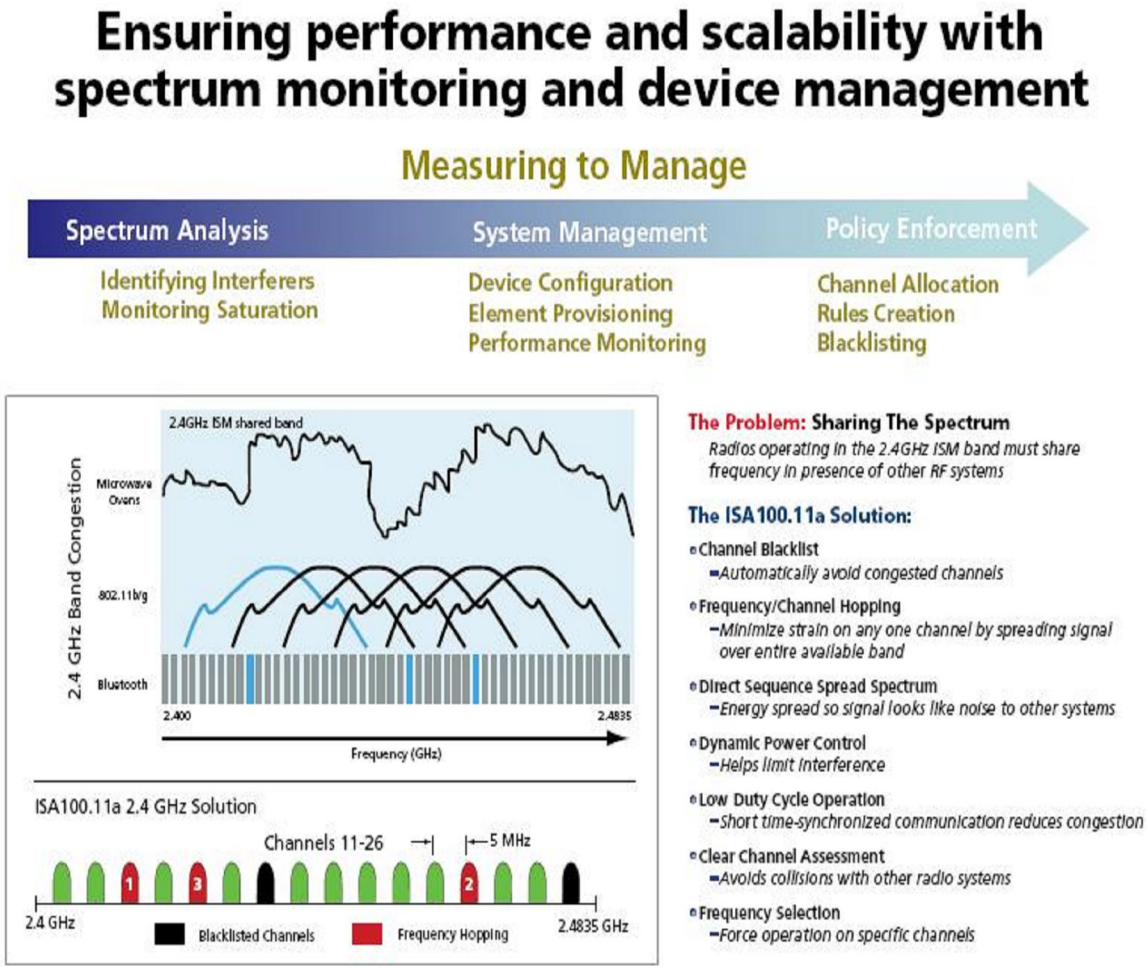

Figura 16: Solução ISA 100 para compartilhamento do espectro.
Fonte: www.isa.org/source/ISA100_Big_Picture.pdf

Existem outros tipos de tecnologias que poderiam ser utilizadas em redes WPAN e WLAN, como: Hiperlan 1 e 2, Infravermelho, Home RF, dentre outros, mas foram escolhidos os mais conhecidos e utilizados em configurações de redes de comunicação sem fios.

4. NORMATIZAÇÃO.

Existem diversas instituições envolvidas com normatização de sistemas *wireless.* São apresentadas as principais no mundo além da instituição brasileira responsável pelo assunto.

4.1 FCC

A FCC - *Federal Communications Commission* é uma agência do governo dos Estados Unidos, independente, ligada diretamente ao Congresso. A FCC foi criada em 1934 com a função de regular e regulamentar as comunicações via todos os meios, nacional e internacionalmente.

4.2 ETSI

O ETSI - *European Telecommunications Standards Institute* produz padronizações para aplicações globais para ICT - *Information and Communications Technologies*, que incluem várias tecnologias: rádios fixos e móveis, radiodifusão e internet.

ETSI é uma organização sem fins lucrativos com mais de 700 membros distribuídos por 60 países ao redor do mundo.

4.3 IEEE

O IEEE tem a função desenvolver padrões de tudo relacionado à tecnologia nos Estados Unidos da América obedecendo às regras estabelecidas pela FCC. O objetivo é promover os processos de criação, desenvolvimento, integração e aplicação do conhecimento em engenharia, tecnologia da informação e ciências para benefício da humanidade.

4.4 Agência Nacional de Telecomunicações - ANATEL

A Agência Nacional de Telecomunicações foi criada em 1997. É uma autarquia federal, vinculada ao Ministério das Comunicações, com a função de regular, regulamentar e fiscalizar os diversos setores das comunicações no Brasil.

A Agência publicou um Regulamento que indica quais as faixas de operação para sistemas *wireless*, indicando as condições para utilização. A Resolução n° 365, de 10 de maio de 2004 - Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita consta o seguinte:

> *"Seção IX - Equipamentos Utilizando Tecnologia de Espalhamento Espectral ou outras Tecnologias de Modulação Digital".*
>
> ...
>
> *"Art. 39. Equipamentos Utilizando Tecnologia de Espalhamento Espectral ou outras Tecnologias de Modulação Digital operando nas faixas de radiofreqüências 902-907,5 MHz, 915-928 MHz, 2400-2483,5 MHz e 5725-5850 MHz devem atender às condições estabelecidas nesta Seção".*

Essas faixas são de uso compartilhado o que traz um certo temor para todos aqueles que tem interesse na utilização de sistemas *wireless*. Mas acreditamos que quando utilizados em ambientes fechados e com os recursos de segurança disponíveis atualmente podem atender a algumas aplicações no chão de fábrica. Futuramente com a utilização desse tipo de tecnologia em uma escala razoável poderá ser alterada a atual regulamentação designando canais exclusivos para utilização no ambiente industrial com autorização específica de canais para cada usuário.

5. VANTAGENS E DESVANTAGENS DA COMUNICAÇÃO SEM FIO

Segue abaixo algumas vantagens de se optar pela comunicação sem fio (Karygiannis, 2002; Mattos, 2006):

- Eliminar a necessidade de passar cabos por tetos, paredes ou solo;
- Manutenção e expansão mais fáceis. Fatores que podem diminuir o retorno dos investimentos realizados na implantação;
- Possibilidade em atingir locais onde não seria possível a instalação de cabos;
- Diversidade de tecnologias: existem diversas opções de padrões o que facilita o atendimento a qualquer tipo de usuário;
- Alteração das configurações dos equipamentos facilitada;
- Possibilidade de operação de vários equipamentos simultaneamente e na mesma faixa de freqüência;
- Utilização em ambientes internos e externos;
- Mobilidade: os usuários podem acessar diversos recursos da rede sem necessidade de conexão física, bastando apenas estar na área de cobertura delimitada para o seu funcionamento;
- Flexibilidade: os usuários podem instalar e desinstalar uma pequena WLAN rapidamente podendo, assim, atender necessidades temporárias de comunicação;
- Instalação mais rápida e facilitada, pois não há necessidade de cabeamento.

Agora, segue abaixo algumas desvantagens de se optar pela comunicação sem fio (Reis, 2003; Sudré, 2006):

- Maior vulnerabilidade em relação à segurança do que na rede cabeada;
- Maior suscetibilidade a interferências do meio ambiente (como obstáculos entre as antenas);
- Interferências de outros sistemas que operam nas proximidades utilizando a mesma faixa de freqüência;
- Taxa de erros elevada;

- Faixa de operação sem necessidade de licenciamento, sendo assim mais propício a interferências devido ao uso indiscriminado;
- Largura de banda limitada: é limitada devido a operar em uma faixa de freqüências de uso compartilhado;
- Alto consumo de baterias (energia) dos equipamentos portáteis;
- Riscos para a saúde causada pela radiação eletromagnética: existe uma grande preocupação quanto a esse risco, mas já existem diversos estudos e recomendações para instalação e certificação de equipamentos de modo a emitir o nível mínimo de radiações.

6. SEGURANÇA EM REDES DE COMUNICAÇÃO *WIRELESS.*

A segurança é um dos assuntos que mais preocupam àqueles que utilizam ou pretendem utilizar redes *wireless*. Os fabricantes e institutos de pesquisas na área buscam, desde seu início, disponibilizar padrões que garantam a segurança nas comunicações sem fio, equivalentes a de redes cabeadas, de modo a difundir ainda mais o uso da tecnologia.

Para se garantir que uma rede sem fios possua características de segurança semelhantes às que possuem as redes cabeadas, tem-se a necessidade de utilização ou desenvolvimento de mecanismos de autenticação de dispositivos e de garantia da confidencialidade da informação transmitida. A área de abrangência de uma rede sem fio é definida pela capacidade de cobertura dos *Access Points*, que podem variar muito dependendo da potência de transmissão e das características das antenas utilizadas nas estações que compõem a rede, um dos pontos que será citado mais à frente. Os mecanismos de segurança devem ser aplicados na camada de enlace de dados e, dependendo de quão crítica sejam as aplicações que se processarem na rede deve-se utilizar segurança adicional nas camadas superiores (Jubran, 2004), para garantir o funcionamento sem risco de todas as aplicações.

Hoje são disponibilizados meios de garantir a segurança nas redes *wireless* através de mecanismos de autenticação (WEP, EAP, listas de acesso e outras) que se bem utilizados podem trazer um nível significativo de segurança.

Como a proposta é a utilização no chão de fábrica como uma extensão da rede cabeada e num ambiente fechado, como mostrado na figura 17, acredita-se que as ferramentas disponíveis atualmente, aliadas a ferramentas de segurança das redes cabeadas, atualmente possam garantir a viabilidade da utilização dos sistemas *wireless*.

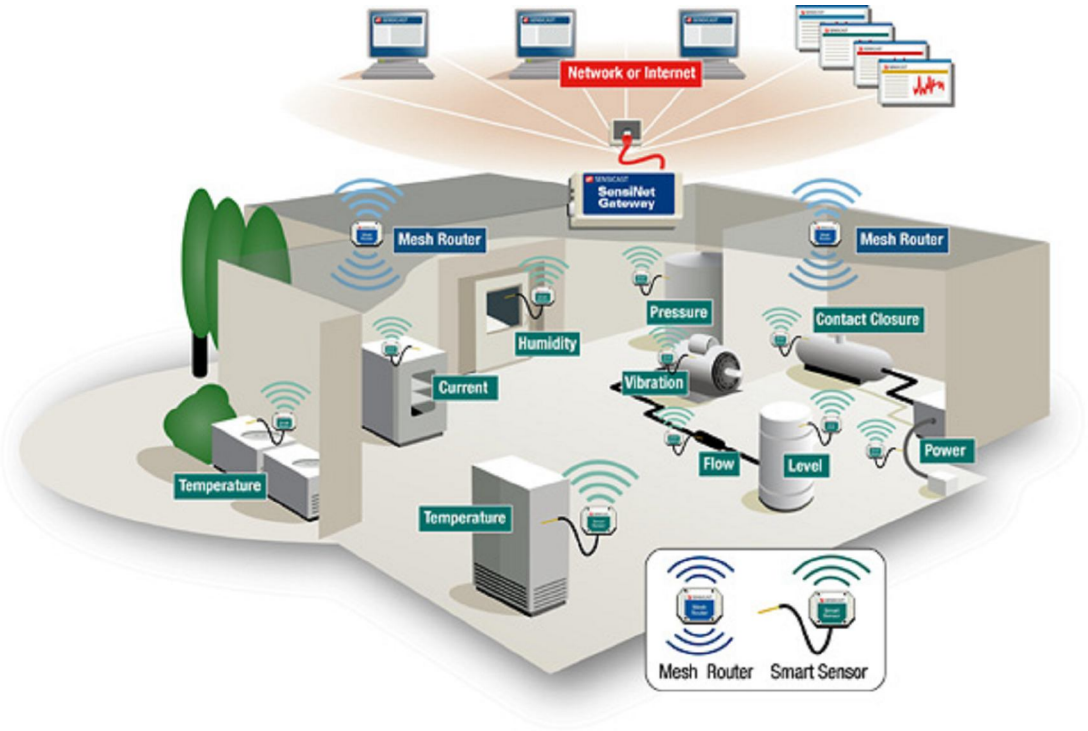

Figura 17: Tecnologia *Wireless* no Chão de Fábrica.
Fonte: http://www.sensicast.com/products.php

Para se proteger uma rede de comunicação cabeada ou sem fios uma seqüência de procedimentos deve ocorrer dependendo de onde vem os recursos se da rede corporativa ou do chão de fábrica (*Prosoft Technology*, 2005):

Autenticação: que é o processo de verificação onde o usuário confirma sua identificação para que possa estabelecer uma conexão com a rede de forma confiável. Esta etapa provê controle de acesso à rede negando acesso a usuários que não podem autenticar-se corretamente;

Autorização: é a fase seguinte à autenticação que protege os recursos do computador permitindo acesso àqueles que realmente possuem autorização. Nesta fase o usuário devidamente autenticado recebe acesso as informações que estão permitidas para ele;

Criptografia: que é o processo utilizado para fazer com que a informação se torne ilegível para quem não possua os recursos específicos para decifrá-la. A criptografia garante a

integridade da informação também já que apenas o usuário autorizado e autenticado, em tese, possui o software para leitura dos dados;

Integridade: refere-se à validação da informação contra alterações acidentais ou maliciosas. Existem protocolos que foram desenvolvidos para assegurar que as informações sejam modificadas em trânsito entre os usuários da rede sem fios e o ponto de acesso no caso de ataques ao sistema de comunicação

Na figura 18 é mostrado um dos processos de autenticação de um usuário buscando obter autorização para obter acesso a uma rede de comunicação sem fio. Esse processo de autenticação é chamado de *Shared Key* e utiliza o recurso da criptografia para fazer a autenticação dos usuários (Karygiannis, 2002).

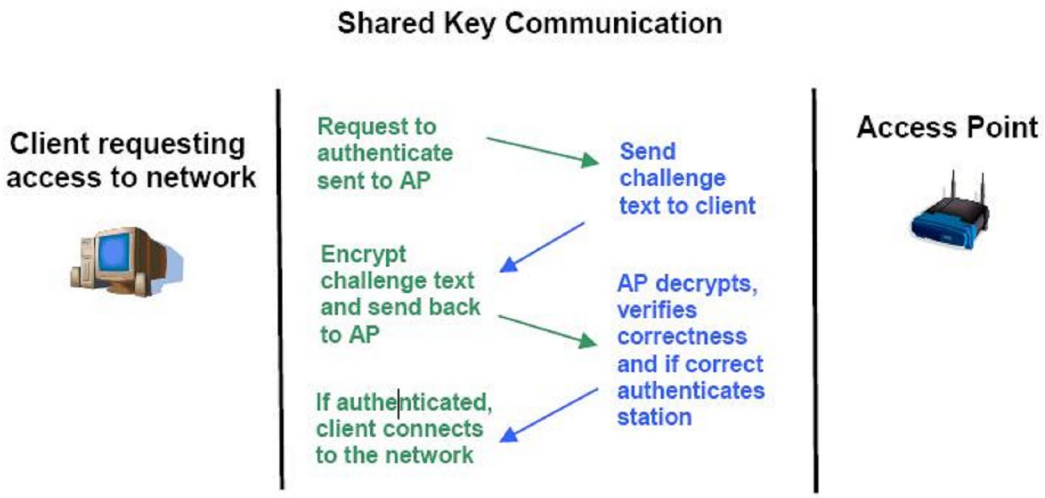

Figura 18: Exemplo de processo de autenticação – *Shared Key*.
Fonte: *Prosoft Technology*, 2005

Foram citadas, anteriormente, diversas desvantagens na utilização de sistemas sem fio. A principal delas, e mais preocupante, é a falta de segurança. Segundo Matthew Gast, no artigo *Seven Security Problems of 802.11 Wireless* (Gast, 2002), são sete os principais problemas de segurança na utilização de redes *wireless*:

- Fácil acesso;
- “Falsos” APs;
- Uso não autorizado do serviço;
- Limitações da tecnologia e desempenho;
- *MAC Spoofing* e *Session Hijacking* (ataque onde uma pessoa ou programa consegue se fazer passar por outra obtendo acesso não autorizado e acesso a informações ou a serviços em uma rede).
- Análise de tráfego e *Eavesdropping* (violação de confidencialidade - grampo);
- Ataques no nível mais alto.

Fácil Acesso: A localização de redes *wireless* é fácil devido às especificações desse tipo de tecnologia serem abertas e existirem diversos softwares que permitem essa ação. Caso não sejam utilizados os recursos mínimos de segurança que cada tecnologia oferece o acesso aos dados da rede fica mais facilitado ainda. No caso do padrão 802.11 deve-se habilitar o protocolo WEP que permite criptografar o tráfego entre as estações e o AP, alterar o SSID (*Service Set IDentifier*) que é a identificação dos APs em redes sem fio, e desabilitar a função de broadcast que emite informações sobre a identificação da rede que podem ser filtradas e permitir acesso não autorizado.

Outro procedimento é dar uma atenção especial a localização dos APs de modo a se obter o maior aproveitamento das características dos equipamento obtendo uma cobertura satisfatória, confinando ao máximo o sinal da rede na área de interesse. Deve-se evitar a proximidade com janelas, para se evitar possíveis interferências, e instalá-los numa disposição o mais central possível.

“Falsos” APs: A adoção e desenvolvimento de procedimentos de segurança e monitoramento de APs que não compõem a rede são de grande importância para evitar acessos indesejados.

Alguns fabricantes oferecem softwares que afirmam poder localizar esses equipamentos com bastante precisão.

Uso não autorizado do serviço: O melhor procedimento para garantir que não haja uso não autorizado é utilizar ferramentas robustas de criptografia que evitem a autenticação de usuários que não devem ter acesso à rede. A utilização de VPNs, que oferecem diversos recursos de segurança que podem ser uma solução eficaz para proteger as informações que transitam pela rede, e IPSEC que é um protocolo que protege os pacotes IP fazendo o encapsulamento dos dados em outros pacotes IP para daí serem transmitidos.

Limitações da tecnologia e desempenho: Existem muitos tipos de tecnologia sem fio disponíveis o que pode ocasionar interferências e congestionamento do tráfego de informações. Foram apresentadas algumas tecnologias que podem ser utilizadas no chão de fábrica. A melhor forma de se garantir a segurança é escolher aquela que ofereça o maior número de recursos, tenha um desempenho satisfatório e que possa coexistir com as outras que possam estar instaladas em regiões próximas.
Uma avaliação prévia do espectro na região onde será instalada uma nova rede sem fio, e avaliações periódicas após a instalação, deverá ser feita para que problemas sejam evitados.

***MAC Spoofing* e *Session Hijacking*:** Usuários não autorizados podem utilizar falsos frames para redirecionar o tráfego e corromper a lista ARP. O *MAC address* dos dispositivos que compõem a rede podem ser observados e utilizados para o acesso. Com isso podem obter autenticação e utilizar a rede.

Nesse caso deve ser utilizada uma lista de acesso com todos os MAC *address* de todos os dispositivos que tem autorização de acesso a rede e novamente adotar protocolos de segurança robustos.

Modificar os parâmetros SNMP (*Simple Network Management Protocol*), já que na utilização no chão será necessário o gerenciamento das informações, para se obter uma maior segurança é recomendado utilizar a versão 2 do protocolo, que corrige algumas das imperfeições da versão 1. Já existe em desenvolvimento o SNMPv3, que define um conjunto de especificações para segurança da rede e controle de acesso. Essa versão não

pode ser utilizada sozinha devendo ser conjugada com o SNMPv2, preferencialmente, ou com o SNMPv1.

Desabilitar o DHCP (*Dynamic Host Configuration Protocol*), com esse procedimento os usuários não autorizados seriam forçados a decifrar o IP, a máscara de rede e outros parâmetros de TCP/IP exigidos para conexão a rede.

Análise de tráfego e *Eavesdropping*: Com a utilização de softwares específicos, muitos disponíveis facilmente na rede mundial de computadores, "*crackers*" podem monitorar o tráfego das redes sem fio e colocar um "grampo" e daí conseguir as informações necessárias para invadir e utilizar os recursos da rede como um usuário autorizado.

Ataques no nível mais alto: Normalmente as redes seguras são configuradas com todas as ferramentas possíveis para proteção. Mas, na maioria das vezes isso só é válido para a segurança contra invasões externas. A segurança interna é deixada de lado o que pode permitir a invasão da rede por usuários não autorizados. A segurança física é muito importante, os equipamentos devem estar localizados onde apenas pessoas autorizadas possam ter acesso, a entrada de equipamentos eletrônicos, possíveis "invasores" deve ser registrada e a monitoração do tráfego de informações sem fio deve ser constante.

Foram apresentadas anteriormente, possíveis soluções para os principais problemas de segurança em redes *wireless*, mas para se ter um bom aproveitamento dos recursos de segurança oferecidos por cada tecnologia deve existir um planejamento para implantação das mesmas da mesma forma que existe quando da implantação de redes cabeadas.

Jubran (2004), propõe uma metodologia, explicada mais à frente, para a implementação de redes locais sem fio em médias e grandes empresas, figura 19. Seu objetivo é obter um roteiro de implantação lógico com vários aspectos como hardware para servidores e clientes, softwares específicos de segurança e adequação do ambiente físico como localização dos *Access Points*, *backbone* cabeado para os *Access Points* e demais equipamentos.

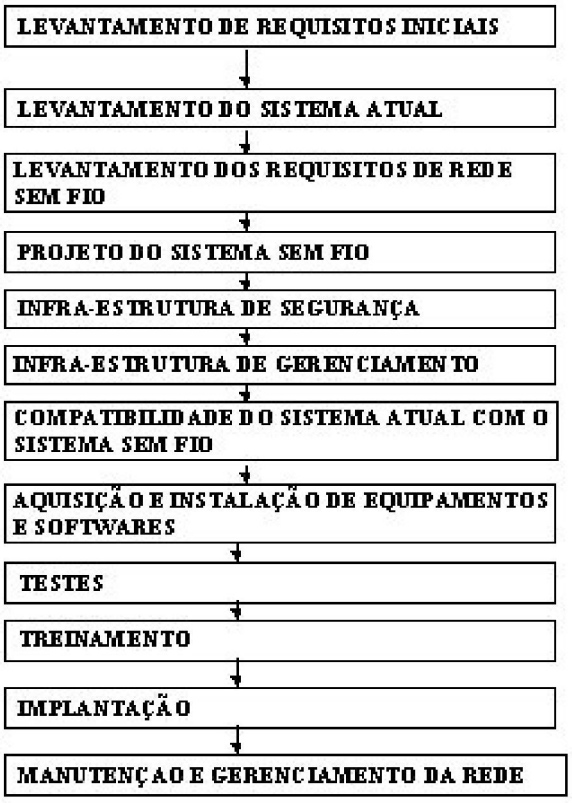

Figura 19: Metodologia Proposta de Projetos de Redes Locais Sem Fio

Fonte: Jubran, 2004

Levantamento de Requisitos Iniciais: Verificação de quantos pontos de acesso sem fio serão necessários para atender a área em que se deseja implantar a tecnologia em complemento a rede local já existente. Deverá ser produzido um relatório com as informações relativas às necessidades da empresa.

Levantamento do Sistema Atual: Realização de um levantamento de todos os componentes existentes na rede local existente, colhendo as informações/características dos equipamentos instalados (*hubs*, *switches*, *gateways*, roteadores, servidores e etc.), dos softwares utilizados e do cabeamento. Esse levantamento é de grande importância já que a intenção é fazer uma integração entre a rede cabeada existente e a rede sem fio e garantir o planejamento para expansões futuras

Levantamento dos Requisitos de Rede Sem Fio: Tendo sido realizado o levantamento das características da rede atual deve-se partir para determinação dos requisitos da rede sem

fio. Determinar quantidade de pontos de acesso, as características físicas das estações, qual o tipo de informação que trafegará na rede, a qualidade do serviço desejada, se há perspectiva de ampliação da rede, os requisitos de segurança, com será feito o gerenciamento, dentre outros itens.

Projeto do Sistema Sem Fio: Após a aquisição das informações das etapas anteriores, deve-se começar os cálculos para definição da quantidade de células que serão necessárias para atendimento a área ou áreas onde será instalado o sistema sem fio, ficando atento as limitações das tecnologias como: quantidade de estações por célula, velocidade e potência de transmissão, alcance e quantidade de canais disponíveis. Determinar os melhores pontos para instalação dos dispositivos de modo a garantir que o sistema funcione satisfatoriamente atendendo a todos os usuários e permitindo que ocorram ampliações da rede e que tenha uma redução significativa nos problemas de interferência externa e interna.

Infra-Estrutura de Segurança de Redes Sem Fio: Para se obter maior nível de segurança nesse tipo de rede busca-se utilizar o máximo de recursos de segurança oferecidos pelos equipamentos e pelos aplicativos, dependendo da necessidade da empresa.

Infra-Estrutura de Gerenciamento: O gerenciamento de uma rede é operado por *softwares* dos próprios fabricantes ou fornecedores dos equipamentos. Estes *softwares* têm a função de gerenciamento de falhas, desempenho, segurança e configuração e devem ser compatíveis com a rede existente.

Compatibilidade do Sistema Atual com o Sistema Sem Fio: Dependendo da rede existente poderá ser necessária a aquisição de novos dispositivos de *software* e *hardware* que suportem a inclusão de novos pontos de acesso com a nova tecnologia e que sejam compatíveis com a mesma.

Aquisição e Instalação de Equipamentos e Softwares: Depois de terminado o projeto deve-se partir para o levantamento de preços dos dispositivos especificados nas empresas disponíveis do mercado. Atentando-se para as características de cada equipamento porque

estas podem ser diferentes a depender do fabricante e fazer com que a rede não opere da forma projetada. Após a instalação devem ser instalados e configurados em cada equipamento os softwares de acordo com o que foi projetado.

Testes: Devem ser realizados todos testes necessários para garantir o funcionamento satisfatório dos dispositivos de software e hardware incluídos na nova rede.

Treinamento: Uma etapa muito importante da metodologia, pois todos os profissionais envolvidos na operação e manutenção da rede devem estar capacitados a administrar, gerenciar, configurar e manter o funcionamento satisfatório do sistema. A contratação de uma empresa para ministrar o treinamento inicial e de futuras atualizações é de grande importância.

Implantação: Esta etapa é feita logo após a realização dos principais testes na rede. Ela deve seguir criteriosamente o cronograma proposto para implantação de modo a não superar os custos previstos inicialmente.

Manutenção e Administração da Rede: O responsável pela administração da rede de comunicação deverá possuir os conhecimentos necessários para verificar se a mesma está operando de forma satisfatória e saber tomar as decisões certas para resolução dos problemas. Nessa etapa, a participação dos profissionais nos treinamentos é de suma importância.

A utilização de uma metodologia tem grande utilidade na garantia de uma implantação e funcionamento satisfatórios de um projeto de uma rede sem fio. Nela será possível definir com maior facilidade todos os pontos críticos na operação e manutenção da rede, pois permite avaliar passo a passo cada uma de suas etapas.

Sendo assim, como no chão de fábrica a maior preocupação é com a segurança dos dados e a garantia da transmissão às estações de monitoramento, o investimento não deve ser apenas em tecnologia, mas, também em treinamento dos profissionais e numa avaliação

criteriosa dos reais objetivos da implantação de uma rede sem fio, de modo a minimizar ao máximo os problemas que afligem os gerentes de plantas industriais.

7. EXEMPLO DE APLICAÇÃO DE UM SISTEMA WIRELESS NO CHÃO DE FÁBRICA.

A seguir tem-se um exemplo de aplicação de redes de comunicação sem fio mostrando que uma solução simples pode oferecer algumas das vantagens, citadas no início do trabalho, para o ambiente industrial.

Lloyd Pentecost, Supervisor de Engenharia de Manutenção da Estação de Geração de Energia Nuclear na cidade de San Onofre, na Califórnia, pesquisou um método para monitorar uma grande planta secundária de motores utilizando um sistema de redes sem fio. (www.wireless.industrial-networking.com)

Monitoramento da temperatura de motores de bombeamento dá uma indicação das condições operacionais ou da "saúde" de motores de 2500 cavalos. Se um motor falhar inesperadamente, a planta funcionaria com apenas 80% da capacidade por um determinado número de dias, o que resultaria em perdas que poderiam exceder U$ 400,000. Coletar e analisar os dados da temperatura dos motores em tempo real permite a tomada de ações antes da ocorrência de uma falha catastrófica.

Com o sistema de monitoração desenvolvido, foi decidido pelo uso de uma nova tecnologia de comunicação de dados sem fio. Sem um novo cabeamento iria se economizar nos gastos, no tempo e ter um ROI - *Return Over Investment* considerável. Pentecost exigiu um sistema que fosse confiável ao operar em um ambiente ruidoso (ruídos de RF – *Radio Frequency*) e que satisfizesse exigentes requisitos de segurança, ao mesmo tempo em que fornecesse possibilidades para uma futura expansão.

Uma rede sem fio 802.15.4 da *Sensicast* foi escolhida. “Avaliando diversas tecnologias sem fios, a plataforma de rede da *Sensicast* apresentou os recursos ideais exigidos para o trabalho”, disse Pentecost. "Com sensores alimentados por baterias, fios não são

necessários. Teve excelente desempenho e escalabilidade, em comparação com as outras tecnologias testadas".

Como parte do sistema de Pentecost, B & B *Electronics* está fornecendo conversor personalizado nós sem fio de RTD para 802.15.4, figura 20. Eles vão se conectar a sensores incorporados ao RTD e converter os sinais analógicos em sinais de RF para a rede sem fio.

FEATURES

- Two or four-channel RTD inputs
- RTD types supported:
  - 2, 3 and 4 wire inputs
  - 10 Ω, Copper RTD support
  - 100 Ω, Platinum RTD support
- Supported by the Sensicast EMS Management software, permitting real-time charting, alerts and historical analysis capabilities
- Data accessible via OPC Server
- Totally wireless – no data or power wiring is required
- Range of up to 212 meters outdoors
- User-definable, remotely settable transmission
- Advanced frequency hopping radio designs provide reliable connectivity in harsh RF environments
- Supports message acknowledgements and redundant routing, for totally reliable wireless connectivity
- Automatic network joining; no configuration required
- Wireless firmware upgrade capability
- Optional 10-30 VDC power input via pluggable terminal

SPECIFICATIONS

Sensor-related Specifications	
Radio	IEEE 802.15.4 compliant, 2.4 GHz DFSS
Regulatory	FCC Part 15 and CE Approval
Antenna	Internal antenna
Range	• Up to 212m (700') range (outdoor, line of sight) • Up to 70m (230') range (typical indoor conditions)
Operating temperature	-10°C to 50°C
Operating humidity	Up to 100% non-condensing
Power Options	AA 3.6V lithium thionyl chloride battery. 10-30V DC power input terminals (optional use)
Battery life	• TEMP- 1022 & TEMP-1122 2 years with two minute reporting interval • TEMP-1024 & TEMP-1124 1.5 year with two minute reporting interval • On board battery life status via LED Indicator
Duty cycle	Remotely user-adjustable; default to 1 minute
LED	Diagnostic LED indicating power/connectivity
Dimensions	• 3.5" x 5.5" x 1.375" • 89 mm x 140 mm x 35 mm
Packaging	ABS Box – IP30 rated.
Mounting options	• One or two screws • Double-sided adhesive tape
RTD-related Specifications	
RTD terminal connection	• #28 to 14 AWG wire gauge • Clamping yoke connection • Pluggable terminal block connector
Supported RTD Types	2, 3 and 4 wire versions of:
TEMP-1022 & TEMP-1024	• 10W @ 25°C, Copper; 0.00427 W/W/°C • 100W @ 0°C, Platinum; 0.00392 W/W/°C • 100W @ 0°C, Platinum; 0.00385 W/W/°C
TEMP-1122 & TEMP-1124	(High Temperature Range) • 100W @ 0°C, Platinum; 0.00385 W/W/°C
Temperature range	TEMP-1022 & TEMP 1024: -100°C to 200°C TEMP-1122-H & TEMP 1124: -20°C to 540°C

Figura 20: RTD da Sensicast

Fonte: http://www.sensicast.com/products.php

"B & B tem trabalhado com a plataforma sem fio 802.15.4 há vários anos. Estamos satisfeitos por ter a nossa tecnologia incorporada neste programa", afirmou Craig Skarpiak, Gerente da Linha de Produtos *Wireless* (sem fio) da B & B *Electronics*. IEEE 802.15.4 é apenas um dos padrões sem fio na qual B & B *Electronics* é especializada.

Com o que foi apresentado, confirma-se que a utilização de uma rede de comunicação sem fio pode ser segura desde que seja bem planejada, seguido os passos apresentados no capítulo 7 e pode operar em ambientes ruidosos desde que seja feita a escolha correta do fabricante/fornecedor da tecnologia. No exemplo mostrado, o fornecedor da solução utiliza uma tecnologia de transmissão de saltos em freqüências que garante a transmissão dos sinais de forma confiável e em tempo real permitindo o gerenciamento das informações da rede satisfatoriamente. Além disso, confirma algumas das vantagens que foram apresentadas no capítulo 5 como redução nos custos de implantação e possibilidade de expansão facilitada.

8. CONCLUSÕES

8.1 CONSIDERAÇÕES FINAIS

As redes de comunicação sem fio podem trazer muitas facilidades para o ambiente industrial mesmo com a existência de algumas desvantagens como problemas de interferências causadas por motores, ou equipamentos diversos que utilizem à mesma freqüência de operação e problemas de segurança que é o assunto principal do trabalho.

Para garantir a eficiência, o aproveitamento de todos os recursos oferecidos e a utilização com segurança de um sistema *wireless*, é necessário um bom estudo das tecnologias disponíveis para se escolher qual atenderá as necessidades do usuário, incluindo aí os protocolos de segurança já oferecidos pela tecnologia, um planejamento criterioso de como serão feitas a instalação e configuração dos dispositivos. Para que sejam reduzidos ao máximo os principais problemas, citados no capítulo 7, na utilização desses dispositivos no chão de fábrica.

Enquanto existir alguma desconfiança por parte dos responsáveis pela plantas industriais, os sistemas poderão ser usados inicialmente em aplicações mais simples como monitoração e coleta de dados, que já tem um nível razoável de segurança, e futuramente em aplicações mais críticas com o desenvolvimento de equipamentos e softwares que dêem à segurança e qualidade de serviço requerida, e tão perseguida pelos institutos de pesquisa do assunto, aliada a maiores taxas de transmissão de dados. Deste modo, essa tecnologia vai envolver um maior número de aplicações e fazer com que o chão de fábrica opere com maior eficiência e com toda segurança necessária.

8.2 PROPOSTA PARA ESTUDOS FUTUROS

Uma proposta para estudo futuro seria a especificação de uma rede de comunicação sem fio para a planta modelo do SENAI/CIMATEC. Com o auxílio da metodologia proposta por Jubran (2004), que é um roteiro de implantação para redes locais sem fio utilizando uma seqüência de etapas que incluem desde especificação de *hardware* e *software* à capacitação dos usuários da rede, apresentada no capítulo 7, seria possível determinar qual a melhor tecnologia *wireless* para fazer o monitoramento de todas as informações que possam ser extraídas da planta. Com a definição da melhor tecnologia e implantação do sistema com todos recursos de segurança necessários seria possível simular invasões de usuários não autorizados à rede de comunicação, simular o monitoramento remoto com sistemas computacionais móveis, alterar parâmetros de funcionamento da planta, enfim testar todos os recursos oferecidos pela tecnologia adotada.

Com isso os alunos da entidade teriam a oportunidade de ter um conhecimento aprofundado das tecnologias *wireless*, compará-las com as tecnologias utilizadas atualmente no chão de fábrica, propor melhorias ao que existe disponível hoje no mercado e com isso contribuir para a difusão das tecnologias de comunicação sem fio no chão de fábrica.

REFERÊNCIA BIBLIOGRAFICA

ANATEL, Agência Nacional de Telecomunicações, Disponível em: http://www.anatel.gov.br . Acessado em 21/09/2007.

Bluetooth Basics. Disponível em: http://www.bluetooth.com/Bluetooth/Learn/. Acessado em 25/10/2007.

Case study: Into a nuclear power plant with 802.15.4 wireless. Disponível em: http://wireless.industrial-networking.com/articles/articledisplay.asp?id=236. Acessado em: 22/10/2007.

Dígitro Tecnologia. Glossário Tecnológico. Coordenação Eng. Juliano Anderson Pacheco, desenvolvida por Adm. Claudio Brancher Kerber, apresenta termos tecnológicos na área de telecomunicações. Disponível em: http://www.digitro.com/glossario_digitro.php. Acessado em: 10/12/2007.

ETSI, *European Telecommunications Standards Institute*, Disponível em: http://www.etsi.org. Acessado em 17/12/2007.

FARIAS, Paulo César Bento. Treinamento Profissional em Redes *Wireless*. – São Paulo: Digerati Books, 2003.

FARIAS, Paulo César Bento. Tutorial em Redes *Wireless* – Parte VI, 26/05/2006. Disponível em http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless006.asp. Acessado em 29/09/2007.

FCC, *Federal Communications Commission*, Disponível em: http://www.fcc.gov. Acessado em 21/09/2007.

GAST, Matthew. Sete Problemas de Segurança de 802.11 - O'Reilly Network - Matthew Gast e AirMagnet, 2002. Disponível em http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html.Acessado em: 28/11/2007.

IEEE, *Institute of Electrical and Electronics Engineers*, Disponível em: http://www.ieee.org . Acessado em 29/09/2007.

ISA100: *Wireless Systems. for Industrial Automation.* Disponível em www.isa.org/source/ISA100_Big_Picture.pdf. Acessado em 12/10/2007.

JUBRAN, Aparecido Jorge; JUBRAN, Laura Martinson Provasi ; CIPPARRONE, F. A. M. et al. Planejamento para Implementação de Redes Locais Sem Fio em Empresas de Médio e Grande Porte. In: WORKCOMP-SUL, 2004, Santa Catarina. Disponível em: http://inf.unisul.br/~ines/workcomp/cd/pdfs/2884.pdf . Acessado em 11/12/2007.

KARYGIANNIS, Tom and Owens, Les. NIST Special Publication 800-48, Wireless Network Security 802.11, Bluetooth and Handheld Devices. November 2002. Disponível em: Acessado em 29/09/2007.

Knowledge Center Overview.
Disponível em: http://www.wi-fi.com/knowledge_center_overview.php?type=3#3794. Acessado em 05/12/2007.

KUROSE, James F., Redes de Computadores e a Internet: uma nova abordagem / James F. Kurose, Keith W. Ross; Tradução Arlete Simille Marques; revisão técnica Wagner Luiz Zucchi. – 1.ed - São Paulo: Addison Wesley, 2003.

MATTOS, Guilherme Marques. Rede de acesso em banda larga utilizando sistema VSAT e Wi-Fi/ Guilherme Mattos Marques; Orientador Luiz A. R. da Silva Mello. Rio de Janeiro: PUC. Departamento de Engenharia Elétrica, 2006. Disponível em: http://www.maxwell.lambda.ele.puc-rio.br/. Acessado em 07/11/2007.

METCALFE, R. M.: “On Mobile Computing”, Byte, vol.20, p.110, setembro, 1995.

SUDRÉ, Gilberto. Minicurso de Redes Locais sem Fio. UNITERA Tecnologia, 2006. Disponível em: http://www.uvv.br/diversos/encasoft/Redes%20sem%20Fio%20-%20Minicurso%20Encasoft%202006.pdf . Acessado em: 29/09/2007.

MONTEBELLER, S. J. Estudo sobre o emprego de dispositivos sem fio – *wireless* na automação do ar condicionado e de outros sistemas prediais. 2006. 129 f. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo (EPUSP), 2006.

Overview Sensinet. Disponível em: http://www.sensicast.com/products.php. Acessado em 30/10/2007.

ProSoft Technology, White Paper: Wireless Security On The Plant Floor, 2005. Disponível em: http://www.pharmaceuticalonline.com/downloads/detail.aspx?docid=478fcad0-041d-4655-9912-4436451aacaa&VNETCOOKIE=NO. Acessado em 20/09/2007.

REIS, Hermevaldo Pereira. Estudo de redes LAN *wireless* em ambiente de laboratório. São Paulo, 2003. Projeto de Pesquisa de Iniciação Cientifica - Universidade de São Marcos.

SNMPV3: A Security Enhancement for SNMP, William Stallings. Disponível em: http://www.comsoc.org/livepubs/surveys/public/4q98issue/pdf/Stallings.pdf . Acessado em 08/12/2007

TANENBAUM, Andrew S., Redes de Computadores; Tradução Vandenberg B. de Souza. – Rio de Janeiro: Elsevier, 2003.

VIDAL, Fernando Richter. Um Estudo Sobre As Redes Ad Hoc, 2004. Disponível em: http://www.dragon4fun.com.br/down/Art/RedesAdHoc.pdf. Acessado em 29/10/2007.

What is HiperLAN?
Disponível em: http://www.webopedia.com/TERM/H/HiperLAN.html. Acessado em: 29/10/2007.

ZigBee and Wireless Frequency Coexistence | ZigBee White Paper. Disponível em: http://www.zigbee.org. Acessado em 30/11/2007.

ANEXOS

Anexo 1 - Equipamentos *wireless* para indústria

FEATURES

- Two-channel 4-20mA inputs
- Radio amplified up to 5dBm for a robust network
- Supports SensiNet networking protocol at 2.4GHz for ultra-reliable connectivity in harsh RF environments
- Supported by SensiNet® Gateway Software for configuration, management and integration into existing automation systems
- Range of up to 700 ft. (212m) outdoors between Smart Sensor and infrastruture device
- User-definable, remotely-settable transmission intervals
- Supports message acknowledgements and redundant routing, for totally reliable wireless connectivity
- Automatic network joining; no network configuration required
- Wireless firmware upgrade capability
- Status indicator LED
- IP30 Enclosure
- Auto-calibrating to eliminate drift effects

SPECIFICATIONS

Sensor-Related Specifications	
Radio	IEEE 802.15.4 compliant, 2.4 GHz DFSS
Regulatory	FCC Part 15 and CE Approval
Antenna	Internal antenna
Output Power	15 dBm
Range	• Up to 700 ft/212m range (outdoor, line of sight) • Up to 230 ft/70m range (typical indoor conditions)
Operating Temperature	-10°C to 50°C
Operating Humidity	Up to 100% non-condensing
Power Options	• AA 3.6V lithium thionyl chloride battery (included) • +10 to +30 VDC
Battery Life	2 years at two-minute reporting interval
Duty Cycle	Remotely user-adjustable; default to 1 minute
Dimensions	• 3.75" x 5.5" x 1.375" • 96 mm x 140 mm x 35 mm
Packaging	ABS Box – IP30 rated.
Mounting Options	• One or two screws • Double-sided adhesive tape
Analog Input Specifications	
Analog Channels	2 channels
Input Range	4-20mA
Accuracy	0.1%
Resolution	12 bit (0.1%)
Zero Drift	Auto-calibrating
Span Drift	Auto-calibrating
Sensor Terminal Connection	• #28 to 14 AWG wire gauge • Clamping yoke connection

Anexo 1 - Equipamentos *wireless* para indústria (continuação)

FEATURES

- Two contacts per device can be monitiored
- Radio amplified up to 15dBm for a robust network
- Supports SensiNet networking protocol for ultra-reliable connectivity in harsh RF environments
- Supported by the SensiNet Gateway for configuration, management and integration into existing automation systems
- Range of up to 700 ft. (212 meters) outdoors
- User-definable, remotely-settable transmission intervals
- Automatic network joining; no network configuration required
- Wireless firmware upgrade capability
- Status Indicator LED
- IP30 Enclosure

SPECIFICATIONS

Sensor-Related Specifications	
Radio	IEEE 802.15.4 compliant, 2.4 GHz DFSS
Regulatory	FCC Part 15 and CE Approval
Antenna	Internal antenna
Output Power	15 dBm
Range	• Up to 700 ft/212m range (outdoor, line of sight) • Up to 230 ft/70m range (typical indoor conditions)
Operating Temperature	-10°C to 50°C
Operating Humidity	Up to 100% non-condensing
Battery	AA 3.6V lithium thionyl chloride battery
Battery Life	2 years at two-minute reporting interval
Duty Cycle	Remotely user-adjustable; default to 1 minute
LED	Diagnostic LED indicating power/connectivity
Dimensions	• 3.5" x 5.5" x 1.375" • 89 mm x 140 mm x 35 mm
Packaging	ABS Box – IP30 rated.
Mounting Options	• One or two screws • Double-sided adhesive tape
Input Specifications	
Number of Circuits	2 channels
Supported Switches	Use with any STSP electrical contact switch, magnetic, mechanical relay, photocell, IR etc.
Frequency of Detected State Change	1/10 second
Switch Cable Distance	10 meters (switch to sensor)
Sensor Terminal Connection	• #28 to 14 AWG wire gauge • Clamping yoke connection

Anexo 2 - Definições

ARP

Address Resolution Protocol. Criado para resolver o problema do mapeamento de endereços lógicos em endereços físicos quando do uso de IP sobre redes Ethernet, mas não restrito a apenas estes dois protocolos.

DHCP

Dynamic Host Configuration Protocol. É um protocolo para atribuição dinâmica de endereços IP, contidos numa lista pré-definida, para nós (dispositivos) em uma rede. Ao efetuar o *log on*, os nós (dispositivos) da rede automaticamente recebem um endereço IP de uma lista de endereços disponibilizadas pelo DHCP. O servidor de DHCP atribui um endereço IP para um cliente para um período específico de tempo. O cliente solicitará uma renovação da atribuição automaticamente quando a mesma estiver preste a expirar. Se uma renovação não é solicitada e expira, o endereço é devolvido à lista de endereços IP disponíveis. DHCP é utilizado para administrar endereços IP, simplificar configuração do cliente e utilizar com eficiência os endereços IP.

DSSS

O DSSS (*Direct Sequence Spread Spectrum*), espectro de dispersão de seqüência direta, também é restrito a 1 ou 2 Mbps. Cada bit é transmitido como 11 chips, usando o que se denomina seqüência de Barker. Ele utiliza modulação por deslocamento de fase a 1 Mbaud, transmitindo 1 bit por baud quando opera a 1 Mbps e 2 bits por baud quando opera a 2 Mbps. (Tanembaum, 2003).

EAP

Extensible Authentication Protocol. Um protocolo que provê um *framework* de autenticação para redes corporativas com ou sem fio. É tipicamente usado com um servidor de RADIUS para autenticação dos usuários em grandes redes.

FHSS

O FHSS (*Frequency Hopping Spread Spectrum*), espectro de dispersão de saltos de freqüência), utiliza 79 canais, cada um com 1 MHz de largura, começando na extremidade baixa da banda ISM de 2,4 GHz. Um gerador de números pseudo-aleatórios é usado para produzir a seqüência de freqüências dos saltos. Desde que todas as estações utilizem a mesma semente para o gerador de números pseudo-aleatórios e permaneçam sincronizadas, elas saltarão para as mesmas freqüências simultaneamente. O período de tempo gasto em cada freqüência, o tempo de parada, é um parâmetro ajustável, mas deve ser menor que 400 ms. A randomização do FHSS fornece um modo razoável de alocar espectro na banda ISM não regulamentada. Ela também fornece alguma segurança, pois um intruso que não conhecer a seqüência de saltos ou o tempo de parada não poderá espionar as transmissões. Em distâncias mais longas, o esmaecimento de vários caminhos pode ser um problema, e o FHSS oferece boa resistência a ele. O FHSS também é relativamente insensível à interferência de rádio, o que o torna popular para enlaces entre edifícios. Sua principal desvantagem é a baixa largura de banda. (Tanembaum, 2003).

Framework

Estrutura de suporte. É um conjunto de classes com objetivo de reutilização de um *design*, provendo um guia para uma solução de arquitetura em um domínio específico de *software*. São projetados com a intenção de facilitar o desenvolvimento de *softwares*.

LEAP

Lightweight Extensible Authentication Protocol. Protocolo proprietário da Cisco utilizado para autenticação 802.1X em WLANs.

MAC address

Media Access Control address. Numeração única do hardware que identifica cada dispositivo em uma rede. Um dispositivo pode ser qualquer sistema computacional.

Modelo OSI

O Modelo OSI (Open Systems Interconnection) foi estabelecido para possibilitar a integração/interconexão de sistemas abertos à comunicação com outros sistemas. O modelo

possui sete camadas, conforme figura abaixo, que possuem funcionalidades bem definidas e que foi criado como referência para “padronização” de arquiteturas de rede.

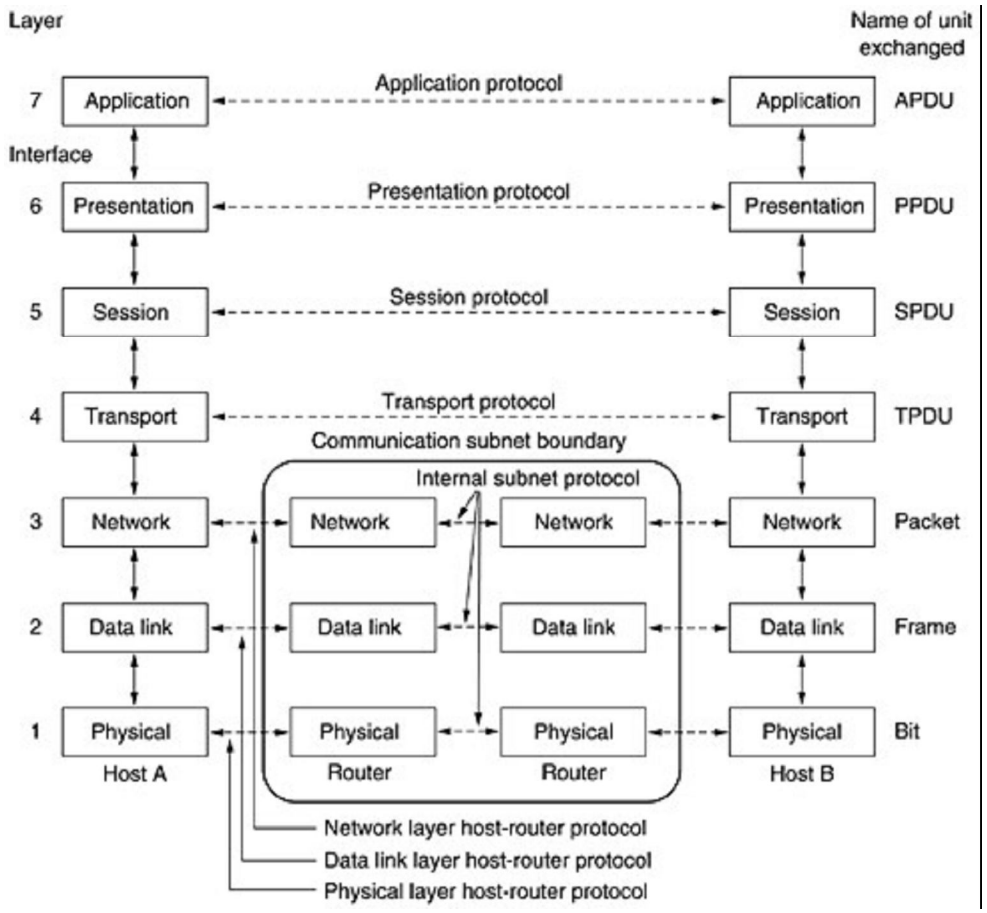

Figura 21: Modelo de referência OSI
Fonte: Tanembaum, 2003.

SNMP

Simple Network Management Protocol - Protocolo de Gerência Simples de Rede é um protocolo de gerência típica de redes TCP/IP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede, como placas e *switches*. O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver seus eventuais problemas, e fornecer informações para o planejamento de sua expansão, dentre outras.

SSID

Service Set Identifier. Nome específico, ou identificador, de rede de 32 caracteres, que diferencia uma LAN sem fios de outra. Todos os pontos de acesso e clientes que tentam conectar a uma WLAN específica têm que usar o mesmo SSID. O SSID pode ser qualquer entrada alfanumérica de até no máximo de 32 caracteres

VPN

Virtual Private Network. Um esquema de criptografia da camada de rede que possibilita conexão segura a redes corporativas utilizando a internet em acessos remotos. Atualmente a maioria das corporações utiliza a VPN para proteger os usuários remotos nas suas conexões a rede corporativa. Opera criando um "túnel" virtual seguro do computador do usuário até o *access point* ou *gateway*, por meio da Internet, conectando a todos os servidores corporativos e aos sistemas. Também pode ser utilizado na proteção de redes sem fio.

WAP

Wireless Applications Protocol. Protocolo projetado disponibilizar aplicativos para dispositivos móveis.

802.1X

Um padrão para autenticação, inicialmente utilizada em redes cabeadas, que foi adaptada para o uso em *WLANs* corporativas para endereçar falhas de segurança do WEP que é a especificação original de segurança do padrão 802.11. O 802.1X provê um *framework* para autenticação dos usuários e controle de acesso a uma rede protegida e chaves de criptografia dinâmica para proteger privacidade de dados.