ANTONIO D'ACOSTA RIVERA

REDES DE EQUIPAMENTOS SEM FIO DE USO PESSOAL:
COMPARAÇÃO DE TECNOLOGIAS EMERGENTES E ANÁLISE DE
TENDÊNCIAS

São Paulo

2010

ANTONIO D'ACOSTA RIVERA

REDES DE EQUIPAMENTOS SEM FIO DE USO PESSOAL:
COMPARAÇÃO DE TECNOLOGIAS EMERGENTES E ANÁLISE DE
TENDÊNCIAS

Dissertação para obtenção do título de
Mestre em Engenharia

Área de Concentração: Sistemas Eletrônicos

Orientador: Prof. Dr. Wagner Luiz Zucchi

São Paulo

2010

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, de outubro de 2010.

Assinatura do autor _____

Assinatura do orientador _____

FICHA CATALOGRÁFICA

Rivera, Antonio D Acosta

**Redes de equipamentos sem fio de uso pessoal: compara -
ção de tecnologias emergentes e análise de tendências / A.D.
Rivera. -- ed.rev. --São Paulo, 2010.
149 p.**

**Dissertação (Mestrado) - Escola Politécnica da Universidade
de São Paulo. Departamento de Engenharia de Sistemas Eletrô-
nicos.**

**1. Redes locais de computadores 2. Wireless 3. Computação
móvel 4. Computador portátil I. Universidade de São Paulo.
Escola Politécnica. Departamento de Engenharia de Sistemas
Eletrônicos II. t.**

Dedico este trabalho a minha esposa Cristina e meus filhos Vanessa, Ricardo e Renata, pois eles são a minha constante inspiração.

AGRADECIMENTOS

À minha Esposa Cristina e filhos Vanessa, Ricardo e Renata pelo apóio e compreensão que me proporcionaram durante o desenvolvimento deste trabalho.

Ao meu orientador, e grande amigo Professor Dr. Wagner Luiz Zucchi pela dedicação e suporte que sempre me proporcionou.

À Professora Dra. Liria Matsumoto Sato e ao Professor Dr. Marcelo Knörich Zuffo pelo apoio que sempre me deram.

À Professora Dra. Íris Gardino pelo seu suporte e dedicação em todos os meus trabalhos.

À Professora Elizabeth Araujo Zucchi pela paciência e suporte na revisão deste trabalho.

RESUMO

No mundo globalizado em que vivemos os sistemas, as aplicações e as pessoas precisam estar conectadas permanentemente à Internet, e a uma variedade de redes de comunicação, com vários dispositivos, simultaneamente. O ideal, devido a esse contexto, seria ter um único dispositivo com uma única interface de rede e um único programa que permitisse fazer diversas conexões com diversos protocolos usados simultaneamente, tornando o sistema simples de usar e fácil de instalar e operar, conseguindo, desta forma, o nível de estabilidade e confiabilidade desejadas. Por isso, as redes de área pessoal (WPAN) estão crescendo em importância desde seu aparecimento em 1991. Diversas tecnologias foram propostas para sua implementação sem que haja um consenso sobre a aplicabilidade de cada opção. Este trabalho realiza uma avaliação crítica das diversas tecnologias propostas e por meio de um laboratório de prototipação procurou obter dados que permitam uma avaliação mais objetiva dessas tecnologias. Esse documento apresenta uma descrição desse laboratório e apresenta a metodologia proposta para comparação das tecnologias para WPAN., e os resultados obtidos em laboratório. O estudo apresentado, demonstra, através de uma avaliação crítica, que as principais alternativas no momento são Wi-Fi e Bluetooth e que com os dados obtidos na prototipação em laboratório se provou que hoje há possibilidade de virtualizar diferentes redes e tipos de interface em uma única interface física. A economia de escala, multiplicada pelo efeito da virtualização das interfaces, leva a conclusão que as tecnologias Wi-Fi e Bluetooth deverão dominar o mercado de WLAN e WPAN nos próximos anos.

Palavras chaves: Redes sem fio; Virtualização de interfaces; Análise de desempenho.

ABSTRACT

In today's globalized world, systems, applications and people need to be permanently connected to the internet, a variety of communications networks and several different devices simultaneously.

Ideally, faced with this context, there should be a single device with a single network interface, and a single program that enables several connections and protocols to be used simultaneously, making the entire systems simple to use and easy to install and operate, thus leading to the desired levels of stability and reliability.

So the personal area networks (WPAN) are growing in importance since its debut in 1991.

Several technologies have been proposed for its implementation without a consensus on the applicability of each option

The proposed work will conduct a critical evaluation of the various proposed technologies and, through a laboratory prototype seek information to enable a more objective evaluation of these technologies.

This document provides a description of the laboratory and presents the proposed methodology to compare technology for WPAN.

Keywords: Wireless LAN, Interface virtualization, Performance Analysis.

LISTA DE ILUSTRAÇÕES

Figura 1 – Válvula.....	29
Figura 2 – Transistor.....	30
Figura 3 - Transistor de 65nm.....	30
Figura 4 - Blusa com Equipamentos.....	33
Figura 5 - Conjunto Básico de Serviços.....	37
Figura 6 – Conjunto de Serviços Estendidos.....	38
Figura 7 - Conjunto Básico de Serviços Independentes	39
Figura 8 – Pacote 802.11 Formato Geral.....	42
Figura 9 – Pacote 802.11 Formato de Dados.....	43
Figura 10 – Pacote 802.11 Pedido Para Transmitir RTS.....	43
Figura 11 – Pacote 802.11 Livre Para Transmitir CTS.....	44
Figura 12 – Pacote 802.11 Confirmação ACK.....	44
Figura 13 - Sistema com várias antenas MIMO-OFDM	48
Figura 14 - Canais no padrão 802.11b.....	49
Figura 15 - Canais no padrão 802.11a.....	51
Figura 16 – Quadro HiperLAN/2 Formato Geral.....	54
Figura 17 – Quadro HiperLAN/2 Tamanho Variavel.....	54
Figura 18 – Logotipo do Bluetooth.....	61
Figura 19 - My Wi-Fi – Placa de Rede + Programas (driver)	88
Figura 20 - Arquitetura do My Wi-Fi.....	90

LISTA DE GRÁFICOS

Gráfico 1 – Equipamentos eletrônicos em casas de jovens com idade de 1 a 18 anos.....	22
Gráfico 2 – Evolução do número de transistores no processadores.....	31
Gráfico 3 – Comparativo WPAN e a WLAN.....	99
Gráfico 4 - Comparativo WPAN e WLAN com tráfego constante	100

LISTA DE TABELAS

Tabela 1 – Esquemas de Segurança padrão 802.11.....	46
Tabela 2 - Canais e Frequências utilizadas no 802.11 b e 802.11 g.....	49
Tabela 3 - Canais e Frequências utilizadas no 802.11 a.....	50
Tabela 4 - Canais e Frequências utilizadas no 802.11 n.....	51
Tabela 5 – Resumo das Tecnologias Pesquisadas.....	84
Tabela 6 - Cópia disco- a- disco dentro do mesmo Notebook.....	95
Tabela 7 - Cópia de arquivos usando-se a WLAN.....	96
Tabela 8 - Cópia de arquivos usando-se a WPAN.....	97
Tabela 9 - Cópia de arquivos usando-se a WPAN com tráfego na WLAN.....	98

LISTA DE ABREVIATURAS E SIGLAS

3G	<i>Third Generation Mobile</i> – Mobilidade de Terceira Geração.
ACK	<i>Acknowledgement</i> – Confirmação.
ACL	<i>Access Control List</i> – Lista de Controle de Acesso.
ACL	<i>Asynchronous Connectionless Link</i> – Ligação Sem Conexão Assíncrona.
ACS	<i>Access Control Server</i> – Servidor de Controle de Acesso.
AD HOC	<i>Ad hoc</i> – do latim para um fim específico. Em redes é uma conexão ponto a ponto sem definição de hierárquica.
ADSL	<i>Asymmetric Digital Subscriber Line</i> – Linha de Assinante Digital Assimétrica.
AES	<i>Advanced Encryption Standard</i> – Padrão de Criptografia Avançado.
AID	<i>Association Identifier</i> – Identificador de Associação.
AM	<i>Amplitude Modulation</i> – Modulação em Amplitude.
AMA	<i>Active Member Address</i> - Endereço de Membro Ativo.
AM_ADDR	<i>Active Member Address</i> – Endereço de Membro Ativo.
AMP	<i>Alternate MAC / PHY</i> – MAC / PHY Alternativo.
ANSI	<i>American National Standard Institute</i> – Instituto Nacional Americano de Padrões.
AP	<i>Access Point</i> – Ponto de Acesso.
APC	<i>Access Point Controller</i> – Controlador de Ponto Acesso.
API	<i>Application Program Interface</i> – Interface para Programas de Aplicação.
APL	<i>Application Layer</i> – Camada da Aplicação.
AP MIB	<i>Access Port Management Information Base</i> - Porta de Acesso a Base de Informações de Gerenciamento.
APS	<i>Application Support Layer</i> – Camada de Suporte a Aplicação.
AR_ADDR	<i>Access Request Member Address</i> – Endereço do Requerimento de Acesso do Membro.
ARIB	<i>Association of Radio Industries and Broadcasting</i> – Associação das Indústrias de Radio e Radiodifusão.
ASK	<i>Amplitude Shift Keying</i> – Modulação por Chaveamento de Amplitude.
ATM	<i>Asynchronous Transfer Mode</i> – Transferência em Modo Assíncrono.

AVCTP	<i>Audio/Visual Control Transport Protocol</i> – Protocolo de Transporte para Controle de Áudio e Vídeo.
AVDTP	<i>Audio/Visual Data Transport Protocol</i> – Protocolo de Transporte de Dados de Áudio e Vídeo.
BD_ADDR	<i>Bluetooth Device Address</i> – Endereço do Dispositivo Bluetooth.
BER	<i>Bit Error Rate</i> – Taxa de Erro nos Bits.
BNEP	<i>Bluetooth Network Encapsulation Protocol</i> – Protocolo de Encapsulamento Bluetooth para Rede.
BPSK	<i>Binary Phase Shift Keying</i> – Modulação por Chaveamento de Fase Binário.
BRAN	<i>Broadband Radio Access Network</i> – Rede de Acesso ao Rádio de Banda Larga.
BREW	<i>Binary Runtime Environment for Wireless</i> – Ambiente para Execução Binária para Redes sem Fio.
BSIG	<i>Bluetooth Special Interest Group</i> – Grupo de Interesse Especial em Bluetooth.
BS	<i>Base Station</i> – Estação Base (Ponto de Acesso).
BSS	<i>Basic Service Set</i> – Conjunto de Serviços Básicos.
BT	<i>Bandwidth Time</i> – Tempo da Largura de Banda.
CA	<i>Collision Avoidance</i> – Tentativa de Evitar as Colisões.
CC	<i>Central Controller</i> – Controlador Central.
CCA	<i>Clear Channel Assignment</i> – Assinalamento de Canal Limpo.
CCK	<i>Complementary Code Keying</i> – Código Complementar por Chaveamento.
CCMP	<i>Counter Mode with Cipher Block Chaining Message Authentication Code Protocol</i> - Protocolo de Autenticação em Modalidade Contador com Mensagens Encadeadas.
CDMA	<i>Code Division Multiple Access</i> – Acessos Múltiplos por Divisão de Código.
CE	<i>Consumer Electronics</i> - Produtos Eletrônicos de Consumo.
CL	<i>Convergence Layer</i> – Camada de Convergência.
CM	<i>Centralized Mode</i> – Modo Centralizado.
CRC	<i>Cyclic Redundancy Codes</i> – Código de Redundância Cíclico.
CSLL	<i>Carrie Small Live Large</i> – Pequeno de Carregar para Viver Grande.
CSMA	<i>Carrier Sense Multiple Access</i> – Acessos Múltiplos Percebendo o Sinal da Portadora.

CSMA/CA	<i>Carrier Sense Multiple Access with Collision Avoidance</i> - Acessos Múltiplos Percebendo o Sinal da Portadora Evitando as Colisões.
CSMA/CD	<i>Carrier Sense Multiple Access with Collision Detection</i> - Acessos Múltiplos Percebendo o Sinal da Portadora Detectando as Colisões.
CTS	<i>Clear To Send</i> – Livre Para Transmissão.
DA	<i>Destination Address</i> – Endereço de Destino.
DCF	<i>Distributed Coordination Function</i> – Função de C ordenação Distribuída.
DES	<i>Data Encryption Standard</i> – Padrão para Criptografia de Dados.
DFS	<i>Dynamic Frequency Seletion</i> - Seleção Dinâmica de Frequência.
DIFS	<i>Distributed Inter Frame Space</i> - Espaço Entre Quadros Distribuído.
DLC	<i>Data Link Control</i> – Controle do Enlace de Dados.
DM	<i>Direct Mode</i> – Modalidade Direta.
DQPSK	<i>Differential Quadrature Phase Shift Keying</i> – Modulação por Chaveamento de Fase por Quadratura Diferencial.
DS	<i>Distribution System</i> – Sistema de Distribuição (Backbone).
DSSS	<i>Direct Sequence Spread Spectrum</i> - Espalhamento Espectral de Sequência Direta.
DVD	<i>Digital Video Disc ou Digital Versatile Disc</i> - Disco Digital de Vídeo ou Disco Digital Versátil.
EC	<i>Error Control</i> – Controle de Erro.
EMS	<i>Enhanced Messaging Services</i> – Serviços de Mensagens Aprimorado.
ESS	<i>Extended Service Set</i> – Conjunto de Serviços Estendido.
ETSI	<i>European Telecommunications Standardisation Institute</i> – Instituto Europeu de Padronização das Telecomunicações.
EWC	<i>Enhanced Wireless Consortium</i> – Consórcio para Melhorar as Redes sem Fio.
FCC	<i>Federal Communication Commission</i> – Comissão Federal de Comunicações.
FDD	<i>Frequency Division Duplex</i> - Compartilhamento Duplo por Divisão de Frequência.
FDMA	<i>Frequency Division Multiple Access</i> – Acessos Múltiplos por Divisão de Frequência.
FFD	<i>Full Function Device</i> – Dispositivo com Função Completa.
FH	<i>Frequency Hopping</i> - Salto de Frequências.
FHSS	<i>Frequency Hopping Spread Spectrum</i> - Espalhamento Espectral por Salto de Frequências.

FIR	<i>Fast-Speed Infrared Mode</i> – Infravermelho com Modalidade de Alta Velocidade.
FM	<i>Frequency Modulation</i> – Modulação em Frequência.
FSK	<i>Frequency Shift Keying</i> – Modulação por Chaveamento de Frequência.
GFSK	<i>Gaussian Frequency Shift Keying</i> – Modulação por Chaveamento de Frequência com o Algoritmo Gaussian.
GHz	<i>Giga Hertz</i> – Giga Hertz.
GPRS	<i>General Packet Radio Service</i> – Serviço Geral de Pacotes por Rádio.
GPS	<i>Global Positioning System</i> – Sistema Global de Posicionamento (localização).
GSM	<i>Global System for Mobiles</i> – Sistema Global para Mobilidade.
H2GF	<i>HiperLAN/2 Global Forum</i> – Forum Global para HiperLAN/2.
HA	<i>Home Appliance</i> – Aparelhos Domésticos.
HCI	<i>Host Controller Interface</i> – Interface Controladora de Dispositivos.
HID	<i>Human Interface Device Applications</i> – Aplicações para Dispositivos para Interface Humana.
HiperLAN/2	<i>High Performance Radio Local Area Network</i> – Rede Local com Rádio de Alto Desempenho.
HomeRF	<i>Wireless Home Networking</i> – Rede Sem Fio para Casas em Rádio Frequência
IAS	<i>Information Access Service</i> – Serviço de Acesso à Informação.
IBSS	<i>Independent Basic Service Set</i> – Conjunto Básico de Serviços Independentes.
IEEE	<i>Institute of Electrical and Electronics Engineers, Inc</i> – Instituto dos Engenheiros Elétricos e Eletrônicos.
IEEE 802	<i>LMSC – LAN/MAN Standards Committee</i> - Comitê de Padronização para Redes de Área Local e Redes de Área Metropolitana.
IEEE 802.11	<i>(WiFi) Wlan Wireless LAN technology including Wi-Fi</i> - Tecnologia de Rede Local Sem Fio incluindo Wi-Fi.
IEEE 802.15	<i>Wpan Wireless Personal Area Networking (WPAN) technology</i> - Tecnologia de Rede de Equipamentos Sem Fio para uso Pessoal.
IEEE 802.16	<i>WiMax WMan Wireless Metropolitan Area Networking (WMAN) and WiMAX technology</i> – Tecnologia de Rede Sem Fio Para Área Metropolitana e Wimax.
IEEE 802.16	<i>ETSI HiperMAN standard</i> - Padrão para redes Hiper Metropolitanas.

IEEE PASC	<i>Institute of Electrical and Electronics Engineers, inc - Portable Applications Standards Committee</i> – Instituto dos Engenheiros Elétricos e Eletrônicos - Comitê de Aplicações Portáteis Padrão.
IEC	<i>International Electrotechnical Commission</i> – Comissão Internacional dos Eletrotécnicos.
IETF	<i>Internet Engineering Task Force</i> – Força Tarefa dos Engenheiros da Internet.
iMode	<i>Mobile Internet Technology</i> – Tecnologia Internet para Mobilidade.
IP	<i>Internet Protocol</i> - Protocolo da Internet.
IPOS	<i>Initial Public Offerings</i> - Oferecimento Público Inicial.
IR	<i>InfraRed</i> – Infravermelho.
IrCOMM	<i>InfraRed Communications Protocol</i> – Protocolo de Comunicações.
IrDA	<i>InfraRed Data Association</i> – Associação para Padronização da Transmissão Dados por luz Infravermelho.
IrLAN	<i>InfraRed LAN Access Protocol</i> – Protocolo de Acesso as Rede Locais.
IrLAP	<i>Infrared Link Access Protocol</i> – Protocolo de Acesso ao Enlace Infravermelho.
IrLMP	<i>InfraRed Link Management Protocol</i> – Protocolo de Gerenciamento do Enlace.
IrOBEX	<i>InfraRed Object Exchange Protocol</i> – Protocolo para Troca de Objetos.
ISM	<i>Industrial, Scientific and Medical</i> - designação genérica das faixas de frequências destinadas ao uso nas indústriais, na área científica e na área médica.
ISO	<i>International Standard Organization</i> – Organização Internacional de Padrões.
L2CAP	<i>Logical Link Control and Adaptation Protocol</i> – Controle Lógico do Enlace e Protocolo de Adaptação.
LAN	<i>Local Area Network, Local means Campus</i> – Rede de Área Local onde Local se refere a um Campus.
LBS	<i>Location Based Services</i> – Serviços Baseados na Localização.
LEB	<i>Location-Enabled Business</i> – Localização Pronta para os Negócios.
LED	<i>Light Emitting Diode</i> – Diodo Emissor de Luz.
LLC	<i>Logical Link Control</i> – Controle Lógico do Enlace.
LM-IAS	<i>Link Management Information Access Services</i> – Gerenciador das Informações de Acesso a Serviços Disponíveis no Enlace.
LM-Mux	<i>Link Management Multiplexer</i> – Gerenciador Multiplexador de Enlaces.

LMSC	<i>LAN & MAN Standards Committee</i> – Comitê de Padronização LAN e MAN.
LMP	<i>Link Management Protocol</i> – Protocolo de Gerenciamento de Enlace.
LOS	<i>Line Of Sight</i> – Linha de Visão.
MAC	<i>Medium Access Control</i> – Controle de Acesso ao Meio.
MAN	<i>Metropolitan Area Network, Metropolitan means Intra City</i> – Rede de Área Metropolitana onde Metropolitana é Dentro da Cidade.
MIMO	<i>Multiple-Input Multiple-Output</i> - Múltiplas Entradas e Múltiplas Saídas onde se tem múltiplas antenas de entrada e múltiplas antenas de saída.
MMS	<i>Multimedia Messaging Services</i> – Serviços de Mensagem de Multimeios.
MT	<i>Mobile Terminals</i> – Terminais Móveis.
NAV	<i>Network Allocation Vector</i> – Vetor de Alocação de Rede.
NLOS	<i>Non in Line Of Sight</i> – Sem Linha de Visada (sem visão direta).
NWK	<i>Network Layer</i> – Camada de Rede.
OBEX	<i>Object Exchange Protocol</i> – Protocolo de Troca de Objetos.
OFDM	<i>Orthogonal Frequency Division Multiplexing</i> - Multiplexação por Divisão de Frequência Ortogonal.
OQPSK	<i>Offset Quadrature Phase-Shift Keying</i> - Modulação por Chaveamento de Fase por Quadratura com Deslocamento.
OSI	<i>Open Standard Interconnection</i> – Padrões Abertos para Interconexão.
PAN	<i>Personal Area Network, Personal means 10 meters</i> – Rede de Área Pessoal onde Pessoal são 10 metros.
PAR	<i>Project Authorization Request</i> – Requerimento de Autorização de Projeto.
PASC	<i>Portable Applications Standards Committee</i> – Comitê de Aplicações Portáteis Standard.
PCF	<i>Point Coordination Function</i> – Ponto de Função de Coordenação.
PD	<i>Photodetector</i> – Detectores de Luz.
PDA	<i>Personal Digital Assistants</i> - Assistente Digital Pessoal.
PDMA	<i>Packet Division Multiple Access</i> – Acessos Múltiplos por Divisão de Pacotes.
PHY	<i>Physical Layer</i> – Camada Física.
Piconet	<i>Pico Net</i> - Pequena Rede.
PIN	<i>Personal Identification Number</i> – Número de Identificação Pessoal.

PLCP	<i>Physical Layer Convergence Protocol</i> – Protocolo de Convergência da Camada Física.
PMA	<i>Parked Member Address</i> – Endereço de Membro Estacionado.
PMD	<i>Physical Medium Dependent</i> – Dependente do Meio Físico.
POS	<i>Personal Operating Space</i> – Espaço de Operação Pessoal.
PPP	<i>Point to Point Protocol</i> – Protocolo Ponto a Ponto.
PRNG	<i>Pseudo Random Number Generator</i> - Número Gerado por algoritmo Pseudo Randômico.
PSK	<i>Pre-Shared Key</i> – Chaves Previamente Compartilhadas.
PSM	<i>Pulse Sequence Modulation</i> – Modulação por Sequência de Pulsos.
QOS	<i>Quality of Services</i> – Qualidade de Serviços.
QPSK	<i>Quadrature Phase Shift Keying</i> – Modulação por Chaveamento de Fase por Quadratura.
RA	<i>Receiver Address</i> – Endereço de Destino.
Radar	<i>Radio Detection And Ranging</i> – Detecção por Rádio e Visor de Área.
RES10	<i>Radio Equipment and Systems 10</i> – Equipamentos de Rádio e Sistemas 10.
RF	<i>Radio Frequency</i> - Rádio Frequência.
RFCOMM	<i>Cable Replacement Protocol</i> – Protocolo de Substituição de Cabos.
RFD	<i>Reduced Function Device</i> – Dispositivo com Função Reduzida.
RFID	<i>Radio Frequency Identification</i> – Identificação por Rádio Frequência.
RLC	<i>Radio Link Control</i> – Controle do Enlace de Rádio.
RTS	<i>Request To Send</i> – Pedido Para Transmissão.
SA	<i>Source Address</i> – Endereço de Origem.
SAFER	<i>Secure And Fast Encryption Routine</i> – Rotina de Criptografia Segura e Rápida.
SAP	<i>Second Audio Program</i> – Segundo Programa de Áudio.
SAR	<i>Segmentation And Reassembly</i> - Segmentação e Remontagem.
Scatternet	<i>Scatternet “Scatter” Disperse and “Net” Network</i> , que é um sistema disperso composto de várias redes cada uma contendo um número limitado de dispositivos.
SCwng	<i>Next Generation Standing Committe</i> - Comitê para Estudo das Redes Sem Fio da Próxima Geração.
SDP	<i>Service Discovery Protocol</i> – Protocolos de Descobrimento de Serviços.
SFD	<i>Start Frame Delimiter</i> – Delimitador de Início de Quadro.

SG	<i>Study Group</i> – Grupo de Estudo.
SIG	<i>Special Interest Group</i> - Grupo Especial de Interesse.
SIG Bluetooth	<i>Bluetooth Special Interest Group</i> – Grupo Especial de Interesse em Bluetooth.
SIR	<i>Slow-Speed Infrared Mode</i> – Infravermelho em Modalidade de Baixa Velocidade.
SMS	<i>Short Messaging Services</i> - Serviços de Mensagens Curtas.
TA	<i>Transmitter Address</i> – Endereço do Transmissor.
TCP	<i>Transport Control Protocol</i> – Protocolo de Controle do Transporte.
TCS BIN	<i>Telephone Control Protocol</i> – Protocolo de Controle de Telefone.
TDD	<i>Time Division Duplex</i> – Divisão de Tempo Duplo.
TDMA	<i>Time Division Multiple Access</i> – Acessos Múltiplos por Divisão de Tempo.
TG	<i>Task Group</i> – Grupo de Trabalho.
TGnsync	<i>Task Group n Synchronization</i> – Força Tarefa n para Sincronização.
TinyTP	<i>Tiny Transport Protocol</i> – Pequeno Protocolo de Transporte.
TKIP	<i>Temporal Key Integrity Protocol</i> - Protocolo de Integridade com Chaves Temporais.
TPC	<i>Transmit Power Control</i> - Controle da Potência de Transmissão.
TV	<i>Television</i> – Televisão.
TXOP	<i>Transmission Opportunity</i> - Oportunidade para Transmitir.
UART	<i>Universal Asynchronous Receiver/Transmitter</i> – Receptor / Transmissor Assíncrono Universal.
UDP	<i>User Datagram Protocol</i> – Protocolo De Datagrama de Usuário.
UMTS	<i>Universal Mobile Telephony System</i> – Sistema de Telefonia Móvel Universal.
UNII	<i>Unlicensed National Information Infrastructure</i> – Infra Estrutura de Informação Nacional Não Licenciada.
USB	<i>Universal Serial Bus</i> – Barramento Serial Universal.
UUID	<i>Universally Unique Identifier</i> – Identificador Universal Único.
UWB	<i>Ultra Wide Band</i> – Banda Ultra Larga.
VCS	<i>Virtual Carrier Sense</i> – Percepção da Portadora Virtual.
VLC	<i>Visible Light Communication</i> – Comunicação com Luz Visível.
VoiceXML	<i>Voice eXtensible Markup Language</i> – Voz por Linguagem de Marcação Extensível.

WAE	<i>Wireless Application Environment</i> – Ambiente de Aplicações de Rede Sem Fio.
WAP	<i>Wireless Application Protocol</i> – Protocolo para Aplicações de Redes Sem Fio.
WECA	<i>The Wireless Ethernet Compatibility Alliance</i> – Aliança para Compatibilidade das Redes sem Fio Ethernet. Também conhecida por Wi-Fi Alliance.
WEP	<i>Wired Equivalent Privacy</i> – Privacidade Equivalente a Rede com Fio.
WIMAX	<i>Worldwide Interoperability for Microwave Access</i> - Interoperabilidade Mundial para Acesso por Microondas.
Wi-Fi	<i>Wireless Fidelity</i> – Fidelidade em Rede Sem Fio. Do termo <i>Hi-Fi - High Fidelity</i> – Alta Fidelidade que por se tratar de redes sem fio foi adaptado para Wi-Fi.
WG	<i>Working Group</i> – Grupo de Trabalho.
WLAN	<i>Wireless Local Area Network, Local means Campus</i> – Rede Sem Fio de Área Local onde Local é Campus.
WLL	<i>Wireless Local Loop</i> – Laço Local para Rede sem Fio.
WPA	<i>Wi-Fi Protected Access</i> – Wi-Fi Com Acesso Protegido.
WPAN	<i>Wireless Personal Area Network, personal means 10 meters</i> – Rede Sem Fio de Área Pessoal onde Pessoal são 10 metros.
WWiSE	<i>World-Wide Spectrum Efficiency</i> – Eficiência no Uso do Espectro Mundial.

SUMÁRIO

1 INTRODUÇÃO	21
1.1 Apresentação do Tema	23
1.2 Objetivos.....	23
1.3 Justificativas.....	24
1.4 Organização da Dissertação	24
1.5 Metodologia.....	25
2 REDES SEM FIO	26
2.1 Início do Rádio e da TV.....	27
2.2 Histórico das WPANs - - Wireless Personal Area Network.	31
2.3 O que são as WPAN – Wireless Personal Area Network.	32
2.4 IEEE 802.11 Wireless Local Area Networks Wi-Fi.....	35
2.4.1 Arquitetura das redes 802.11 – Wi-Fi.	37
2.5.1 Arquitetura do HiperLAN/2.....	53
2.5.2 Outros Serviços do HiperLAN2.....	55
2.6 Tecnologias de rede sem fio usando a luz infravermelha – InfraRed.....	55
2.6.1 Arquitetura do Infravermelho.....	56
2.6.2 IrDA – Control.....	57
2.6.3 IrDA – Data	58
2.6.4 Segurança no Infravermelho.....	60
2.7 Tecnologias de rede sem fio Bluetooth.....	60
2.7.1 Arquitetura do Bluetooth.	62
2.7.2 Segurança no Bluetooth.	64
2.8 - Tecnologias de rede sem fio Zigbee.....	65
2.8.1 Arquitetura do ZigBee.	65
2.8.2 Segurança no ZigBee.	67
2.9 Tecnologias de rede sem fio IEEE 802.15 Working Group for Wireless Personal Area Networks.....	68
2.9.1 802.15.1 Personal Area Network Bluetooth v1.1	68
2.9.2 802.15.2 Coexistence Task Group	69
2.9.3 802.15.3 High Rate Task Group.....	69
2.9.4 802.15.4 Low Data Rate with Battery Life and Very Low Complexity – Zigbee.....	69
2.9.5 802.15.5 Enable Mesh Networking	69
2.9.6 802.15.6 BAN Body Area Networks.....	70
2.9.7 802.15.7 Visible Light Communication Task Group.....	70
2.9.8 Outros Grupos do 802.15.	70
3 DEFINIÇÃO DE CRITÉRIOS DE COMPARAÇÃO	71
3.1 IEEE 802.11 – Wireless Local Area Networks.....	74
3.2 HiperLAN/2.....	76
3.3 Infra vermelho – Infra Red	78
3.4 Bluetooth.....	79
3.5 ZigBee.....	81
3.6 Análise dos dados da Tabela	85
3.7 Conclusão do Estudo Comparativo.....	85
4 DESCRIÇÃO DOS TESTES E RESULTADOS EXPERIMENTAIS.	87
4.1 A interface 802.11 My WiFi.....	88
4.2 Equipamentos e Programas usados durante os testes.....	91
4.3 Descrição do teste	92
4.4 Descrição Geral dos Testes	92

4.5	<i>Observações sobre o ambiente de Testes.....</i>	92
4.5.1	<i>Testes de Compatibilidade e Aderência.....</i>	93
4.5.2	<i>Testes de Desempenho.....</i>	93
5	RESULTADOS DOS TESTES	95
5.1	<i>Comparativos dos Resultados dos Testes de Desempenho.....</i>	98
6	CONCLUSÃO.....	102
	REFERÊNCIAS	104
	APÊNDICES.....	109
	APENDICE A - Estrutura do Grupo IEEE 802.11.	109

1 INTRODUÇÃO

O ser humano, para poder viver, conviver e sobreviver, precisa, pela sua natureza, estar em permanente contato com outras pessoas e com o meio ambiente no qual ele vive e para poder atender a todas as suas necessidades vitais ou não, tem que estar em constante movimento.

Para poder efetuar trocas com as outras pessoas e com o meio ambiente, muitas vezes ele, por si só, não basta e, por isso, precisa usar alguns meios, métodos, utensílios ou ferramentas. Alguns deles são tão usados no seu dia a dia que ele os carregar consigo, e os utiliza, incorporando-os no seu cotidiano e eles chegam a formar uma extensão do seu próprio corpo, tornando-se, desta forma, uma espécie de “kit” de sobrevivência. Porém, nem sempre consegue carregar todas essas ferramentas nem mantê-las o tempo todo ao seu alcance, mas as utiliza quando necessário. Pode-se dizer que esse “kit” de sobrevivência é sua rede pessoal (conjunto de meios, métodos, informações, utensílios e ferramentas que são interligados entre si, logicamente por pertencerem e serem usados sempre pela mesma pessoa no seu dia a dia) de objetos que o ajudam..

As pessoas vivem num mundo globalizado, digital de permanente comunicação, onde é fundamental estar sempre conectado, independentemente do momento e lugar em que se esteja. Para termos uma idéia até o fim de 2008 segundo a UTI (União Internacional de Telecomunicações), já havia 4 bilhões de celulares no mundo, o que representava 61% por cento da população mundial [1].

Para poder sobreviver, as pessoas precisam não só de celular, mas de diversos dispositivos eletrônicos, motivo pelo qual a rede pessoal de objetos hoje incorpora vários desses dispositivos, alguns móveis e outros fixos que se comunicam entre si sem a necessidade de fios.

Segundo a 11.^a pesquisa de mercado realizada pela CEA (*Consumer Eletronics Association*) [2] em maio de 2009, nas casas em que havia jovens com idade de 1 a 18 anos, nos EUA, foram gastos 59 bilhões de dólares em equipamentos eletrônicos em 2008 e, como podemos observar no gráfico 1 e em 96% delas havia um aparelho que tocava DVD, 96% tinham celulares, 89% tinham câmeras digitais, 78% tinham um computador de mesa, 76% modem de banda larga, 72% um console de vídeo game, 68% um MP3 player, 68% uma impressora

multifuncional, 66% uma filmadora camcorder, 59% uma TV HD, 59% um laptop, 58% de unidade de disco externo, e 57% uma rede sem fio.

Gráfico 1 – Equipamentos eletrônicos em casas de jovens com idade de 1 a 18 anos

A esse conjunto de dispositivos eletrônicos que se comunicam sem fio, de uso particular, que hoje o homem utiliza para a sua sobrevivência, dá-se o nome de Rede de Equipamentos sem Fio de uso Pessoal - WPAN- *Wireless Personal Area Network*.

As redes pessoais podem ser conectadas a outras redes de maior alcance (locais, metropolitanas ou globais) com fios ou sem fios, para aumentar a sua abrangência e alcance. Isso permite que hoje, por exemplo, seja possível trocar idéias e trabalho com uma pessoa que está do outro lado do mundo como se as duas estivessem face a face, ou usar um dispositivo (uma impressora, por exemplo) que esteja também do outro lado do mundo como se estivesse ao lado. Hoje isso já é uma realidade não só nas regiões mais desenvolvidas onde 58% das pessoas já usam e dependem da Internet como também em regiões em desenvolvimento como na América Latina e Caribe, nessas, esse número já chega a 18,7% segundo pesquisa das Nações Unidas de 2008 (*United Nations - The Millenium Development Goals Report*) [3].

1.1 Apresentação do Tema

Vive-se hoje o grande desafio da sobrevivência em um mundo totalmente globalizado, que impõe a obrigatoriedade da permanente comunicação com o mundo, não importando quem seja nem a cidade ou país onde se esteja no momento, motivo pelo qual a comunicação sem fio pessoal se tornou vital já que estamos em constante movimento.

Desde 1989 quando foi regulamentado o uso das frequências de 900 MHz, 2,4 GHz e 5 GHz na indústria, na ciência e na medicina [4], o mundo todo vem trabalhando no desenvolvimento das redes de equipamentos sem fio de uso pessoal, por isso, hoje há mais de 10 tecnologias diferentes em uso sem que se tenha o estabelecimento de um padrão, o que dificulta de sobremaneira o desenvolvimento, o custo, sua utilização e aceitação por parte do mercado.

Definiu-se como problema para o estudo desta dissertação: a comparação das tecnologias em uso e análise de tendências.

Procura-se com este trabalho suprir o mercado e o mundo acadêmico com um estudo que apresente uma análise dessas tecnologias, do desenvolvimento, e das tendências das redes de equipamentos sem fio de uso pessoal.

1.2 Objetivos

Os objetivos deste trabalho são:

- a) verificar quais são as redes sem fio de uso pessoal que existem à venda atualmente no mercado e quais são as mais usadas;
- b) selecionar, estudar e analisar as cinco mais usadas;
- c) comparar os tipos de redes, suas tecnologias, suas aplicações, sua aceitação, custo e a possibilidade de coexistência delas;
- d) detectar tendências e procurar determinar os padrões do futuro e as novas aplicações.

1.3 Justificativas

Conforme se pode verificar no artigo escrito no dia 10 de janeiro de 2008 por Darren Waters da *BBC News* durante a sua cobertura da CES – *Consumer Electronics Show* em Las Vegas, Estados Unidos da America [5] foram fabricados no ano passado 800 milhões de dispositivos com tecnologia Bluetooth e já existem mais de 350 milhões de dispositivos instalados usando a tecnologia de rede sem fio Wi-Fi que está crescendo a uma velocidade sem precedentes. A aliança Wi-Fi prevê para 2011 a venda de mais de 1.2 bilhões de dispositivos equipados com rede sem fio Wi-Fi em um único ano.

Como comentado, nesse mesmo artigo, cada dia aparecem novas aplicações utilizando a tecnologia de rede de uso pessoal sem fio como, por exemplo, um estetoscópio que capta as batidas do coração do paciente e simultaneamente as envia para o computador pessoal e para os fones de ouvido sem fio do médico.

Como se pode ver claramente, num futuro bem próximo, não haverá uma única pessoa que não esteja usando um dispositivo com tecnologia de rede sem fio de uso pessoal e, por isso, a realização deste estudo deve-se à importância de se ter uma clara visão das tendências tecnológicas para o desenvolvimento dessas redes, contribuindo, dessa forma, para as novas pesquisas e desenvolvimento de trabalhos nesta importante área que, sem sombra de dúvida, fará parte do dia a dia de todas as pessoas.

1.4 Organização da Dissertação

O texto desta tese está organizado em seis seções:

Na primeira seção apresenta-se a introdução, que contém a apresentação do problema, objeto da dissertação, seus objetivos e a metodologia utilizada.

A segunda seção contém um tutorial das tecnologias de rede sem fio de uso pessoal estudadas, destacando-se as características relevantes para comparação.

A terceira seção apresenta a comparação das tecnologias sendo que primeiro é feita a definição formal dos critérios de comparação, e depois é feita a análise comparativa das tecnologias sob esses critérios.

A quarta seção apresenta a experiência prática realizada em laboratório com a relação de testes realizados, os resultados obtidos, feitos de forma a permitir uma análise da tecnologia.

A quinta seção apresenta a análise dos resultados da experiência prática.

A sexta seção é dedicada à conclusão final da dissertação, e a propostas de trabalhos futuros.

Por fim são apresentadas as conclusões finais e tendências futuras para a tecnologia das redes sem fio de uso pessoal WPANs.

1.5 Metodologia.

Através de um estudo de mercado deve-se definir o escopo de estudo da dissertação, selecionando as cinco tecnologias de rede sem fio de uso pessoal mais usadas no mercado. Devem ser estudadas as características destas tecnologias, de modo a aprofundar sua comparação.

Definir quais devem ser os parâmetros e critérios que serão usados na avaliação e comparação.

Comparar as tecnologias através dos parâmetros definidos, construindo uma tabela comparativa, que permita criar uma conclusão sobre os padrões e tendências.

Escolher uma tecnologia para montar um laboratório experimental de uso que permita executar uma análise de desempenho e viabilidade.

Escrever uma conclusão sobre a experiência de uso realizada comentando os resultados.

2 REDES SEM FIO

Sobre este tema pode-se escrever vários livros e centenas de páginas, o que não é o caso, mas para se obter as informações necessárias que permitam o perfeito entendimento deste trabalho, aqui se faz um pequeno resumo da história das comunicações.

O ser humano, para poder sobreviver, sempre teve que se comunicar com os outros e com o meio ambiente, tanto de perto como à distância. Devido às características do meio ambiente, a existência de outros seres humanos, animais e acidentes geográficos, ele tinha que se comunicar muitas vezes em movimento, porque, se ficasse parado, poderia ser atacado, interceptado, ou simplesmente não ser visto ou ouvido por causa de uma montanha ou um rio.

Em outras palavras, a mobilidade, privacidade, segurança e o alcance sempre foram fundamentais para a perfeita comunicação do homem.

No início serviam-se de estafetas, mensageiros, para levar as suas mensagens escritas ou faladas. Na selva e nos lugares mais inóspitos, usava tambores e, para aumentar o seu alcance (distância), às vezes se fazia valer de repetidores.

Em outros lugares onde houvesse mais visibilidade, usou o fogo e a fumaça. Com o auxílio de tapetes e barreiras, criava vários sinais visuais e o desenho das formas requeria alta ciência o que, com o passar do tempo, se tornou uma verdadeira arte.

Com o auxílio do fogo, da luz, de bandeiras, espelhos e materiais refletivos, desenvolveu diversos códigos de comunicação à distância e muitos deles ainda são usados hoje no mar, no campo e nas guerras. Para poder usar esse modelo de transmissão, porém, havia a necessidade de visibilidade, isto é, os sinais precisavam ser vistos.

Esses métodos também eram usados em comunicações sem fio para uso pessoal para curtas distâncias. Os jovens de todo o mundo usam ainda alguns desses meios para se comunicarem secretamente, seja nas escolas, nas suas casas, seja em qualquer lugar onde querem um pouco de privacidade e cumplicidade.

Todos esses mecanismos de comunicação permitiram desenvolver o uso de meios, de interfaces, tecnologias de codificação, linguagens, protocolos e

procedimentos que se usam nas mais modernas transmissões de comunicação à distância.

2.1 Início do Rádio e da TV

A construção do eletroímã em 1820 pelo francês André-Marie Ampère foi vital para o desenvolvimento da comunicação e do eletromagnetismo. Em 1832, Samuel Finley Breese Morse criou o primeiro manipulador de telegrafia.

O sistema múltiplo Baudot permitiu aumentar muito a produtividade de transmissão e recepção dos telegramas e podia se transmitir até 300 telegramas/hora. Esse sistema foi inventado em 1874 por Jean Maurice Emilio Baudout.

Já em 1876, Alexander Graham Bell conseguiu a patente para o equipamento que lhe permitia transmitir e receber voz.

A decomposição do movimento em quadros sucessivos foi descoberta em 1880 pelo francês Maurice Le Blanc, técnica usada hoje para os desenhos animados. A decomposição da imagem em pontos e a sua posterior reconstrução a partir deles foram idealizadas e comprovadas pelo alemão Paul Gottlieb Nipkow em 1884.

O descobrimento das ondas eletromagnéticas foi possível com o trabalho teórico de James Clerck Maxell apresentado em 1863. Com base nesse trabalho, o alemão Henrich Rudolph Hertz conseguiu que uma faísca saltasse entre duas esferas de cobre, comprovando a existência do eletromagnetismo em 1887.

O início das comunicações sem fio, com o uso de ondas de rádio frequência, deu-se em 1896 quando o grande inventor italiano, Guglielmo Marconi, enviou e recebeu no seu laboratório o primeiro sinal de rádio por meio de ondas eletromagnéticas [6]. Quatro anos mais tarde ele fez a primeira comunicação pública sem fio, numa emissora inglesa.

A seleção de uma frequência, seja para transmissão, seja para recepção só foi possível graças ao circuito inventado em 1897 por Oliver Lodge. Essa frequência recebeu o nome de circuito sintonizador de frequência. Nesse mesmo ano foi inventado o tubo de raios catódicos por Karl Ferdinand Braun

Em 1903, foi feita a primeira conferência internacional de comunicação sem fio, wireless, em Berlim, na Alemanha. Três anos mais tarde, em 1906, em Brant Rock, Massachussets, Estados Unidos, Reginald Fessenden realizou no seu laboratório uma chamada de telefone sem fio que alcançou 11 milhas de distância.

A primeira legislação para o uso de rádio frequência, em que se definiu a alocação das faixas (bandas) do espectro a serem usadas para a comunicação doméstica foi publicada em 1912. Depois de muito trabalho e pesquisas, em 1916, Lee Forest instalou a primeira rádio em Nova Iorque.

Vladimir Kosma Zworykin, em 1923, patenteou o iconoscópio e, com ele, transmitiu imagens a 45 quilômetros de distância.

John Baird, em 1926, apresentou para os membros do Royal Institution e para repórteres do Times a transmissão experimental de televisão. O sistema de frequência modulada (FM) foi demonstrado aos executivos da RCA por Edwing Armstrong. A primeira transmissão oficial de televisão foi feita em 1930 nos Estados Unidos, em 1935 na Alemanha, 1936 em Londres e, em 1938, na Rússia, mas foi em 1939 que se iniciaram as transmissões regulares de televisão pela NBC.

A partir de 1941, o som da televisão passou a ser transmitido em FM.

A Motorola instalou em 1941 os primeiros rádios de comunicação bidirecional nos carros da polícia dos Estados Unidos e, em 1946, foi iniciada a comercialização dos serviços de radiotelefonia na cidade de St. Louis, Missouri, nesse país.

A televisão chegou ao Brasil apenas em 1950. Em 1951, a CBS iniciou nos Estados Unidos a transmissão de televisão em cores. A primeira transmissão por satélite foi realizada nos EUA em 1962.

A AT&T disponibilizou em 1965 os serviços de telefonia móvel que não precisavam mais do uso de botões para que as pessoas pudessem se comunicar (*push to talk*).

A FCC (*Federal Communication Commission*) [4], órgão regulador das comunicações dos Estados Unidos, em 1968 endereçou os questionamentos sobre a realocação do uso das faixas (bandas) de rádio frequência. A patente que descreveu como era possível executar, na comunicação sem fio, a transição automática sem intervenção manual entre células (*handoff*) foi concedida aos laboratórios da Bell em 1972.

Na década de 1980 teve início a telefonia celular analógica que usava as tecnologias NMT (*Nordic Mobile Telephone Network*), AMPS (*Advanced Mobile*

Phone System) e TACS (*Total Access Communication System*) conhecidas como a primeira geração. Depois vieram as tecnologias GSM (*Global System for Mobile Communications*), FDMA (*Frequency Division Multiple Acces*), TDMA (*Time Division Multiple Access*) e CDMA (*Code Division Multiple Access*) que formaram a segunda geração desenvolvida no final dos anos 80 e início de 1990.

Além dessas, houve, também, o que se considerou a segunda geração e meia no final da década de 90 quando apareceram as tecnologias GPRS (*General Packet Radio Service*), EDGE (*Enhanced Data Rates for GSM Evolution*), HSCSD (*High Speed Circuit Switched Data*), EVDO (*Evolution Data Only*). Na terceira geração, apareceu a tecnologia UMTS (*Universal Mobile Telecommunication System*),

Em 2009, houve geração 3,5 com tecnologias como HSDPA (*High Speed Downlink Packet Access*), HSPA (*High Speed Packet Access*) e HSUPA (*High Speed Uplink Packet Access*). Falou-se muito na quarta geração que chegaria no final de 2009 e início de 2010 com tecnologias LTE (*Long Term Evolution*), UMB (*Ultra Mobile Broadband*) e WIMAX (*Worldwide Interoperability for Microwave Access*).

A televisão com transmissão em HD (*High Definition*) foi anunciada pela Warner Bros pela primeira vez em 2007.

Na história da humanidade nunca houve uma evolução tão rápida de tecnologia como a que encontramos na eletrônica digital nestas últimas décadas: iniciou-se na década de 50 com a válvula.

Figura 1 – Válvula

Fonte: Apresentação Intel IDF

Nas décadas de 60 e 70 tem-se o aparecimento dos transistores de estado sólido aqui mostrado na figura 2.

Figura 2 – Transistor

Fonte: Apresentação Intel IDF

Na década dos anos 80 tem-se o aparecimento dos circuitos integrados o que permite hoje estar trabalhando com transistores integrados de 65 nanômetros, visíveis somente através de fotografia obtida por microscópio eletrônico com aumento de milhares de vezes como mostrado na figura 3.

Figura 3 - Transistor de 65 nanômetros – foto microscópio eletrônico.

Fonte: Intel

Só para se ter uma idéia dessa evolução, observa-se o tamanho dessa tecnologia: as válvulas usadas no início dos anos 50 que normalmente tinham 2 a 3 cm de largura por 5 a 10 cm de altura e os equipamentos possuíam, uma dezena de válvulas; o transistor tinha 0,5cm por 2 cm e os equipamentos usavam uma centena de transistores. O primeiro microprocessador da Intel, o 4004 de 1971, tinha 2.300 transistores. Em 2009, um processador Core i7 tinha mais de 800 milhões de transistores, isto é, um core i7 traz dentro de si, o equivalente a 350.000 processadores 4004 aproximadamente. Como se pode notar, essa evolução foi exponencial, como podemos ver no gráfico 2 e desde o início até agora transcorreram apenas 50 anos.

Gráfico 2 – Evolução do número de transistores no processadores – Fonte IEEE

http://www.ieee.org/portal/cms_docs/sscs/sscs/08Fall/BellFig6.JPG

2.2 Histórico das WPANs - – Wireless Personal Area Network.

Pode-se dizer que o início das redes sem fio pessoais deu-se quando a Zenith criou o primeiro controle remoto sem fio usando a tecnologia do infravermelho, em 1950, para o desenvolvimento de radares. Na década de 60, foi usada a tecnologia de UWB que, na década de 70, seria também usada para comunicações.

Em 1989 houve a regulamentação para o uso das frequências de 900MHz, 2,4GHz e 5GHz e, em 1990, formou-se um grupo para iniciar o estudo das transmissões sem fio no IEEE - *Institute of Electrical and Electronics Engineers*, nos Estados Unidos [7]. Em 1991, como alternativa europeia para o 802.11, surge o HIPERLAN.

Em 1993, foi fundado o IrDA *Infrared Data Association* [8], com o objetivo de promover o padrão de infravermelho para a transmissão de dados e o

desenvolvimento de dispositivos de controle remoto. Em 1996, o padrão HIPERLAN/1 foi aprovado na Europa.

Em 1996, após sete anos de pesquisas e desenvolvimento, o primeiro padrão de comunicação sem fio, 802.11, foi aprovado para transmissões com 1 e 2Mb [9]. Nesse mesmo ano também se criou um grupo no IEEE dentro do PASC (*Portable Applications Standard Committe*) para estudar as redes pessoais sem fio, WPANs.

Em 1998, surgiram as primeiras redes e equipamentos sem fio para uso doméstico: Any Point, Proxim, Symphony. Nesse ano também se iniciou o desenvolvimento do Bluetooth.

Em março de 1999, no IEEE, foi criado o Grupo de Trabalho 802.15 especificamente para cuidar do estudo e padronização da WPANs [10].

Em 14 de fevereiro de 2002, o FCC (*Federal Communication Commission*) liberou o uso do UWB. Nesse mesmo ano também foi liberado o primeiro padrão do 802.15.1 derivado do Bluetooth V 1.1.

Em 2003, o 802.15 publicam dois padrões: o 802.15.3a UWB *Multi-Band Orthogonal Frequency Division Multiplexing* (MB-OFDM) e o 802.15.4^a, definindo redes de muito baixo consumo. O segundo padrão deu origem às redes ZigBee que serão descritas no trabalho.

Em 2005, a Zensys desenvolveu uma rede para uso doméstico chamada Z-Wave que operava a 2.4GHz. Em 2006 foi o ano em que teve início as pesquisas para o uso de redes sem fio com 60GHz. Em janeiro de 2008, foram publicadas as primeiras especificações para as redes sem fio multigigabit para alta definição digital (*WirelessHD*).

O IEEE 802.11 monta o PAR 802.11.ad para estudar o padrão de rede sem fio que opera na frequência de 60GHz.

2.3 O que são as WPAN – Wireless Personal Area Network.

Hoje, a maioria dos jovens que mora nos grandes centros urbanos usa e leva consigo em média cinco equipamentos eletrônicos de uso pessoal [11]. Como exemplo, pode-se citar um telefone celular, um “tocador” de músicas do tipo MP3, um conjunto de fones de ouvido, um microfone, um equipamento de jogos, um armazenador de informações do tipo pen drive e um cartão com chip.

Além de todos esses equipamentos, os jovens ainda têm a sua disposição, tanto em casa quanto na escola ou no trabalho, outra grande quantidade de equipamentos de uso em seu dia a dia como podemos observar na blusa com equipamentos, mostrada na figura 4.

Figura 4 - Blusa com Equipamentos

Fonte: Intel IDR

Um dos maiores problemas desse ambiente está em como fazer para manter todos esses equipamentos atualizados e sincronizados, isto é, como garantir que todos estejam com a mesma informação e que ela seja a mais atual. Por esse motivo existe um grande interesse no desenvolvimento e uso das WPANs, Redes de Equipamentos Sem Fio de Uso Pessoal.

O interesse comercial pelas WPANs iniciou-se na década de 1990 (1991) quando surgiram, para uso em casa, as “*HomeRFs*” – redes de equipamentos interconectados por ondas de rádio, que operam na faixa de uso livre de 2.4GHz. Devido ao tamanho desse mercado e de seu enorme potencial, muitos grupos e empresas têm desenvolvido as mais variadas tecnologias e soluções, de tal maneira que hoje se encontram mais de dez tecnologias.

Dentre elas, pode-se destacar: Irda, Bluetooth, Hiper/LAN, IEEE 802.15, IEEE 802.11, 5GHz-UP, UWB, WUSB, ZigBee, Z-Wave etc.,.

Na área de equipamentos de uso pessoal, como se vê, cada um de nós, hoje, dispõe de quase uma dezena de equipamentos eletrônicos: celular, máquina fotográfica, microcomputador, tocador de músicas etc. Cada vez mais sente-se novas necessidades e, em contrapartida, dispõe-se de menos tempo para a atualização e sincronismo desses equipamentos.

Por isso, cada vez mais se torna importante e necessária a WPAN, rede de equipamentos sem fio de uso pessoal. O que se vê na pesquisa e desenvolvimento, é que na própria indústria e no mercado há uma forte pressão para a convergência e padronização dessas tecnologias.

Há diversos equipamentos e aplicações trabalhando em WPAN como mouses e teclados sem fio que além de prático, pois elimina os fios, permite mobilidade e comodidade. Pode-se operar hoje um micro com um controle remoto infravermelho sem fio, parecido com aqueles usados para operar as televisões, que em conjunto com o Centro de Entretenimento do Microsoft *Windows Media Center* permite uma dezena de operações sem a necessidade de conhecimento prévio.

Existe hoje uma infinidade de dispositivos que, com relativa facilidade, nos permite transferir informações de Celulares e Organizadores Pessoais PDAs (*Personal Digital Assistants*) para os computadores e vice e versa, por meio de tecnologia sem fio Bluetooth que possibilita um certo grau de sincronia entre esses dispositivos.

Pode-se também usar fones de ouvido, microfones, controladores de apresentação e tocadores de música que se comunicam com os computadores com alguma tecnologia sem fio permitindo grande facilidade de uso e mobilidade.

Como se vê neste trabalho, as WPANs já são uma realidade e cada vez mais tem-se novas aplicações e tecnologias que vão permitir um aumento na qualidade de vida. Como exemplo pode-se citar: O “*SYNC AND GO*” que é o processo no qual dois equipamentos se reconhecem e trocam informações automaticamente a fim de conseguir partilhar as mesmas informações, todas elas na sua última versão. É claro que essa troca de informações, se configurada, vai ocorrer de forma segura e só após os equipamentos terem checado as suas credenciais será executado o sincronismo. Esse procedimento tem que ser muito rápido e deve ser feito em questão de minutos ou segundos, pois muitas vezes, o tempo de que se dispõe para isso acontecer é muito curto.

Outra aplicação necessária atualmente é o reconhecimento automático das redes e lugares percorridos: ora se está em casa, ora na escola, ora no trabalho, ora em trânsito. Por isso os equipamentos terão que conseguir detectar a localização e o ambiente e serem inteligentes o suficiente para saber qual procedimento deve ser executado nesse contexto. Por exemplo, detectar a proximidade de um amigo, ou de

algo que se busca, e imediatamente sinalizar o fato de alguma forma pré-definida, é conhecido como “*Place and Context Recognition*” [14].

Todos os dias, ou em períodos pré-estabelecidos, executa-se tarefas repetitivas, o ideal seria se os equipamentos eletrônicos tivessem a capacidade de perceber a repetição dessas tarefas, aprender e, sem necessidade de pedir, que eles as executassem quando necessário, por meio de inteligência artificial com o aprendizado do comportamento.

Sem sombra de dúvida, é isso que se terá em pouco tempo, mas, para isso acontecer, é necessário que existam nas WPANs um padrão ou padrões com os quais os aparelhos consigam conviver e tenham a maturidade, estabilidade e desempenho requeridos pelas aplicações que os usuários desejam.

2.4 IEEE 802.11 Wireless Local Area Networks Wi-Fi.

Em 1989 o FCC - Comissão Federal de Comunicações dos Estados Unidos da América regulamentou e liberou dentro do capítulo 47 (Telecomunicações) na parte 15 sub parte B os equipamentos que usam o espectro de frequências, de uso livre, conhecidas como ISM - *Industrial, Scientific and Medical*: 902-928 MHz, 2400-2483.5 MHz, e 5725-5850, MHz .que foram destinadas à utilização por equipamentos industriais, científicos e médicos [4].

Em 1990 o IEEE - criou dentro do Projeto 802 LMSC- *LAN/MAN Standards Committee* [7] (que desenvolve padrões de Redes para Áreas Locais e de Redes para Áreas Metropolitanas) um grupo de trabalho com a finalidade de estudar e verificar a viabilidade de ter um padrão para as camadas físicas e camadas de acesso ao meio para as WLAN – *Wireless Local Area Network* - Redes sem Fio para Áreas Locais.

Em 1997 o grupo de trabalho IEEE 802.11 *TM WIRELESS LOCAL AREA NETWORKS - The Working Group for WLAN Standards* – Redes Locais Sem Fio – Grupo de trabalho para padronização da WLAN, termina o estudo e publica o primeiro padrão como IEEE *Standard 802.11* em 1997 que definia as redes sem fio operando nas frequências de 2.4 GHz e 5 GHz com velocidades de 1 Mbps e 2 Mbps.[9]

Em 1999 a ISO - *International Organization for Standardization* - Organização Internacional de Padrões e o IEC - *International Electrotechnical Commission* - Comissão Internacional de Eletrotécnica aprova o padrão 802.11 com a denominação ISO/IEC 8802-11:1999, e título: *Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications* [12].

Também em 1999 é formado o WECA - *Wireless Ethernet Compatibility Alliance* – Aliança para Compatibilizar as Redes Sem Fio Ethernet com a finalidade de permitir a interoperabilidade de equipamentos de diversos fabricantes dentro do padrão.

No ano de 2000 ocorreu o lançamento dos primeiros “*Hot Spots*” – Pontos Quentes, que são lugares onde existe sinal público de rede sem fio. Nestes lugares também foi lançado o selo Wi-Fi – *Wireless Fidelity* que garante o perfeito acesso da rede sem fio aos equipamentos que efetuaram os testes de compatibilidade definidos pelo WECA - *Wireless Ethernet Compatibility Alliance* – Aliança para Compatibilizar as Redes Sem Fio Ethernet.

Em 2001 a rede de cafeterias americana Starbucks instala em todas as suas lojas, pontos de acesso à Internet com a tecnologia de rede sem fio 802.11 com selo de compatibilidade Wi-Fi. Neste ano também fica demonstrada a fragilidade do protocolo de segurança WEP *Wired Equivalent Privacy* usado nas redes sem fio 802.11.

Em 2002 a aliança WECA muda de nome para WFA – *Wi-Fi Alliance*. Neste ano é publicado um novo conjunto de protocolos de segurança WPA – *Wi-Fi Protected Access* para as redes sem fio [13].

Em 2003 as redes sem fio aumentam a velocidade de operação para 54 Mbps sendo também publicadas as recomendações para permitir trânsito e mudança entre pontos de acesso.

No ano de 2004, são implementadas melhorias significativas na autenticação, autorização e criptografia grupo de trabalho 802.11i.

Em 2005 houve o desenvolvimento do padrão para atender os requisitos de QoS grupo 802.11e.

Em 2007 houve o aumento da velocidade do padrão 802.11g para velocidades acima de 22 Mbps.

Em 2009 houve o aumento nas velocidades de transmissão com a utilização das novas tecnologias MIMO - *Multiple Input Multiple Output* – Múltiplas Entradas e Múltiplas Saídas permitindo atingir velocidades de até 600 Mbps.

Em 2010 encontram-se estudos, adaptação e definição do padrão para trabalhar com as novas tecnologias de *High Definition* – Alta Definição tanto de áudio quanto de vídeo.

2.4.1 Arquitetura das redes 802.11 – Wi-Fi.

Na rede sem fio 802.11 [9][15] o sistema é dividido em células chamadas de BSS – *Basic Service Set* – Conjunto Básico de Serviços como mostrada na figura 5 onde todas as operações são controladas pela BS – *Base Station* – Estação Base que também é denominada de AP – *Access Point* – Ponto de Acesso.

BSS – Basic Service Set – Conjunto Básico de Serviços

Figura 5 -Conjunto Básico de Serviços

Uma rede sem fio pode ser construída com uma única célula, isto é com um único Ponto de Acesso (ou mesmo sem Ponto de Acesso) ou por vários Pontos de Acesso formando várias células. Essas células podem ser conectadas por um “*Backbone*” (canal central / espinha dorsal) ethernet que é chamado de DS – *Distribution System* – Sistema de Distribuição que estabeleça a conexão por meio dos Pontos de Acesso.

A rede local sem fio com toda a totalidade dos equipamentos incluídos nas células, os Pontos de Acesso – APs e o “Backbone” - DS é vista como uma única rede local sem fio 802 como se pode ver na figura 6, este tipo de rede é chamada de ESS – *Extended Service Set* – Conjunto de Serviços Estendido.

Figura 6 - Conjunto de Serviços Estendido

Para permitir a conexão da rede local sem fio 802.11 a outras redes foi definido dentro do padrão o conceito de “portal” que é o nome dado ao dispositivo que vai permitir que através dele ocorra essa conexão, funcionalmente é o equivalente ao conceito de Ponte – “*Bridge*” em outras redes.

Não há restrições no padrão que impeçam a um único dispositivo de exercer mais de uma função, isto é, um dispositivo pode funcionar como AP, Portal e estação de trabalho simultaneamente.

É possível ter um grupo pequeno de estações sem um ponto de acesso em uma configuração denominada IBSS - *Independent Basic Service Set* – Conjunto Básico de Serviços Independentes, como mostra a figura 7 que também é conhecida por rede sem fio Ad-hoc que é uma rede com conexão ponto a ponto sem definição de hierarquia e sem conexão ao sistema de distribuição, isto é, independente.

IBSS - Independent Basic Service Set – Conjunto Básico de Serviços Independentes

Figura 7- IBSS - Conjunto Básico de Serviços Independentes

No padrão 802.11 atualmente são definidas a Camada Física – PHY – *Physical Layer* e a camada de Controle de Acesso ao Meio - MAC – *Medium Access Control*.

Tem-se na camada física os seguintes padrões de codificação e transmissão:

802.11

IR – *InfraRed* – Infravermelho com 1 ou 2 Mbits/s.

DSSS – *Direct Sequence Spread Spectrum* - Espalhamento Espectral de Seqüência Direta operando na banda de 2.4GHz com 1 ou 2 Mbits/s.

FHSS – *Frequency Hopping Spread Spectrum* - Espalhamento Espectral por Salto de Frequências operando na banda de 2.4GHz com 1 ou 2 Mbits/s.

802.11a

OFDM - *Orthogonal Frequency Division Multiplexing* - Multiplexação por Divisão de Frequência Ortogonal operando na banda de 5GHz com velocidade de 54Mbits/s.

802.11b

DSSS – *Direct Sequence Spread Spectrum* - Espalhamento Espectral de Seqüência Direta operando na banda de 2.4GHz com 11Mbits/s.

802.11g

OFDM - *Orthogonal Frequency Division Multiplexing* - Multiplexação por Divisão de Frequência Ortogonal operando na banda de 2.4GHz com velocidade de 54Mbits/s.

802.11n

MIMO-OFDM - *Multiple-Input Multiple-Output - Orthogonal Frequency Division Multiplexing* – Múltiplas Entradas e Múltiplas Saídas - Multiplexação por Divisão de Frequência Ortogonal operando na banda de 2.4GHz e/ou 5GHz com velocidade de 65 Mbits/s até 600Mbits/s

Camada MAC - *Medium Access Control* - Controle de Acesso ao meio.

Tem-se na camada MAC duas diferentes modalidades, DCF – *Distributed Coordination Function* – Função de Coordenação Distribuída e PCF – *Point Coordination Function* – Função de Coordenação Local.

O método de acesso básico chamado de DCF – *Distributed Coordination Function* – Função de Coordenação Distribuída é baseada no CSMA/CA - *Carrier Sense Multiple Access with Collision Avoidance* - Acessos Múltiplos Percebendo o Sinal da Portadora Evitando as Colisões . O segundo método de acesso PCF – *Point Coordination Function* – Função de Coordenação Local é usado para priorização de tráfego quando houver necessidade, como é o caso de tráfego de voz ou vídeo.

No 802.11 se evita a colisão usando um esquema de confirmação positiva para a transmissão onde a estação que quer transmitir verifica o meio e se ele estiver ocupado deixa para transmitir depois, mas se ele estiver livre por um tempo determinado chamado de DIFS – *Distributed Inter Frame Space* Espaço Entre Quadros Distribuídos a estação pode transmitir, a estação receptora verifica a mensagem recebida calculando o CRC – *Cyclic Redundancy Codes* – Código de Redundância Cíclico e responde com uma mensagem de confirmação ACK – *Acknowledgment Packet* – Pacote de Confirmação pelo recebimento do ACK a estação que transmitiu tem a garantia de que não houve colisão. Se ela não recebe o ACK ela retransmite a mensagem até receber o ACK ou até que seja esgotado o número máximo de retransmissões.

Para evitar a probabilidade de colisão pelo fato de duas estações não se escutarem, problema conhecido como *Hidden Node* – Estação Escondida ou não visível, foi definido o mecanismo VCS – *Virtual Carrier Sense* – Percepção da Portadora Virtual onde a estação que quer transmitir envia, quando o meio está livre, um pequeno pacote de controle chamado RTS – *Request To Send* – Pedido Para Transmissão que leva os endereços de origem e destino e o tempo estimado da transmissão, a estação destino, se o meio estiver livre responde com um outro pacote de controle chamado CTS – *Clear To Send* – Livre Para Transmissão contendo as mesmas informações. Como todas as estações recebem o par RTS /

CTS chamado de NAV – *Network Allocation Vector* – Vetor de Alocação de Rede, pois eles são enviados via AP que os retransmite, é formado o canal virtual VCS durante todo o período de transmissão e estas informações são usadas pela camada física para o cálculo do tempo de espera.

As redes sem fio trabalham com fragmentação e reconstrução de pacotes: nas redes sem fio, devido a transmissão ser via RF, é preferível o uso de pacotes menores para evitar erros, a corrupção e retransmissão, e para manter a compatibilidade com outros padrões de rede foi definida na camada MAC do 802.11 um esquema de fragmentação e reconstrução de pacotes chamado *Send-and-Wait* – Envia e Espera onde a estação que transmite não pode enviar um segundo pacote enquanto não receber o ACK do fragmento enviado ou esgotar o número máximo de retransmissões.

Esta regra vale para o par origem-destino, isto é, se a estação tiver que enviar mensagens para destinos diferentes o esquema Envia e Espera vale para cada origem-destino, isto é, enquanto está esperando a confirmação de um fragmento de uma estação ela pode enviar um fragmento para outra estação destino.

Para resolver possíveis problemas de contenção foi definido no padrão 802.11, que deve ser usado o algoritmo *Exponential Backoff* – Espera Exponencial o qual irá determinar o tempo que cada estação deverá esperar para tentar transmitir de novo, no caso dela ter encontrado o meio ocupado e ter tido um problema de colisão.

Quando uma estação quer se conectar a uma rede existente seja por meio de um Ponto de Acesso AP, ou de uma rede Ad-Hoc, ela precisa trocar certas informações de sincronismo. Isso pode ser feito de duas maneiras:

- 1) de forma passiva, isto é, esperando receber um pacote de Beacon, que é um pacote que o Ponto de Acesso AP envia, quando configurado para isso, periodicamente para anunciar os serviços e permitir o sincronismo.

- 2) de forma ativa enviando pacotes de *Probe Request* – Pedido de Procura para o Ponto de Acesso AP e esperando a resposta. Estas duas formas são válidas e a opção por uma ou pela outra depende do esquema de segurança escolhido e do consumo de energia desejado.

Após a estação ter estabelecido o contato com o AP desejado, ela precisa seguir os procedimentos de autenticação onde tanto a estação como o Ponto de Acesso AP provam a suas identidades, credenciais e senhas. Em seguida ela deve

efetuar os processos de associação onde troca, com o Ponto de Acesso, informações sobre os serviços disponíveis e a estrutura da rede DS /ESS e a sua posição dentro dela, somente após ter completado todos estes procedimentos, a estação pode começar a transmitir e receber pacotes de dados.

O processo de Mudança de uma célula BSS para outra chamada de – *Roaming* [16]: é parcialmente definido pelo padrão 802.11 que define como essa mudança de célula deve ser processada, as ferramentas necessárias para que isso possa ocorrer, isto é, descobrimento (da estação base AP) ativo e passivo, o processo de associação e re-associação de forma que com esse processo seja possível implementar a mudança de célula sem perda de conexão.

O sincronismo é vital para todos os sistemas de comunicação e sobretudo para os sistemas móveis, por esse motivo o padrão 802.11 definiu um processo de sincronismo que é controlado pela estação base AP a qual periodicamente envia um pacote de controle conhecido por beacon frame onde a estação base AP coloca o valor de seu relógio, na hora da transmissão do beacon. Todas as estações dentro da BSS célula recebem este pacote e acertam seu relógio para manter o sincronismo com a estação base e por conseguinte com todos os participantes da BSS célula.

Existem três tipos principais de pacotes no padrão 802.11: Pacotes de Dados, que são usados para levar as informações da camada superior, Pacotes de Controle que são usados para controlar o acesso ao meio tais como, RTS, CTS e ACK e Pacotes de Gerenciamento que são usados para trocar informações de gerência e que não são passados para as camadas superiores e usam o mesmo formato do Pacote de Dados. A figura 8 mostra o formato geral dos pacotes do padrão 802.11.

Preâmbulo	Cabeçalho PLCP	Dados MAC	CRC
-----------	----------------	-----------	-----

Figura 8 – Quadro 802.11 Formato Geral

O Preâmbulo é usado para permitir o estabelecimento de sincronismo que é uma sequência de 80 bits alternados de zeros e um seguido por um delimitador de início de quadro ou pacote SFD – *Start Frame Delimiter* – Delimitador de Início de Quadro que são 16 bits com o seguinte conteúdo 0000 1100 1011 1101.

O cabeçalho de PLCP - *Physical Layer Convergence Protocol* – Protocolo de Convergência da Camada Física, contém informações de tamanho, velocidade

usada e campo de verificação de cabeçalho que serão usadas para tratar o quadro ou o pacote. A figura 9 abaixo mostra o pacote formato de dados do padrão 802.11.

Controle	Duração	end.1	end. 2	end. 3	Sequencia	end. 4	dados	crc
----------	---------	-------	--------	--------	-----------	--------	-------	-----

Figura 9 – Quadro 802.11 Formato de Dados

O campo Controle tem informações sobre a versão do 802.11 em uso, o tipo de frame que está sendo transmitido, informações de controle de célula, fragmentação, retransmissão, gerenciamento de energia, segurança e tipo de serviço.

O campo Duração pode indicar duas coisas: mensagem de aviso em caso de estado de baixo consumo ou duração do tempo de transmissão.

Os endereços especificam origem e destino ou encaminhamento do quadro ou pacote dentro da infra-estrutura da rede.

O campo de sequência é usado quando da fragmentação de quadros ou pacotes para permitir a reconstrução da mensagem a partir dos fragmentos na ordem correta.

O campo de dados como o próprio nome diz, leva a mensagem ou parte dela.

O CRC – *Cyclic Redundancy Codes* – Código de Redundância Cíclico é um campo de 32 bits que serve para verificar se o quadro ou pacote chegou ao destino de forma íntegra, isto é, se a informação enviada é a mesma recebida.

No padrão 802.11 temos três tipos de pacotes para o formato de controle::

Formato de RTS — *Request To Send* – Pedido Para Transmissão, este quadro é usado para solicitar o meio de acesso. A figura 10 mostra o pacote de controle para o formato de Pedido Para Transmitir.

Controle	Duração	RA	TA	CRC
----------	---------	----	----	-----

Figura 10 – Quadro 802.11 Pedido Para Transmitir RTS

Os campos de Controle e Duração são os mesmos do quadro de Dados MAC o Campo de RA – *Receiver Address* – Endereço de Destino é o endereço para onde a estação que está solicitando o meio quer transmitir a mensagem, o TA – *Transmitter Address* – Endereço do Transmissor é o endereço da estação que está

solicitando a obtenção do meio de acesso, em outras palavras solicitando a permissão para o uso do canal de transmissão

O quadro *Clear to Send* - Livre Para Transmissão - é enviado pela estação de destino indicando que o meio está livre para transmissão. A figura 11 mostra o pacote de controle para o formato de Livre Para Transmitir.

Figura 11 –Quadro 802.11 Livre Para Transmitir CTS

A estação do destino, quando recebe o quadro RTS indicando que o meio está livre, copia o endereço de TA para o endereço de RA e após o tempo determinado o envia para indicar que o meio está livre para transmissão.

Formato do ACK — *Acknowledgment Packet* – Pacote de Confirmação. este quadro ou pacote é usado para indicar ao transmissor que o quadro ou pacote foi recebido de forma correta. A figura 12 mostra o formato do quadro de Confirmação.

Figura 12 – Quadro 802.11 Confirmação ACK.

Como já foi dito este quadro serve para indicar a correta recepção de um quadro ou pacote.

2.4.2 Segurança dentro da rede sem fio 802.11 – WiFi.

Inicialmente foi definido, para atender os requisitos de segurança, no padrão 802.11[9][17] o uso do WEP *Wired Equivalent Privacy* – Privacidade Equivalente à Rede Com Fio, onde os principais objetivos eram prevenir que pessoas não autorizadas acessassem os recursos da rede e não permitir que as mensagens transmitidas fossem ouvidas ou capturadas (*eavesdropping* – espionadas) por terceiros mal intencionados.

Para acessar os recursos da rede o usuário tem que se autenticar com o uso de uma senha previamente definida. A escuta não autorizada é prevenida usando-se

a criptografia de 40, 64 ou 128 bits baseada no algoritmo RC4 que usa chaves combinadas com um PRNG – *Pseudo Random Number Generator* - Gerador de Números Pseudo Aleatórios - inicializado no começo da transmissão.

O problema neste esquema de segurança é que ele usa para a autenticação e criptografia chaves pré-definidas estáticas, combinadas com um vetor de inicialização que sempre começa do zero o que facilita muito a quebra deste esquema de segurança.

Para melhorar o esquema de segurança das redes sem fio, foi proposta a criação de um grupo de estudo que passou a fazer parte do padrão com o nome de 802.11i e que iniciou seus trabalhos com base no esquema de segurança WPA – *Wi-Fi Protected Access* – Wi-Fi com Acesso Protegido proposto pelo Wi-Fi Alliance.

Em vez de usar chaves estáticas como é no WEP no WPA foi desenhado um mecanismo de troca de chaves de segurança de forma dinâmica o que sem dúvida melhora muito os processos de autenticação e de criptografia.

Para o mundo empresarial tem-se o WPA-802.1x que combina a autenticação do Ponto de Acesso AP com um serviço de autenticação externa do tipo RADIUS ou Kerberos que também fornece dinamicamente as chaves de segurança.

Para os usuários domésticos tem-se o WPA – PSK – *Pre-Shared Key* – Chaves Previamente Compartilhadas que é similar ao WEP só que mais segura.

O WPA tem um mecanismo de múltiplas chaves conhecido por TKIP - *Temporal Key Integrity Protocol* - Protocolo de Integridade com Chaves Temporais onde em cada determinada duração de tempo as chaves são trocadas a fim de prevenir o descobrimento das mesmas por pessoas mal intencionadas

As diferenças entre o WEP e o WPA são: os dois usam a criptografia RC4 porém o WPA usa 128 bits em vez dos 104 usados no WEP, o WPA usa um vetor de 48 bits em vez dos 24 bits usados no WEP e finalmente o WPA usa a troca de chaves a cada determinado tempo TKIP.

Também existe o WPA2 que complementa o TKIP usando um mecanismo de criptografia mais elaborado chamado de AES – CCMP, sendo AES - *Advanced Encryption Standard* - Padrão Avançado de Criptografia e CCMP – *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol* – Protocolo de Autenticação em Modalidade Contador com Mensagens Encadeadas que tem a finalidade de atender a demanda das empresas.

A seguir se mostra uma tabela onde se pode comparar as características e finalidades dos diferentes esquemas de segurança que existem no padrão de redes sem fio 802.11.

	Autenticação	Criptografia	Empresarial	Uso Doméstico
WEP	none	WEP	fraco	Não muito bom
WPA (PSK)	PSK	TKIP	fraco	Muito bom
WPA2 (PSK)	PSK	AES-CCMP	fraco	Muito bom
WPA (full)	802.1x	TKIP	Melhor	bom (caro)
WPA2 (full)	802.1x	AES-CCMP	Ótimo	bom (caro)

Tabela 1 - Esquemas de Segurança padrão 802.11

Além desses esquemas de segurança o WPA 802.1x pode ser implementado com o uso de um servidor de autenticação do tipo RADIUS, mas isto não é recomendado para usuários domésticos devido à complexidade da sua configuração.

Outro cuidado que se deve ter é quanto ao gasto de CPU, quando se usa AES-CCMP, pois estes mecanismos usam algoritmos complicados para efetuar a criptografia o que exige muito poder de processamento, o que pode acarretar aumento de tempo e queda de desempenho.

2.4.3 Duração da bateria e consumo de energia no 802.11 - WiFi.

O desenvolvimento do padrão 802.11 foi feito, pensando especialmente nos equipamentos móveis e por isso dentro do padrão houve a preocupação de especificar mecanismos de como os equipamentos podem entrar no estado de baixo consumo [18] (estado dormente – *sleep mode*) para economizar o uso de energia e consequentemente aumentar o tempo de duração da bateria.

Para isso o Ponto de Acesso AP mantém uma tabela atualizada e áreas reservadas para armazenamento (*buffers*) de mensagens dos equipamentos de sua célula que se encontram no estado de baixo consumo. Para que não ocorra perda

de informações, ele mantém essas tabelas e áreas da memória até que a estação solicite o envio ou até que ela mude seu estado de operação.

O Ponto de Acesso AP dentro do processo de envio das mensagens de controle de sincronismo (envio do Beacon), envia a informação se existem mensagens armazenadas na memória para a estação e com isso a estação pode solicitar (*Poll*) o envio das mensagens que estão em espera no Ponto de Acesso AP.

As mensagens de Multicast e Broadcast endereçadas às estações que estão em estado de baixo consumo, também ficam armazenadas no Ponto de Acesso até que elas requisitem o envio.

2.4.4 O aumento da velocidade de transmissão das redes Wi-Fi com o aparecimento do padrão 802.11n.

Como os 50 Mbps de taxa de transmissão nominal, cerca de 30 Mbps de taxa real, não são suficientes para atender a demanda das aplicações do mercado. Em janeiro de 2004 foi formado, dentro do padrão 802.11, o subgrupo “n” o qual tinha como objetivo estudar as propostas do mercado para aumentar a velocidade das redes sem fio. [9][13]

Inicialmente surgiram em 2005 as propostas da WWiSE (*World-Wide Spectrum Efficiency* – Eficiência no Uso do Espectro Mundial) e TGnsync (*Task Group n Synchronization* – Força Tarefa n para Sincronização) e em 2006 a proposta do EWC (*Enhanced Wireless Consortium* – Consórcio para Melhoria das Redes sem Fio). Todas propunham a utilização de várias antenas para transmitir e para receber os sinais e essa técnica é conhecida como MIMO (*Multiple-Input Multiple-Output* Múltiplas - Entradas e Múltiplas Saídas) ou por multiplexação espacial. Para a codificação é usado o OFDM e por isso o sistema final é conhecido por MIMO-OFDM com várias antenas como podemos ver na figura 13 onde todas as propostas têm a operação a 20 MHz, mas também suportando 40 MHz., todas contemplando a interoperabilidade com os padrões anteriores 802.11 a/b/g.

Figura 13 - Sistema com várias antenas MIMO-OFDM.

A WWiSE e a TGnsysnc decidiram se unir e apresentar uma proposta conjunta JP (*Joint Proposal*) para o IEEE, mas o EWC decidiu acelerar o processo de adoção com o Wi-Fi levando a velocidade limite a 600 Mbps o que levou os três grupos a se unirem e levarem uma proposta única baseada nas definições do EWC para o IEEE, o primeiro rascunho (*Draft*) foi aprovado em 2007 e a versão final foi aprovada em 2009.

No padrão 802.11 está definido a utilização de vários Canais de comunicação dependendo da largura de banda e das frequências que são utilizadas. As redes 802.11b e 802.11g têm disponíveis 11 canais de transmissão operando entre as frequências de 2.412 GHz (canal 1) a 2.462 GHz (canal 11), com intervalos de 5 MHz.

Os canais utilizam uma banda de 22 MHz e por isso as bandas de frequências acabam sendo compartilhadas e isto faz com que as redes que operam em canais próximos interfiram entre si..

Apenas três canais, os canais 1, 6 e 11, não apresentam sobreposição e podem ser utilizados ao mesmo tempo por redes distintas de uma determinada região sem que ocorram fenômenos de interferência.

A tabela 2 abaixo mostra os 11 canais disponíveis nas redes 802.11 b e 802.11 g e as frequências utilizadas.

Canal	Frequência nominal	Frequência prática
1	2.412 GHz	2.401 a 2.423 GHz
2	2.417 GHz	2.405 a 2.428 GHz
3	2.422 GHz	2.411 a 2.433 GHz
4	2.427 GHz	2.416 a 2.438 GHz
5	2.432 GHz	2.421 a 2.443 GHz
6	2.437 GHz	2.426 a 2.448 GHz
7	2.442 GHz	2.431 a 2.453 GHz
8	2.447 GHz	2.436 a 2.458 GHz
9	2.452 GHz	2.441 a 2.463 GHz
10	2.457 GHz	2.446 a 2.468 GHz
11	2.462 GHz	2.451 a 2.473 GHz

Tabela 2 - Canais e Frequências utilizadas no 802.11b e 802.11g

Na figura 14 pode ser observada a sobreposição dos canais no 802.11 b e g, nela são observados os canais 1, 6 e 11 que são os únicos que não apresentam sobreposição e por isso são os mais usados.

Figura 14 – Canais no padrão 802.11 b e 802.11 g.

Fonte: Cisco Systems.

O padrão 802.11a utiliza 300 MHz de banda na frequência de 5 GHz e tem 12 canais não sobrepostos. Sendo 8 para redes sem fios (*indoor*) 200MHz operando entre as frequências de 5.15GHz a 5.32GHz e 4 para conexões ponto a ponto (*outdoor*) 100MHz operando entre as frequências de 5.725GHz a 5.825GHz. A tabela 3, apresenta os 12 canais e frequências utilizadas no padrão 802.11 a.

Canal	Frequência nominal	Frequência prática
36	5180	5171 a 5188 GHz
40	5200	5191 a 5208 GHz
44	5220	5211 a 5228 GHz
48	5240	5231 a 5248 GHz
52	5260	5251 a 5268 GHz
56	5280	5271 a 5288 GHz
60	5300	5291 a 5308 GHz
64	5320	5311 a 5328 GHz
149	5745	5736 a 5753 GHz
153	5765	5756 a 5773 GHz
157	5785	5776 a 5793 GHz
161	5805	5796 a 5813 GHz

Tabela 3 - Canais e Frequências utilizadas no 802.11a.

O espaçamento entre as portadoras é de 20 MHz e como a largura de banda de cada portadora é de 16,6 MHz, este esquema não tem sobreposições como podemos observar na figura 15.

Figura 15 - Canais no padrão 802.11 a.

Fonte: Cisco Systems

O padrão 802.11n usa canais com 20 ou 40MHz operando nas frequências de 2.4 GHz e 5 GHz, sendo que na frequência de 2.4 GHz existem 3 canais de 20 MHz sem sobreposição enquanto na frequência de 5 GHz tem 24 canais de 20 MHz sem sobreposição, já usando canais de 40 MHz há somente 1 canal quando opera na frequência de 2.4 GHz e 12 canais quando opera na frequência de 5 GHz.

A tabela 4, apresenta os canais e frequências utilizadas no padrão 802.11 n.

Canal	Frequência nominal
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437

Canal	Frequência nominal
34	5170
36	5180
38	5190
40	5200
42	5210
44	5220

7	2442
8	2447
9	2452
10	2457
11	2462

2.4 GHz com 3 canais de 20 MHz

46	5230
48	5240
52	5260
56	5280
60	5300
64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
149	5745
153	5765
157	5785
161	5805
165	5825

5 GHz com 24 canais de 20 MHz

Tabela 4 - Canais e Frequências utilizadas no padrão 802.11n

2.5 HiperLAN/2 – High Performance Radio Local Area Network – Rede Local com Rádio de Alto Desempenho.

Em abril de 2000 o ETSI - *European Telecommunications Standardisation Institute* (Instituto Europeu de Padronização das Telecomunicações), liberou as especificações do padrão HiperLan/2 [19] o qual faz parte do projeto de uma família de padrões para banda larga o BRAN *Broadband Radio Access Network* (Rede de

Acesso ao Rádio de Banda Larga). Nele foram definidas as características de acesso às redes fixas, tanto públicas como privadas, a uma velocidade de 54 Mbps através de rádio frequência operando a 5 GHz com QoS *Quality of Service* – (Qualidade de Serviço) flexível e extensível.

O HiperLAN/2 é promovido pelo H2GF – *HiperLAN/2 Global Forum* WWW hiperlan2, o qual foi fundado em 1999 pela Bosch, Dell, Ericsson, Nokia, Telia e a Texas Instruments. Até 2001 mais de 50 companhias já tinham se unido a este fórum.

O grupo RES10 *Radio Equipment and Systems 10* (Equipamentos de Rádio e Sistemas 10) do ETSI antes de definir o padrão do HiperLAN/2 definiu uma versão inicial para redes ponto a ponto de dispositivos móveis chamada de HiperLAN que já suportava transmissões de dados assíncronos e aplicações de tempo real. Assim que o BRAN foi estabelecido este passou a liderar o estudo do HiperLAN e o RES10 foi encerrado.

O padrão do HiperLAN/2 teve suas funcionalidades estendidas com a inclusão da arquitetura ponto a multi-ponto que recebeu o nome de HIPERAccess e da tecnologia de alta velocidade, 155 Mbps, para ligações ponto a ponto.

2.5.1 Arquitetura do HiperLAN/2

A rede HiperLAN/2 consiste de vários Pontos de Acesso AP que são responsáveis pela cobertura de uma região chamada de *Cell* (Célula) dentro desta célula pode-se ter um ou mais dispositivos móveis chamados de MT (*Mobile Terminals* – Terminais Móveis), os quais se comunicam entre si, por meio do Ponto de Acesso AP. Este tipo de comunicação recebe o nome de CM *Centralized Mode* (Modo Centralizado), que também suporta a comunicação direta a qual é chamada de DM *Direct Mode* (Modalidade Direta). Nesta modalidade os participantes se comunicam desde que estejam dentro do alcance da transmissão e um deles opere como CC – *Central Controller* – Controlador Central. Todos os dispositivos suportam nativamente a modalidade DM e a modalidade CM é oferecida como opcional.

O protocolo definido no padrão opera nas três camadas mais baixas do modelo de referência ISO / OSI que no HiperLAN/2 são chamadas de *Physical Layer* (Camada Física), *Transmission / Security Layer* (Transmissão / Camada de

Segurança) e *Switching Layer* (Camada de Chaveamento). A segunda camada de transmissão e segurança também é chamada de DLC *Data Link Control* (Controle do Enlace de Dados) que é dividido em três unidades funcionais RLC – *Radio Link Control* – Controle do Enlace de Rádio, EC – *Error Control* – Controle de Erros, e MAC *Medium Access Control* (Controle de Acesso ao Meio). A camada de chaveamento é dividida em duas subcamadas a subcamada SAR *Segmentation And Reassembly* (Segmentação e Remontagem) que divide as mensagens na transmissão e reconstrói na recepção e a subcamada CL *Convergence Layer* (Camada de Convergência) que faz a ponte entre as camadas superiores e a camada de segurança, resultando em independência entre as camadas, facilitando as operações de movimentação entre células e redes.

O acesso ao canal é controlado de forma centralizada onde o gerenciamento fica a cargo da estação Mestre, estação CC *Central Controller* (Controle Central), em um esquema de protocolo Mestre / Escravo, a estação Mestre determina a quantidade de dados que a estação Escrava vai poder transmitir, dependendo dos serviços requeridos por todas as conexões existentes.

O tamanho do quadro do HiperLAN/2 é de 2 ms o que corresponde a 500 caracteres por quadro. Afigura 16 apresenta o quadro de tamanho fixo.

Quadro MAC com um tamanho fixo $t = 2\text{ms}$

Figura 16 – Quadro HiperLAN/2 Formato Geral

Os quadros podem ser espalhados nas diferentes funcionalidades nas diferentes fases e com duração de tamanho variável como mostra a figura 17 abaixo.

Fase de Broadcast	Fase de Fim de Enlace	Fase de Início de Enlace	Fase de Acesso Randomico
-------------------	-----------------------	--------------------------	--------------------------

Figura 17 – Quadro HiperLAN/2 Tamanho Variável

São criados tantos canais lógicos, quantos tipos de serviços forem requisitados, isto é, é criado um canal lógico para cada tipo de serviço / transmissão. Certos canais são criados para solicitar criação / finalização de canais.

Os canais existentes são: Canal de Broadcast usado para enviar informações de controle, Canal de Quadro usado para enviar informações para todas as estações da célula, Canal de Acesso usado para responder as estações, Canal Curto e Canal Longo usado para transmitir os Dados e informações de controle, Canal do Usuário usado para transmitir dados, Canal Dedicado usado para aplicações específicas, Canal de Controle Lógico usado para transmitir informações de erro e gerenciamento, e Canal de Acesso Randômico usado para enviar solicitações e pedidos.

A transferência das informações é feita, usando a faixa de rádio frequência dos 5 GHz e usa a Multiplexação por Divisão Ortogonal de Frequência que possibilita diversas velocidades de transferência, dependendo da modulação usada, com 6 Mbps no uso de BPSK até 54 Mbps usando 64QAM.

2.5.2 Outros Serviços do HiperLAN2.

O HiperLAN/2 oferece uma grande gama de serviços sobretudo para gerenciamento e controle de segurança o que a torna uma tecnologia muito apropriada para ser usada na infra estrutura central (*Backbone*) de redes metropolitanas e corporativas.

Como principais características podem-se destacar: Seleção Dinâmica de Frequência, Controle e Ajuste da Potência conforme as necessidades, Segurança, Gerenciamento, Suporte a Qualidade de Serviços e facilidade de integração com outros padrões tais como o UMTS *Universal Mobile Telecommunication System* (Universal de Telecomunicações Móveis).

2.6 Tecnologias de rede sem fio usando a luz infravermelha – *InfraRed*

Foi a Zenith Radio Corporation que em 1950 criou um dispositivo através do qual eram enviados comandos ao televisor por meio de ondas de luz infravermelha sem o uso de cabos o qual chamou de "*Lazy Bones*", só mais tarde foi desenvolvido um controle que além dos comandos conseguia ligar e desligar a televisão e foi chamado de "*Flashmatic*". Nos anos 80 todos os televisores já incorporavam esta

tecnologia, e hoje 99% dos produtos eletrônicos de consumo como aparelhos de som, DVD - *Digital Video Disc* ou *Digital Versatile Disc* - Disco Digital de Vídeo ou Disco Digital Versátil., etc., vendidos em todo o mundo, foram incorporados com o infravermelho devido ao seu baixo custo e facilidade de operação.

Os dispositivos infravermelho para enviar comandos trabalham de forma unidirecional, com comunicação em um único sentido (*Simplex*), os comandos são enviados do controle remoto à TV, isto é, ela só recebe e executa, ela não envia nenhum sinal de volta.

Como decorrência da grande utilização dos controles remotos apareceram diversas propostas de sistemas bidirecionais onde tanto o receptor como o emissor poderiam enviar e receber comandos (*Half Duplex*).

Em 1993 foi fundada pela HP, IBM e a Sharp a IrDA *Infrared Data Association* (Associação para Transmissão de Dados por Infravermelho) [8] que é uma organização internacional com o objetivo de estabelecer um padrão para os dispositivos com infravermelho. O primeiro padrão foi publicado em junho de 1994 e hoje já se tem mais de 150 milhões de dispositivos usando o Infravermelho no mercado mundial.

Em dezembro de 2007 foi criado um SIG *Special Interest Group* (Grupo Especial de Interesse) para o desenvolvimento da comunicação usando infravermelho como taxa de transferência de dados de 1 (um) Gigabit/s. Já foram feitas algumas demonstrações em eventos usando esta tecnologia para transmissão de vídeos.

2.6.1 Arquitetura do Infravermelho.

O IrDA definiu no padrão dois tipos de arquiteturas, o *IrDA-Control* ou IrDA-C (Conexão orientada entre dispositivos e periféricos para envio de comandos e controles e o *IrDA-Data* ou IrDA-D (Conexão orientada entre dispositivos para transferência de dados).

Tanto no IrDA-C como no IrDA-D a comunicação é feita através do esquema Mestre / Escravo com esquema de *Polling* onde o Mestre pergunta de forma sequencial aos dispositivos, se têm algo para transmitir, se têm, o dispositivo é

selecionado / liberado para transmitir. Após a transmissão o Mestre consulta o próximo dispositivo.

Foram definidos três estados de operação: *link initialization* (Inicialização do enlace), Non Operational Mode (Modo não Operacional) e Operational Mode (Modo Operacional). No modo de inicialização do enlace, a estação mestre seleciona um endereço de estação e faz a consulta para ver se ela quer transmitir. No modo não operacional, é efetuada a verificação do meio e o estabelecimento dos parâmetros para transmissão. Após o estabelecimento dos parâmetros os dispositivos entram no modo operacional onde é feita a transmissão de dados e/ou comandos, uma vez terminada a transmissão a conexão é desfeita e os dispositivos voltam à modalidade de inicialização do enlace. Se não houver nada a transmitir / receber a estação entra em estado de descanso para economizar energia.

A transmissão, que é ponto a ponto, pode ocorrer simultaneamente entre vários dispositivos e inclusive um dispositivo pode estar participando de várias comunicações ao mesmo tempo. Os dispositivos podem em um determinado momento operar como Mestre e em outro como Escravo dependendo das necessidades de transmissão. Foi definido no padrão, o descobrimento de dispositivos e a resolução de endereços para solucionar possíveis conflitos de endereçamento de forma segura e dinâmica.

2.6.2 IrDA – Control

O padrão IrDA-C tem três camadas: PHY *Control Physical Layer* – (Camada Física), MAC *Media Access Control Layer* (Camada de Controle de Acesso ao Meio) e LLC *Logical Link Control Bridge Layer* (Camada de Controle do Enlace).

Camada Física: A modulação do sinal é feita usando 16 PSM *Pulse Sequence Modulation* (Modulação por Sequência de Pulsos usando amplificadores e circuitos com LED), *Light Emitting Diode* (Diodos Emissores de Luz e PD, *Photodetector* (Detectores de Luz), com dois tipos de pacotes um curto e um longo se consegue uma velocidade de transmissão de 75 Kbps.

Controle de Acesso ao Meio: como já foi mencionado é realizado no esquema Mestre / Escravo com consulta / seleção para transmissão, sendo que no IrDA-C não há transmissão de dados somente comandos e controles já que a

comunicação ocorre entre dispositivos e periféricos. A comunicação sempre é iniciada pelo dispositivo e não pelos periféricos a não ser que o dispositivo esteja no modo de descanso onde nesse caso o periférico poderia requerer a atenção. É prevista a comunicação entre um dispositivo e oito periféricos podendo haver comunicação com quatro periféricos simultaneamente.

É prevista no padrão a possibilidade de haver vários dispositivos com seus periféricos dentro do mesmo ambiente, neste caso eles se reconhecem e diminuem a transmissão, para diminuir a interferência.

Controle do Enlace: Foram definidos dois tipos de controle simples de enlace um para HA *Home Appliance* (Aparelhos Domésticos), desenvolvido para ser usado em aplicações residenciais como, por exemplo, acender luzes ou aquecedores e outro para HID *Human Interface Device Applications* (Aplicações para Dispositivos para Interface Humana), usado para controlar periféricos de informática como, por exemplo, teclados e monitores.

2.6.3 IrDA – Data

O padrão IrDA-D tem oito camadas: PHY *Physical Layer* (Camada Física), IrLAP *Infrared Link Access Protocol* (Protocolo de Acesso ao Enlace Infravermelho), IrLMP *Link Management Protocol* (Protocolo de Gerenciamento do Enlace), IAS *Information Access Service* (Serviço de Acesso à Informação), TinyTP *Tiny Transport Protocol* (Pequeno Protocolo de Transporte), IrOBEX *Object Exchange Protocol* (Protocolo de Troca de Objetos), IrCOMM *Communications Protocol* (Protocolo de Comunicação), IrLAN *LAN Access Protocol* (Protocolo de Acesso as Rede Locais).

Camada Física: No padrão 1.0 foi definido o SIR *Slow-Speed Infrared Mode* (Infravermelho com Modo de Baixa Velocidade) de 115 Kbps utilizando os mesmos circuitos projetados para a porta serial UART *Universal Asynchronous Receiver/Transmitter* (Receptor / Transmissor Assíncrono Universal). No padrão 2.0 foi definido o FIR *Fast-Speed Infrared Mode* (Infravermelho com Modo de Alta Velocidade) que trabalha com velocidades de 1,152 Mbps a 4 Mbps.

IrLAP - Infrared Link Access Protocol : Esta camada / protocolo é responsável pelo estabelecimento de conexão entre dois dispositivos, ela faz o

reconhecimento, levanta as informações necessárias, negocia os parâmetros, envia dados, e abre / fecha as conexões além de avisar as camadas superiores sobre o estado das conexões e possíveis erros.

IrLMP - *Link Management Protocol* : A camada / Protocolo IrLMP é composta na realidade por duas sub camadas / protocolos a saber: 1) O LM-Mux *Link Management Multiplexer* (Gerenciador Multiplexador de Enlaces) o qual permite que várias conexões / comunicações existam simultaneamente inclusive com vários dispositivos e que também permitam o chaveamento entre a função de Mestre e de Escravo, isto é, permitam que o dispositivo ora opere em uma conexão como Mestre e em determinado momento que seja exigido, passe a operar como Escravo e 2) LM-IAS *Link Management Information Access Services* (Gerenciador das Informações de Acesso a Serviços disponíveis no Enlace) que é responsável por receber, catalogar e publicar os anúncios de serviços recebidos das respectivas aplicações sendo o centro do Anúncio de Serviços.

IAS - *Information Access Service* Serviço de Acesso à Informação: é através desta camada / Protocolo que é possível a implementação das Páginas Amarelas – Anúncio de Serviços em toda a rede, aqui são implementados os serviços tanto de Servidor de Anúncio de Serviços (Banco de Dados de Serviços) como de Cliente, isto é, de como efetuar uma busca por um serviço.

TinyTP - *Tiny Transport Protocol* – Pequeno Protocolo de Transporte: Os serviços de transporte simples de mensagens são implementados por esta camada / protocolo sendo também responsável pela SAR – Segmentation And Reassembly – Segmentação e Remontagem de Mensagens.

IrOBEX - *Object Exchange Protocol* – Protocolo de Troca de Objetos: Esta camada / protocolo é opcional e serve para permitir que grandes quantidades de dados sejam transmitidos de forma confiável através da rede infravermelha, como exemplo pode-se destacar que é nesta camada que é implementada a transferência de arquivos na rede, ela permite que um objeto seja enviado para qualquer dispositivo.

IrCOMM - *Communications Protocol* – Protocolo de Comunicação Camada / Protocolo, especificado para permitir que aplicativos e programas escritos para trabalhar com portas seriais ou paralelas possam ser usados sem grandes mudanças. É uma camada que emula as portas, serial e paralelas, e não aproveita as facilidades de conexão definidas no IrDA.

IrLAN - LAN Access Protocol – Protocolo de Acesso às Redes Locais: A especificação do IrLan dentro do padrão serve para permitir a interconexão da Rede Infravermelho com outras redes locais, esta camada serve para definir a ponte de comunicação do IrDA com outras infra estruturas de redes locais.

2.6.4 Segurança no Infravermelho.

Por se tratar de uma rede ponto a ponto, onde para poder existir a comunicação entre os dispositivos deve ter visada completa, isto é, não pode ter nenhum objeto na área de visada dos dispositivos, o que proporciona um certo nível de segurança nativa, pois para invadir ou interceptar o sinal é necessário de alguma maneira que ocorra uma quebra ou invasão do meio físico o que por si só, sinaliza a existência de algum problema de segurança.

Além disso, também tem a codificação e modulação do sinal e em alguns casos também pode haver a criptografia dos dados a serem transmitidos.

Por isso o infravermelho é considerado um meio de transmissão relativamente seguro.

2.7 Tecnologias de rede sem fio Bluetooth

A IBM, Ericsson, Toshiba e a Nokia se juntaram em 1998 para formar um consórcio, O SIG Bluetooth *Bluetooth Special Interest Group* (Grupo Especial de Interesse em Bluetooth) [20][21][22] , com o objetivo de desenvolver uma especificação aberta de como deveria ser a comunicação em uma rede de equipamentos sem fio para dispositivos pessoais móveis, este consórcio recebeu o nome código de *Bluetooth*.

Eles deram este nome em homenagem ao rei da Dinamarca e Noruega, *Harald Blatand* que em inglês se escreve *Harold Bluetooth*, o qual ficou muito conhecido por ter unificado as tribos Dinamarquesas, Norueguesas e Suecas, pois o motivo deste consórcio é unificar a comunicação entre as tribos de telefones celulares, computadores e PDA - *Personal Digital Assistants* - Assistentes Digitais Pessoais.

O logotipo do *Bluetooth* é a união das runas nórdicas (*Hagall*) e (*Berkanan*) correspondentes às letras H e B no alfabeto latino.

Figura 18 – Logotipo do Bluetooth.

Fonte: SIG Bluetooth (22)

Em 1999 a Microsoft, Motorola, 3Com e a Lucent se juntaram ao consórcio que é uma sociedade privada com sede em Belluevue Washington com alguns escritórios espalhados por todo o mundo.

Existe uma regulamentação dos governos através do mundo e como exemplo de aplicações podemos citar: comunicação de telefones celulares com fones de ouvido que também podem ser usados como sistemas de viva voz, comunicação entre computadores quando for necessária pouca banda ou velocidade de transmissão, comunicação entre computadores e dispositivos PDA - *Personal Digital Assistants* (Assistentes Digitais Pessoais), telefones celulares, dispositivos ou equipamentos periféricos como impressoras, câmaras fotográficas, teclado, microfones, mouses, etc.

A comunicação *Bluetooth* também é usada para sincronizar dispositivos, arquivos e sistemas como, por exemplo: agendas telefônicas, sistemas de correio eletrônico, equipamentos de uso médico hospitalar, equipamentos de posicionamento global (GPS - *Global Positioning System*), e jogos (*Video Games*) com seus controles.

Em 2002 a versão 1.1 foi ratificada como padrão pelo IEEE sob o grupo 802.15.1, a versão corrente 3.0 recebeu a aprovação da especificação no dia 21 de abril de 2009 e a maior novidade é a facilidade de ter um AMP - *Alternate MAC / PHY* – MAC / PHY Alternativo como meio de transporte de alta velocidade e duas tecnologias foram apresentadas como solução para o AMP: o 802.11 - Wi-Fi e o UWB.

2.7.1 Arquitetura do Bluetooth.

Bluetooth é uma arquitetura em camadas que possui como centro um protocolo para substituir os cabos um controle de telefonia e protocolos adotados. [1]

O *Bluetooth* é uma rede de comunicação pessoal sem fio que opera via ondas de rádio na faixa de 2.45GHz . Dependendo da potência, o alcance pode ser de 1m com um sinal usando 1mW de potência ou 0 dBm até 100m usando 100 mW ou 20 dBm.

A comunicação entre os dispositivos ou estações é feita seguindo o esquema Mestre / Escravo de forma omnidirecional e permite a prestação de serviços assíncronos e isócronos e pode ser facilmente integrada a redes TCP/IP.

A banda é dividida em 79 portadoras espaçadas de 1 MHz portanto cada dispositivo pode transmitir em 79 frequências diferentes usando a multiplexação TDD *Time Division Duplex* (Transmissão nos Dois Sentidos), usando Divisão de Tempo; para minimizar as interferências, o dispositivo mestre, após sincronizado, pode mudar as frequências de transmissão de seus escravos por até 1600 vezes por segundo. Teoricamente sua velocidade pode chegar a 721 Kbps e ainda possui três canais de voz com multiplexação temporal (TDD).

Por motivos de segurança usa-se o FH *Frequency Hopping* (Salto de Frequência) pulando de canais durante o estabelecimento da conexão. Cada rede suporta até 8 dispositivos conectados simultaneamente, um mestre e sete escravos, e por isso recebe o nome de *Piconet* (*Pico Net*, pequena rede), mas pode ter até duzentos e cinquenta e cinco escravos estacionados, isto é que não estão conectados a nenhuma rede nesse momento. Dois ou mais dispositivos podem compartilhar um mesmo canal.

Denomina-se Scatternet a interconexão de várias piconets por meio do compartilhamento de um dispositivo mestre ou escravo, o dispositivo pode ser escravo em uma piconet e mestre na outra, os dispositivos podem transitar entre as piconets livremente.

Além da camada física (rádio) tem-se os protocolos obrigatórios do *Bluetooth* que são o LMP *Link Management Protocol* (Protocolo de Gerenciamento de Enlace), o L2CAP *Logical Link Control and Adaptation Protocol* (Controle Lógico do Enlace e Protocolo de Adaptação), e o SDP *Service Discovery Protocol* (Protocolos de Descobrimto de Serviços). Além dos protocolos obrigatórios podem ser usados

o HCI *Host Controller Interface* (Interface Controladora de Dispositivos) e o RFCOMM *Cable Replacement Protocol* (Protocolo de Substituição de Cabos), que são frequentemente usados. Também existem os protocolos que normalmente são adotados de outras especificações onde pode-se destacar: o PPP *Point to Point Protocol* (Protocolo Ponto a Ponto), o TCP *Transport Control Protocol* (Protocolo de Controle de Transporte), o UDP *User Datagram Protocol* (Protocolo de Datagrama de Usuário), o IP *Internet Protocol* (Protocolo Internet), o OBEX *Object Exchange Protocol* (Protocolo de Troca de Objetos), o WAE *Wireless Application Environment* (Ambiente de Aplicações de Rede sem Fio) que é parte do WAP *Wireless Application Protocol* (Protocolo de Aplicações de Rede sem Fio).

Descreve-se a seguir as funções de alguns desses protocolos:

LMP - *Link Management Protocol*: é usado para controlar o enlace entre dois dispositivos da rede e é através deste protocolo que é feito o controle do rádio, da banda base, do estabelecimento / término das conexões e do sincronismo dos dispositivos através do qual a estação mestre fornece o relógio e a sua identificação que é única a nível mundial. Além da identificação tem dois tipos de endereços que são usados o AMA - *Active Member Address* - Endereço de Membro Ativo de 3 bits e o PMA - *Parked Member Address* – Endereço de Membro Estacionado de 8 bits.

L2CAP - *Logical Link Control and Adaptation Protocol* : é usado para permitir que sejam estabelecidas diversas conexões lógicas com aplicações distintas simultaneamente. Este protocolo também é responsável pela fragmentação e remontagem das mensagens e sequenciamentos confiáveis dos pacotes e posterior verificação, o tamanho mínimo de um pacote é de 672 bytes e o tamanho máximo de uma mensagem é de 64KB, no caso de erro de sequência ele controla a retransmissão. Existe a modalidade aprimorada “*Enhanced*” desse protocolo que melhora o esquema do controle de fluxo e retransmissões.

SDP – *Service Discovery Protocol* : é usado para informar aos dispositivos quais os serviços que os outros dispositivos possuem, as suas versões e quais são as informações necessárias (perfis e parâmetros) para sua correta utilização. Cada serviço é identificado pelo seu UUID – *Universally Unique Identifier* – Identificador Universal Único de 128 bits, nos perfis é usado uma versão oficial curta de 16 bits.

HCI - *Host/Controller Interface* -: aqui é definida a comunicação padrão que deve ser feita entre o dispositivo e o circuito integrado controlador de Bluetooth, onde a idéia do padrão é que a comunicação possa ocorrer praticamente de forma

transparente, adaptando outras tecnologias como UART - *Universal Asynchronous Receiver/transmitter* – Receptor Transmissor Assíncrono Universal para telefones móveis e PDA's - *Personal Digital Assistants* - Assistentes Digitais Pessoais, e USB - *Universal Serial Bus* – Barramento Serial Universal para computadores.

RFCOMM - *Cable Replacement Protocol* : o RFCOMM é um protocolo de comunicação por radiofrequência criado para virtualizar a comunicação de cadeias de dados seriais permitindo simular a comunicação e o controle dos sinais da EIA-RS-232 dentro da banda base do *Bluetooth*. Essa foi uma forma muito simples e segura de permitir a transmissão de dados no *Bluetooth*.

Há outros protocolos de menor importância na pilha do Bluetooth tais como: BNEP - *Bluetooth Network Encapsulation Protocol* (Protocolo de Encapsulamento *Bluetooth* para Rede); usado para transmitir pacotes IP, AVCTP *Audio/Visual Control Transport Protocol* (Protocolo de Transporte para Controle de Áudio e Vídeo); usado para enviar comandos de controle para os dispositivos de Áudio e Vídeo, AVDTP *Audio/Visual Data Transport Protocol* (Protocolo de Transporte de Dados de Áudio e Vídeo) usado para a transferência de áudio e vídeo para os dispositivos como exemplo, podemos citar o envio de música para os fones de ouvido, TCS BIN *Telephone Control Protocol* (Protocolo de Controle de Telefone) é um protocolo orientado a bit, que define sinais de controle para estabelecimento de chamadas.

O acesso ao canal no *Bluetooth* é feito usando TDD – *Time Division Duplex* -, onde cada canal é dividido em espaços de tempo de duração de 625 μ s, permitindo que o pacote tenha um tamanho de até 2.745 bits podendo usar até 5 compartimentos de tempo.

2.7.2 Segurança no Bluetooth.

O *Bluetooth* usa um esquema de autenticação e confiabilidade baseado no uso de chaves e criptografia baseado no algoritmo SAFER - *Secure And Fast Encryption Routine* (Rotina de Criptografia Segura e Rápida) que usa o PIN - *Personal Identification Number* (Número de Identificação Pessoal) para a geração das chaves. Existem algumas ressalvas sobre a segurança do *Bluetooth*, mas deve-se considerar que ele foi projetado para uso doméstico. Em 2008 o NIST -

National Institute of Standards and Technology (Instituto de Padrões e Tecnologia Nacional) dos Estados Unidos publicou um guia para configurar de forma segura o *Bluetooth*.

2.8 - Tecnologias de rede sem fio *Zigbee*

Diferentemente dos outros tipos de redes onde se procura a transmissão de grande quantidade de dados e de desempenho, o padrão de redes *Zigbee* foi criado por 45 empresas que formaram o *Zigbee Alliance* – Aliança *Zigbee* [23][24][25] para desenvolver uma rede sem fio com o objetivo de possibilitar o controle e monitoramento de diversos equipamentos e sensores de forma segura, de baixo custo, flexível e de baixo consumo para atender o mercado de automação e controle militar, industrial, predial, médico, científico, pesquisa, etc., enfim de um largo espectro de aplicações.

A rede sem fio *Zigbee* opera com ondas de rádio frequência na faixa ISM 2.4 GHz (Global), 915 MHz (Estados Unidos) e 868 MHz na Europa com uma velocidade de transferência de dados que pode ir de 10 Kbps até 115 Kbps. Ela permite uma cobertura de transmissão entre 10 m e 100 m de alcance dependendo da potência dos equipamentos e das características do ambiente e tem a sua alimentação elétrica feita normalmente por baterias (pilhas) comuns que podem funcionar até por 6 meses.

2.8.1 Arquitetura do *ZigBee*.

No padrão *Zigbee* foram definidos dois tipos de dispositivos o RFD *Reduced Function Device* (Dispositivo com Função Reduzida) e o FFD *Full Function Device* (Dispositivo com Função Completa).

O RFD é de construção mais simples e exige uma configuração menor Além das funções de monitoramento e controle se comunica somente em ponto a ponto e por isso é usado em configurações simples onde toda a comunicação é enviada a um dispositivo coordenador.

O FFD é de construção mais sofisticada e normalmente tem uma configuração mais complexa, pois, além das funções de monitoramento e controle se comunica com vários dispositivos, podendo fazer as funções de armazenamento, encaminhamento (ponte), roteamento e gerenciamento.

Os dispositivos dentro da rede *Zigbee* podem ser usados para montar redes com diversos tipos de topologias, ponto a ponto, estrela, árvore e malha dependendo das necessidades da aplicação.

A estrutura do *Zigbee* foi definida em cinco camadas: PHY *Physical Layer* -, MAC *Medium Access Control Layer* -, NWK - *Network Layer*, APS – *Application Support Layer*, APL – *Application Layer* –.

Detalham-se a seguir as principais funções de cada camada. A camada física trabalha com RF na faixa ISM 898/915 Mhz e 2.4 GHz com modulação DSSS, com uma cobertura de até 100m com velocidade de até 250 Kbps.

A camada MAC no *Zigbee* foi projetada de maneira simples para permitir múltiplas topologias com baixo consumo de energia e usa quatro tipos de quadros: quadro Beacon, quadro de Dados, quadro de Confirmação e quadro de Comando. Na rede *Zigbee* sempre é definido um Coordenador que é responsável pelo sincronismo da rede e no caso pelo envio dos Beacons e quadros de confirmação para aumentar a eficiência, pode ser usado um super quadro com 16 espaços de igual tamanho onde, se necessário, até sete deles podem ser reservados para que requeiram baixa latência e uma quantidade específica de banda.

A camada de rede é responsável por iniciar a configuração da rede já que no *Zigbee* normalmente a rede se auto-configura, o controle da entrada de dispositivos na rede e da sua saída, a configuração e acerto de parâmetros dos novos dispositivos, o endereçamento, o sincronismo a segurança e o roteamento dos pacotes. Em todos os algoritmos das redes *Zigbee* o fator de consumo de energia é vital já que a maioria dos dispositivos da rede é alimentado por baterias (pilhas).

A camada de suporte a aplicação é responsável pela manutenção das tabelas que contem as informações das aplicações, dos caminhos, e das mensagens que deverão ser transmitidas e os controles necessários para a completa comunicação. Nesta camada também podem ser definidos caminhos e procedimentos alternativos para o aumento da confiabilidade da aplicação.

Finalmente a camada de aplicação é onde são executadas as aplicações, isto é os programas que normalmente controlam os sensores/motores ou dispositivos e enviam ou recebem as informações.

2.8.2 Segurança no ZigBee.

Para poder prover a rede de integridade, confidencialidade e autenticidade foram previstos na definição do padrão o uso de vários conjuntos de regras de segurança baseados no AES *Advanced Encryption Standard* (Padrão Avançado de Criptografia) o que permite adequar o grau de segurança desejado a necessidade da aplicação.

Como as redes Zigbee são usadas na área militar como redes de sensores para monitoramento e mapeamento de terrenos, o desenvolvimento de vários algoritmos de segurança tem sido motivos de inúmeras teses de doutorado nas mais diversas universidades, algoritmos hoje exportados para os mais diversos tipos de redes.

2.8.3 Outras facilidades do ZigBee.

A rede *Zigbee* tem sido, com muito sucesso, usada em redes de sensores onde é vital a duração da baterias, descobrimento da topologia e a auto configuração e reconfiguração da rede, a alta eficiência na comunicação e a segurança, justificando o uso da rede *Zigbee* nas áreas de biologia e no estudo de perturbação de ecossistemas, na área médica, no acompanhamento de pacientes à distancia, na indústria na linha de produção, nas cidades, no acompanhamento das vias públicas, e na área militar na área de monitoramento e mapeamento de terrenos.

Por estes motivos a rede *Zigbee* hoje é um celeiro de desenvolvimento de algoritmos de rede de alta eficiência, pois em todos os casos, o consumo de energia é prioridade máxima o que leva os pesquisadores e desenvolvedores a tomar um cuidado muito especial no desenvolvimento. Estes algoritmos são usados no

desenvolvimento da mais variada gama de dispositivos onde pode-se citar os celulares, notebooks, pontos de acesso e equipamentos eletrônicos de consumo.

2.9 Tecnologias de rede sem fio IEEE 802.15 *Working Group for Wireless Personal Area Networks*

No dia 12 de março de 1998 o IEEE 802.11 formou um SG *Study Group* (Grupo de Estudo) para pesquisar a necessidade de ter dispositivos de uso pessoal com comunicação sem fio de baixo consumo, muito simples que trabalhassem no POS *Personal Operating Space* (Espaço de Operação Pessoal). Isto inclui dispositivos que a pessoa carrega, usa ou leva perto do corpo. No dia 11 de março de 1999 este grupo foi transformado em um grupo de trabalho dentro do IEEE 802 LMSC *LAN & MAN Standards Committee* (Comitê de Padronização LAN e MAN) com o número P802.15 *Working Group for Wireless Personal Area Networks* [26] com a finalidade de padronizar as telecomunicações e a troca de informações entre sistemas dentro do POS especificando a camada física, e a camada de controle de acesso.

Devido a complexidade do assunto e abrangência do mesmo, o IEEE 802.15 dividiu o estudo em vários grupos de trabalho com o objetivo de facilitar e agilizar as conclusões e o estabelecimento de padrões.

2.9.1 802.15.1 *Personal Area Network Bluetooth v1.1*

Devido ao grande sucesso e utilização do padrão baseado nas especificações da Aliança *Bluetooth*, o IEEE decidiu adotar esse padrão derivado da versão 1.1 e que foi publicada no dia 14 de junho de 2002 como padrão IEEE 802.15.1 *Wireless Personal Area Network standard* baseado no *Bluetooth v1.1 Foundation Specifications*.

2.9.2 802.15.2 Coexistence Task Group

O grupo 802.15.2 foi montado para definir práticas e recomendações que facilitem a coexistência das redes 802.15 e 802.11, desenvolvendo também um modelo que quantifique a interferência mútua de forma que ela possa ser medida e controlada, permitindo a operação de dispositivos de ambas as redes no mesmo ambiente.

2.9.3 802.15.3 High Rate Task Group

O Task Group High Rate foi estabelecido para definir padrões para comunicação em velocidades de 11, 22, 33, 44 e 55 Mps, com comunicação isócrona, com qualidade de serviços, em redes ponto a ponto, provendo segurança, de baixo consumo, e baixo custo para atender a demanda de dispositivos de consumo que operam com imagens e multimídia.

2.9.4 802.15.4 Low Data Rate with Battery Life and Very Low Complexity – Zigbee

Este grupo foi formado para investigar e definir a comunicação entre dispositivos de baixo custo, com baixa potência, simples e alimentados por bateria ou pilhas de modo que possam operar meses ou se possível anos sem ter a necessidade da troca da bateria ou pilhas. As aplicações potenciais para este tipo de redes são sensores [27], crachás inteligentes, identificadores remotos, controles remotos, automação industrial, predial, ou residencial, controles remotos, etc. Comercialmente este tipo de rede é conhecido pelo nome de Zigbee.

2.9.5 802.15.5 Enable Mesh Networking

O grupo 802.15.5 foi formado em 2004 com a finalidade de estabelecer padrões para a comunicação em malha, permitindo dois tipos de configuração; a

malha total onde todos os dispositivos vão ter comunicação com todos os participantes da rede e a malha parcial onde os dispositivos vão ter comunicação com todos os dispositivos que sejam adjacentes. Com isso permite a economia de energia, o aumento de duração da bateria, e a facilidade de reconfiguração, o que resultaria no aumento da confiabilidade e no aumento da cobertura da rede sem a necessidade do aumento da potência de transmissão.

2.9.6 802.15.6 BAN Body Area Networks

O grupo de trabalho 802.15.6 foi formado em 2007 para desenvolver a padronização da comunicação de baixa potência e a operação dos dispositivos que operam no corpo do ser humano ou de outros seres vivos para atender as aplicações da área médica, de equipamentos de consumo, de entretenimento pessoal, de jogos e outros.

2.9.7 802.15.7 Visible Light Communication Task Group

Formado em 2009 o grupo 802.15.7 VLC – *Visible Light Communication* – Comunicação com Luz Visível foi formado para padronizar a comunicação usando a luz visível que utiliza ondas com largura de 400 nm (750 THz) a 700 nm (428 THz) e que é muito segura pois não faz mal ao ser humano e não requer regulamentação podendo ser usada em lugares restritos.

2.9.8 Outros Grupos do 802.15.

Estão em andamento outros grupos de interesse dentro do 802.15 dentre os quais podemos destacar o Grupo de Interesse em comunicação em Tera Hertz onde estão estudando a comunicação usando de 300 GHz a 2700 GHz, há também outro grupo de interesse que é SCwng - *Next Generation Standing Committee* - Comitê para Estudo das Redes Sem Fio da Próxima Geração que estimula os debates e apresentações de tecnologias de Redes sem Fio.

3 DEFINIÇÃO DE CRITÉRIOS DE COMPARAÇÃO

A análise, estudo e comparação das tecnologias de redes sem fio para uso pessoal foi realizada comparando-se os seguintes itens: Identificação, Organização, Disponibilidade, Enlace, Topologia, Espectro, Modulação, Canais, Compartilhamento, Acesso ao Meio, Velocidade, Alcance, QoS, Deslocamento, Aplicações e Observações, itens estes que serão descritos e explicados a seguir:

Identificação do padrão, nome do padrão dessa tecnologia.

Organização que desenvolveu as especificações da tecnologia.

Disponibilidade, isto é, se os produtos que permitem o uso desta tecnologia podem ser facilmente achados no mercado.

Tipo de transmissão quanto à visada ou condição do **Enlace**: a comunicação entre os dispositivos pode ser classificada como LOS *Line Of Sight* (Linha de Visão), ou como em Linha de Visada isto quando se pode unir os dispositivos envolvidos por uma reta imaginária ou como NLOS *Non in Line Of Sight*, quando isto não é possível, e eles não estão em Linha de Visada em uma linha reta.

Tipo de **topologias** que podem ser usadas: a palavra “topologia” vem do grego “*Topos*” forma ou lugar e “*Logos*” estudo desta forma quando se fala em topologia de uma rede nos referimos à forma, regra em que os dispositivos podem se comunicar entre si, isto é, “*Point to Point*” um dispositivo só pode falar com um dispositivo por vez, “ponto” *MultiPoint* um fala e vários escutam, “Estrela” todos falam com um dispositivo central que é o responsável em retransmitir para os outros, “*Mesh*” todos os dispositivos podem falar com todos, “Celula” todos os dispositivos falam com um dispositivo central similar à estrela. Chama-se de domínio de rede, o conjunto de dispositivos que estão em um determinado momento exercendo alguma função dentro de uma topologia de rede específica.

Espectro / frequência ou frequências utilizadas: quando se fala em comunicação sem fio é obrigatório se especificar em qual espectro ou espectros de frequência se estará operando, para que seja possível verificar a regulamentação e as características dos sinais eletromagnéticos que serão usados, exemplo: 2.4 GHz Banda Livre.

Técnica de **modulação** do sinal de transmissão e recepção: a técnica usada para se colocar um dado qualquer em um determinado canal (frequência – portadora) de um espectro de frequência é chamada de “modulação do sinal” e a técnica usada para retirar o dado de um determinado canal de um espectro de frequência é chamada de “demodulação do sinal”.

Número de **canais** utilizados e largura de banda de cada canal: normalmente o espectro de frequências em uso, por exemplo: 2.4 GHz são divididos em faixas ou pistas (Canais) de frequência, exemplo: 79 canais de 1 MHz ou quais terão a capacidade para a transmissão dos dados requeridos pela aplicação, estas faixas ou pistas são conhecidas como “Canais de Comunicação”. A largura de banda e o tamanho do canal são medidos pela variedade de frequências que podem ser transmitidas, por exemplo: 1 MHz e que normalmente está relacionada com quantidade de informações que podem ser transmitidas 3 Mbps no caso deste exemplo.

Técnica de **compartilhamento** da banda (*duplexing*): neste item é analisado se a comunicação ocorre somente em um sentido de cada vez (*Half-Duplex*) ou se pode haver a comunicação entre os dispositivos nos dois sentidos simultaneamente (*Duplex*) e como isto é implementado. São possíveis os esquemas TDD *Time Division Duplex* (Compartilhamento por Divisão de Tempo) e FDD *Frequency Division Duplex*, (Compartilhamento por Divisão de Frequência), etc..

Método de **acesso ao meio** de comunicação. Quando dois dispositivos transmitem informações ao mesmo tempo, no mesmo espectro e canal, usando a mesma frequência, ocorre uma colisão de sinais o que impossibilita a recuperação da informação transmitida, como exemplo disso podemos verificar o que acontece quando duas pessoas começam a falar ao mesmo tempo, os sinais sonoros se misturam e fica difícil entender o que foi falado, por isso é necessário estabelecer um mecanismo que regulamente ou organize a maneira e o momento em que os dispositivos poderão acessar (transmitir sinais), o meio (canal) de comunicação. Para esta finalidade foram desenvolvidos vários métodos:

- FDMA – *Frequency Division Multiple Access* – Acessos Múltiplos por Divisão de Frequência;
- TDMA – *Time Division Multiple Access*- Acessos Múltiplos por Divisão de Tempo;

- CDMA – *Code Division Multiple Access* – Acessos Múltiplos por Divisão de Código;
- CSMA/CA - *Carrier Sense Multiple Access with Collision Avoidance* - Acessos Múltiplos com Detecção da Portadora Evitando as Colisões;
- CSMA/CD - *Carrier Sense Multiple Access with Collision Detection* – Acessos Múltiplos com Detecção da Portadora e Detecção de Colisão.

Taxas de transmissão de dados, **velocidade**: a taxa de transmissão na área de comunicação de dados normalmente é medida verificando a quantidade de bits que podem ser transmitidos por segundo.

Alcance do sinal, cobertura: é sempre muito importante, quando se trata de comunicação sem fio, saber até que distância (em metros ou quilômetros) o sinal pode chegar com qualidade, isto é, saber até que distância o sinal será recebido de forma que o dado possa ser extraído e entendido, e qual é a potência elétrica (W – Watts ou mW – miliWatts) que é usada para poder obter esta cobertura de distância.

Há facilidades para tratar a qualidade de serviços **QoS**. A comunicação seja de voz, dados, músicas, imagens ou de qualquer outro tipo é uma prestação de serviços e como tal, há necessidade de se garantir que a voz, dados, músicas ou imagens cheguem ao destino em perfeitas condições e em um intervalo de tempo pré estabelecido, esta garantia da prestação do serviço é denominada de QoS – *Quality of Services* – Qualidade de Serviços.

Permite **deslocamento** entre os domínios de transmissão; outra análise importante das tecnologias de redes de comunicação sem fio é saber se é permitido na tecnologia mudar a qualquer momento a função exercida dentro das regras de topologia em tempo de execução da comunicação, isto é, em tempo real, e se é possível mudar dinamicamente de domínio de rede.

Aplicações típicas para as quais a tecnologia foi especificada: é importante analisar se a tecnologia em estudo aceita as aplicações mais usadas hoje em dia e também se está aberta para aceitar as tecnologias futuras, como exemplo podemos citar: a aplicação de voz, dados, música, imagens e vídeo conferências.

3.1 IEEE 802.11 – *Wireless Local Area Networks*

Identificação: hoje em dia as redes sem fio que utilizam o padrão de comunicação definido pelo IEEE 802.11- *Wireless Local Area Networks* são conhecidas por redes Wi-Fi, esta denominação surgiu no, WECA - *The Wireless Ethernet Compatibility Alliance* em 1999, do termo Hi-Fi - *High Fidelity* – Alta Fidelidade que por se tratar de redes sem fio foi adaptado para Wi-Fi – *Wireless Fidelity*.

Organização: A organização que desenvolveu o padrão para as redes sem fio para área local foi o IEEE 802. O início destas redes se deu com a liberação em 1989 pelo FCC de 3 faixas de frequência e com a formação em 1990 no IEEE de um comitê para estabelecer a definição de um padrão para as redes sem fio, a definição do padrão levou sete anos sendo que o padrão foi aprovado em 1997 com uma taxa de transmissão inicial de 1 Mbps e 2Mbps.

Disponibilidade: hoje, sem sombra de dúvida, é a tecnologia mais usada e mais conhecida para dispositivos móveis de computação com pontos de acesso em quase todos os lugares, atualmente a tecnologia está começando a ser usada também nos telefones celulares, dispositivos eletrônicos de consumo tornando-se praticamente um padrão de uso geral.

Enlace: o 802.11 opera com ondas de rádio frequência RF a transmissão é por difusão e por isso não precisa de visada.

Topologias: as redes sem fio do tipo 802.11 normalmente trabalham com a topologia estrela com todos os dispositivos se comunicando através de um ponto de acesso que faz a função de centralizador e ponte para outras redes, mas também permite a comunicação ponto a ponto para o estabelecimento de redes ad-hoc.

Espectro: o padrão 802.11 define a utilização das frequências de 2,4 GHz e 5 GHz mas hoje em dia existe um grupo do 802.11 estudando a possibilidade de utilização da faixa de 60GHz.

Modulação: no padrão 802.11 para modulação são usadas as codificações FHSS que consistem em dividir a banda larga de frequência num mínimo de 75 canais (*hops* ou saltos de uma amplitude de 1MHz), e seguidamente transmitir utilizando uma combinação de canais conhecida de todas as estações da célula. Na norma 802.11, a codificação DSSS que consiste em transmitir para cada bit uma sequência Barker (às vezes chamada ruído pseudo-aleatório ou em inglês

“*pseudorandom noise*”, denotado PN) também é usado um método alternativo CCK - *Complementary Code Keying* (Código Complementar por Chaveamento) que permite codificar directamente vários bits de dados numa só microplaqueta (*chip*) utilizando 8 sequências de 64 bits. Estas codificações são usadas em conjunto com os seguintes tipos de modulação: PSK – *Phase Shift Keying* (Modulação por Chaveamento de Fase), BPSK – *Binary Phase Shift Keying* (Modulação por Chaveamento de Fase Binário), QPSK *Quadrature Phase Shift Keying* (Modulação por Chaveamento de Fase por Quadratura), OFDM *Orthogonal Frequency Division Multiplexing* (Multiplexação por Divisão de Frequência Ortogonal) e MIMO *Multiple Input Multiple Output* (Múltiplas Entradas ,Múltiplas Saídas OFDM).

Canais: o número de canais das redes sem fio 802.11 pode variar de país a país, mas a grande maioria segue o padrão dos Estados Unidos que define 11 canais de comunicação para o 802.11b/g/n sendo três sem sobreposição e 12 canais de comunicação de 40 MHz ou 24 de 20 MHz para o 802.11a.

Compartilhamento: as redes sem fio 802.11 não tinham compartilhamento de banda, mas com a evolução do padrão hoje pode ter compartilhamento de banda dependendo da versão e configuração.

Acesso ao meio: para o acesso ao meio o 802.11 usa o CSMA/CA *Carrier Sense Multiple Access with Collision Avoidance* (Acessos Múltiplos Percebendo o Sinal da Portadora Evitando as Colisões) ou o PDMA *Packet Division Multiple Access* (Acessos Múltiplos por Divisão de Pacotes).

Velocidade: o 802.11 permite obter as seguintes taxas de transmissão: 1) 802.11b com PSK = 1 Mbps, 2) 802.11b com QPSK = 2 Mbps, 3) 802.11b com QPSK e CCK = 5.5 Mbps ou 11 Mbps, 4) 802.11a e 802.11g com OFDM e CCK54 Mbps, 5) 802.11n com MIMO / OFDM = de 65 Mbps a 600 Mbps.

Alcance: o alcance das redes sem fio 802.11 depende da tecnologia e frequência em uso, do tipo e potência da antena, do ambiente (interno ou externo) da velocidade em uso, e do nível de interferências existentes e por isso, pode variar de alguns poucos metros a quilômetros de distância, porém para aplicações tradicionais normalmente a distância é de 30 a 100 metros entre os dois dispositivos que vão se comunicar.

QoS: foi definido pelo IEEE em 2005 o padrão 802.11e que adiciona qualidade de serviço (QoS - *Quality of Services*) às redes IEEE 802.11. Esta

facilidade possibilita a transmissão de diferentes tipos de serviços de comunicação (Voz, Som, Imagem, etc.) com certos controles específicos.

Deslocamento: foi terminado o padrão 802.11r para definir a possibilidade de re-associação quando houver locomoção rápida do domínio de um ponto de acesso para o domínio de outro ponto de acesso, este deslocamento entre pontos de acesso é conhecido tecnicamente como *hand-off*.

Aplicações: hoje as redes sem fio 802.11 ou Wi-Fi são usadas em todos os segmentos do mercado, desde informática, medicina, indústria até equipamentos eletrônicos de consumo.

Observações: as redes sem fio 802.11 ou Wi-Fi são hoje um padrão quando se quer falar de redes sem fio para uso dentro de ambientes fechados (*indoor*).

3.2 HiperLAN/2

Identificação: Hiperlan/2- *High Performance Radio LAN* – Rede Local com Ondas de Rádio de Alta Performance foi desenvolvida na Europa como alternativa à rede sem fio padronizada pelo IEEE 802.11..

Organização: o Hiperlan/2 foi definido pelo ETSI – *European Telecommunications Standards Institute* – Instituto Europeu de padrões de Telecomunicações no projeto BRAN – *Broadband Radio Access Networks* – Redes com Acesso a Ondas de Rádio de Banda Larga e teve sua primeira versão do padrão aprovada em 1996.

Disponibilidade: hoje existem alguns produtos comercializados pela SICE “*Società Italiana Costruzioni Elettroniche*”, Pela Motorola, e pela Alvarion.

Enlace: como o Hiperlan/2 opera com ondas de rádio frequência RF a transmissão é por difusão e por isso não precisa de visada.

Topologias: as redes Hiperlan/2 suportam conexões do tipo estrela com um ponto de acesso centralizando as comunicações com ótimos recursos para ser a espinha dorsal das redes (centralização das conexões) como IP *Internet Protocol* (Protocolo da Internet), ATM *Asynchronous Transfer Mode* (Transferência em modo assíncrono), UMTS *Universal Mobile Telecommunication System* (Sistema Universal de Telecomunicações Móveis).

Espectro: utiliza a faixa de 5 GHz .

Modulação: Na versão 1.0 era usado a modulação FSK *Frequency Shift Keying* (Modulação por Chaveamento de Frequência) e GMSK *Gaussian Minimum Shift Keying*, na versão 2.0 era usada a modulação BPSK *Binary Phase Shift Keying* (Modulação por Chaveamento de Fase Binário), QPSK *Quadrature Phase Shift Keying* (Modulação por Chaveamento de Fase por Quadratura), 16QAM *16-State Quadrature Amplitude Modulation* (Modulação por Amplitude com Quadrantes) em 16 Estados e 64QAM *-64-State Quadrature Amplitude Modulation* (Modulação por Amplitude com Quadrantes) em 64 Estados.

Canais: como a maioria das redes de comunicação sem fio, ele usa basicamente um único canal de comunicação.

Compartilhamento: é usado TDD – *Time Division Duplex* – Compartilhamento por Divisão de Tempo com 2 ms de janela de tempo (slots).

Acesso ao meio: o acesso ao meio é feito usando *Dynamic TDMA – Time Division Multiple Access* (Acessos Múltiplos Alocados Dinamicamente por Divisão de Tempo) que faz a alocação dos espaços de tempo de forma dinâmica dependendo do algoritmo de escalonamento e da qualidade de serviços necessária.

Velocidade: no Hiperlan/2 a velocidade máxima é de 54 Mbps.

Alcance: o alcance de um Ponto de Acesso de HiperLAN2 tipicamente se estende aproximadamente a 30 metros no interior de ambientes e a 150 metros fora dos ambientes fechados, mas depende muito do tipo de antena usada.

QoS: os serviços básicos do Hiperlan/2 são dados, som e transmissão de vídeo com ênfase na qualidade de serviços e por isso se torna uma tecnologia ideal para funcionar como espinha dorsal de redes IP, ATM ou UTMS.

Deslocamento: o deslocamento não é o forte desta rede tendo um tempo de deslocamento muito grande 1.4m/s.

Aplicações: basicamente é usado como espinha dorsal para outras redes que precisem de qualidade de serviços.

Observações: esta tecnologia tem serviços para monitorar a segurança e para os dados tem DES *Data Encryption Standard* (Padrão para Criptografia de Dados) ou *Triple DES* e para todos os dispositivos pode-se requerer a autenticação.

3.3 Infra vermelho – *Infra Red*

Identificação: Infravermelho – *Infrared*.

Organização: IrDA – *Infrared Data Association* <http://www.irda.org> tem os seus escritórios em Walnut Creek, Califórnia, ela foi fundada em 1993 como uma organização sem fins lucrativos. As companhias que promovem a IrDA são: IBM, HP, Sharp, Nokia, Sony, Casio e outras.

Disponibilidade: praticamente todos os Controles Remotos vendidos com Televisões e Aparelhos de Som que vêm com tecnologia de infravermelho são produzidos em larga escala e por isso se tornam muito baratos. Essa tecnologia também é usada por outros dispositivos de uso pessoais como fones de ouvidos sem fio, Telefones Celulares, Notebooks e PDAs - *Personal Digital Assistants* – Assistentes Pessoais Digitais.

Enlace: praticamente todas as aplicações que usam o infravermelho operam com enlaces em LOS, ou seja, em linha de visada de curta distância, mas existem algumas poucas aplicações que colocam repetidores ou espelhos para permitir outros tipos de configurações de enlace.

Topologias: quase 100% dos dispositivos que utilizam infravermelho operam com configurações ponto a ponto, mas existem algumas poucas aplicações que usam outros tipos de topologias.

Espectro: utiliza a faixa de 300 GHz a 400 THz com um comprimento de onda de 1mm a 700nm.

Modulação: utiliza a modulação em banda base sem portadora com as técnicas, PPM - *Pulse Position Modulation* - Modulação por Posição de Pulso, HHH (1,13) que é uma abreviação dos nomes Hirt, Hassner e Heise que desenvolveram este código de modulação, EPM – *Edge Position Modulation* – Modulação na Posição da Borda e ASK – *Amplitude Shift Keying* – Modulação por Chaveamento de Amplitude.

Canais: como a operação é em banda base, é usado somente um canal de comunicação para transmissão em cada sentido.

Compartilhamento: para a grande maioria das aplicações a transmissão só ocorre em um único sentido por vez, isto é, *Half Duplex*.

Acesso ao meio: o acesso ao meio é feito através do IrLAP – *Infrared Link Access Protocol* – Protocolo de Acesso ao Enlace Infravermelho

Velocidade: a velocidade depende da técnica de modulação em uso e pode ser: PPM com velocidade de 2,4 Kbps a 115,2 Kbps chamada de SIR – *Serial Infrared* – Infravermelho Serial, 4-PPM ou 16-PPM com velocidade de 1Mbps a 4 Mbps Chamado de FIR – *Fast Infrared* – Infravermelho Rápido, HHH com velocidade de 16 Mbps chamado de VFIR – *Very Fast Infrared* – Infravermelho Muito Rápido, EPM com velocidade de 19,2 Mbps e ASK com codificação 8B10B com velocidade de 1 Gbps chamado de Infravermelho Giga.

Alcance: o alcance da tecnologia depende muito do dispositivo e do LED em uso, mas nas aplicações domésticas normalmente vai de 0,5 metros a 4,5 metros porém para aplicações profissionais pode alcançar 1.600 metros.

QoS: no protocolo de acesso ao enlace IrLAP podem ser negociados os parâmetros de QoS.

Deslocamento: como é necessário ter visada entre os dispositivos não possui controles para deslocamento.

Aplicações: controles Remotos, Telefones, Fones de Ouvidos, Mouses, Teclados, Instrumentação Médica, Assistentes Digitais Pessoais, Impressoras e outros,.

Observações: custo baixo menos de 1US\$, como é conexão ponto a ponto tem segurança, mas para operar tem que ter visada.

3.4 Bluetooth

Identificação: Bluetooth que recebeu este nome código em homenagem ao rei da Dinamarca e Noruega, Harald Blatand que em inglês se escreve *Harold Bluetooth*, o qual ficou muito conhecido por ter unificado as tribos Dinamarquesas, Norueguesas e Suecas, pois o motivo deste consórcio foi unificar a comunicação entre as tribos de telefones celulares, computadores e assistentes digitais pessoais (PDA - *Personal Digital Assistants*).

Organização: *Bluetooth SIG* - *Special Interest Group* - Grupo Especial de Interesse *Bluetooth* <http://www.bluetooth.org>, a IBM, Ericsson, Toshiba e a Nokia se juntaram em 1998 para formar este consórcio, com o objetivo de desenvolver uma especificação padrão aberta de como deveria ser a comunicação em uma rede de equipamentos sem fio de uso pessoal. Em 1999 a Microsoft, Motorola, 3Com e a

Lucent se juntaram a este consórcio que é uma sociedade privada com sede em Bellvue Washington com alguns escritórios espalhados por todo o mundo. O logotipo do Bluetooth é a união das runas nórdicas (*Hagall*) e (*Berkanan*) correspondentes às letras H e B no alfabeto latino.

Disponibilidade: segundo a Bluetooth SIG existem cerca de três bilhões de dispositivos Bluetooth no mercado e esse número cresce todos os dias, a tecnologia Bluetooth está nos telefones celulares, aparelhos de som, televisões, computadores, impressoras e periféricos, tocadores de música, fones de ouvidos, nos automóveis, e equipamento médicos e o número de aplicações também cresce dia a dia.

Enlace: como o Bluetooth opera com ondas de rádio frequência RF a transmissão é por difusão e por isso não precisa de visada .

Topologias: as redes Bluetooth suportam conexões do tipo PP - Ponto a Ponto, conexões PMP – Ponto Multi Ponto, conexões Piconets que são pequenas redes Bluetooth com oito dispositivos sendo um na Função de Mestre e até sete na função de escravos, e Scatternet, que é um sistema disperso composto de várias redes cada uma contendo um número limitado de dispositivos.

Espectro: utiliza a faixa ISM - *Industrial, Scientific and Medical*

Modulação: Na versão 1.0 era usada a modulação GFSK - *Gaussian Frequency Shift Keying* – Modulação por Chaveamento de Frequência com o algoritmo Gaussian, na versão 2.0 era usada a modulação DPSK – *Differential Phase Shift Keying* - Modulação por Chaveamento de Fase Diferencial, e na Versão 3.0 é usada a Modulação OFDM – *Orthogonal Frequency Division Multiplexing* – Multiplexação por Divisão de Frequência Ortogonal.

Canais: o Bluetooth define 79 canais de comunicação cada um com a largura de 1 MHz.

Compartilhamento: é usado TDD – *Time Division Duplex* – Compartilhamento por Divisão de Tempo com 625 µs de janela de tempo (slots).

Acesso ao meio: o acesso ao meio no Bluetooth é feito usando TDMA – *Time Division Multiple Access* - Acessos Múltiplos por Divisão de Tempo com FHSS – *Frequency Hopping Spread Spectrum* – Espalhamento Espectral por Salto de Frequência.

Velocidade: na versão 1.0 a velocidade podia chegar a 1 Mbps, na versão 2.0 se tem até 3 Mbps e na versão 3.0 onde passou a se usar o 802.11 conhecida como *High Speed* – Alta Velocidade chega a 24 Mbps.

Alcance: o alcance depende da classe do dispositivo. Para dispositivos da classe 3 onde se usa potência de 1 mW ou 0 dBm o alcance pode chegar a 1 metro, na classe 2 com potência de 2.5 mW ou 4 dBm o alcance é de até 10 metros já na classe 1 onde os dispositivos tem potência de 100mW ou 20 dBm o alcance pode chegar até 100 metros.

QoS: o Bluetooth implementa a qualidade de serviços para Voz em comunicações orientadas à conexão e para Dados em comunicações sem conexão.

Deslocamento: o deslocamento é implementado e permitido entre Piconets.

Aplicações: existem inúmeras aplicações que usam a tecnologia Bluetooth dentre as quais podem-se destacar telefones celulares, fones de ouvidos, computadores de bordo em automóveis, aparelhos de som, controles remotos, comunicação entre computadores, comunicação de dispositivos com seus periféricos, aparelhos médicos, controles de vídeo games e outros.

Observações: está em desenvolvimento a versão 4.0 onde se prevê um consumo mínimo de energia e velocidade de 1 Mbps e chave de segurança de 128 bits.

3.5 ZigBee

Identificação: *ZigBee* é uma rede sem fio que permite a comunicação entre dispositivos de forma segura, usando baixa potência e baixo custo, acredita-se que recebeu esse nome porque sua arquitetura em malha se assemelha ao Zigue Zague das Abelhas –“*Bee*”.

Organização: a Aliança *ZigBee* foi montada em 2002 por um grupo de mais de 40 empresas, que trabalharam com o IEEE para construir o padrão. No IEEE foi montado o grupo de estudos 802.15.4 que em maio de 2003 homologou a primeira versão do padrão.

Disponibilidade: devido ao baixo custo, baixo consumo e facilidade de programação e ao grande volume de bibliotecas existentes, esta solução é muito usada nas Universidades e Centros de Pesquisa e por isso se tem muitas soluções disponíveis no mercado.

Enlace: como o *ZigBee* opera com ondas de rádio frequência RF a transmissão é por difusão e por isso não precisa de visada.

Topologias: Para poder atender a todas as aplicações do mundo de sensores, ele permite as mais diversas topologias como conexões ponto a ponto, ponto multiponto, árvore, estrela e malha.

Espectro: trabalha com a frequência ISM que na Europa é de 868 MHz, 915 MHz nos Estados Unidos e de 2.4 GHz em outras partes do Mundo.

Modulação: para permitir uma transmissão confiável com baixa interferência em locais adversos o ZigBee usa o DSSS com modulação BPSK – *Binary Phase Shift Keying* – Modulação por Chaveamento de Fase Binária e OQPSK - *Offset Quadrature Phase-Shift Keying* - Modulação por Chaveamento de Fase por Quadratura com Deslocamento.

Canais: o ZigBee tem comunicações muito robustas pois opera na frequência ISM, tendo um canal na Europa, 10 canais nos Estados Unidos, e 16 canais no resto do mundo.

Compartilhamento: como o princípio do ZigBee é de uma comunicação simples, de curta duração, consumindo o mínimo de potência ele não tem compartilhamento de banda.

Acesso ao meio: o método de acesso definido no padrão é o CSMA/CA - *Carrier Sense Multiple Access with Collision Avoidance*, evitando as colisões de comunicação.

Velocidade: é possível ter a velocidade de 20 Kbps a 868 MHz, 40 Kbps na frequência de 915 MHz e de até 250 Kbps na frequência de 2.4 GHz.

Alcance: define-se como um alcance típico de 50 metros, por isso depende muito da aplicação e do consumo de potência que se quer e da duração da bateria, no caso das redes de sensores é muito importante balancear o alcance, a distância, o consumo e a velocidade.

QoS: não tem definição para a implementação de qualidade de serviços, vai depender exclusivamente da aplicação.

Deslocamento: devido ao controle de consumo o deslocamento de dispositivos não é previsto, mas depende da aplicação.

Aplicações: a aplicação onde esta tecnologia é mais usada é para a rede de sensores, mas também é usada em aplicações domésticas, aplicações médicas e outras onde se queira baixo consumo, e custo reduzido.

Observações: tecnologia muito usada em pesquisa e desenvolvimento, sobretudo em universidades devido as suas características de baixo custo e baixo consumo **e grande utilização na área de rede de sensores tendo sido base para muitas pesquisas de algoritmos de roteamento, auto configuração e economia de energia.**

A tabela 5 a seguir apresenta um resumo comparativo das tecnologias estudadas de redes locais sem fio.

Tabela 5 - Resumo das Tecnologias Pesquisadas:

Column1	802.11	HiperLAN	Infra Vermelho	Bluetooth	ZigBee
Data	1990	1991	1993	1998	2002
Identificação	Wi-Fi	HiperLAN / 2	Infravermelho	Bluetooth	ZigBee
Organização	IEEE	ETSI	IrDA	Bluetooth SIG	ZigBee Alliance
Disponibilidade	2 bilhões	poucos - Backbones	larga escala - produtos de consumo	3 bilhões	bastante - pesquisa
Enlace	NLOS	NLOS	LOS	NLOS	NLOS
Topologia	Ponto a ponto Estrela	Estrela	Ponto a Ponto	Ponto a Ponto	Ponto a Ponto Multi Ponto Estrela
Espectro	2.4 GHz e 5 GHz	5 GHz	300 GHz a 400 THz	2.4 GHz	868 MHz 2.4 GHz 915 MHz
Modulação	PSK BPSK QPSK OFDM MIMO	FSK GMSK BPSK QPSK 16QAM 64QAM	PPM EPM ASK	GFSK DPSK OFDM	BPSK OQPSK
Canais	11 Canais para o 802.11b/g/n e 12 ou 24 Canais para 802.11a	1 Canal	1 Canal	79 Canais de 1 MHz	1 Canal em 868 MHz 10 Canais em 915 MHz e 16 Canais em 2.4 GHz
Compartilhamento	Depende da Versão	TDD	Não tem	TDD	Não tem
Acesso ao Meio	CSMA/CA ou PDMA	TDMA	IrLAP	TDMA	CSMA/CA
Velocidade	1 Mbps a 600Mbps	54 Mbps	1 Mbps a 1Gbps	1 Mbps a 24 Mbps	20 Kbps a 250 Kbps
Alcance	30m a 100m	30m a 150m	0,5m a 4,5m	1m a 100m	50m
QoS	Tem	Tem	Tem	Tem	Não tem
Deslocamento	Tem 802.11r	Tem com restrições	Não tem	Entre Piconets	Não tem
Aplicações	Todos os Mercados	BackBone	Aparelhos de Consumo	Mobilidade	Pesquisa
Observações	Padrão em ambientes fechados	Bom Gerenciamento Segurança	Custo Baixo	Baixo Consumo	Pesquisa em Universidades

Tabela 5- Resumo das Tecnologias Pesquisadas

3.6 Análise dos dados da Tabela

O padrão 802.11 é a tecnologia mais antiga e tem o IEEE como organismo de padronização. Tem mais de 2 bilhões de dispositivos instalados e trabalha na faixa de frequências livres, tendo o melhor desempenho e um bom alcance. O HiperLAN/2 teve seu início em 1991 com um bom desempenho, mas hoje é mais usado para backbone de redes.

O infra vermelho tem uma grande utilização e um bom desempenho, mas tem a limitação de ser preferencialmente ponto a ponto e não permite deslocamento, porém está incluído no padrão 802.11 como uma das possibilidades para a camada física. O padrão Bluetooth como podemos verificar nos dados obtidos, é um padrão de fato com grande aceitação no mercado, com 3 bilhões de dispositivos, trabalha na faixa de frequência livre, tem um bom alcance, permite mobilidade e tem um baixo consumo. O Zigbee é muito usado em pesquisas nas universidades por causa de sua utilização nas redes de sensores, trabalha na faixa de frequências livres, tem um bom alcance, um baixo custo e consumo.

3.7 Conclusão do Estudo Comparativo

Com este estudo comparativo pode-se verificar que as tecnologias de WPAN têm evoluído muito, o que permite se ter hoje tecnologias maduras com um crescimento muito grande nas tecnologias *Zigbee*, *Bluetooth* e 802.11.

No caso do *Zigbee* houve um grande avanço nos algoritmos e protocolos de roteamento, segurança e de economia da energia utilizada.

A tecnologia *Bluetooth* tem um crescimento expressivo devido ao seu uso na telefonia celular e produtos de consumo tendo hoje um grande parque de dispositivos no mercado.

Já o padrão 802.11 teve uma evolução muito significativa devido a sua utilização na computação móvel sendo hoje uma das tecnologias que mais recebe atenção do mercado, estando disponível em praticamente todos os aeroportos e hotéis do mundo todo. Permite velocidades de até 600 Mbps estando já em estudo e desenvolvimento velocidades superiores a 1 Gbps.

Pode-se também notar algum tipo de convergência onde algumas tecnologias desenvolvidas em um padrão muitas vezes são incorporadas e utilizadas em outro padrão.

A existência de diversas tecnologias justifica-se, ao menos em parte, pela existência de aplicações nativas para cada uma delas.

Existe a possibilidade de “virtualizar” uma interface de rede sem fio, isto é, fazer com que uma única interface atenda as necessidades de aplicações originalmente desenvolvidas para diversos ambientes.

O uso desse tipo de virtualização tende a concentrar as soluções em torno das tecnologias mais usadas e de menor custo. Há dúvidas quanto à funcionalidade ampla e ao desempenho dessa solução em um ambiente no qual várias aplicações desejam utilizar a mesma rede sem fio, por isso, essas questões são abordadas na próxima seção e são objeto de estudo do laboratório desta dissertação.

4 DESCRIÇÃO DOS TESTES E RESULTADOS EXPERIMENTAIS

O desenvolvimento de programas (*drivers/softwares*) de virtualização para as interfaces de rede Wi-Fi IEEE 802.11 já foram objeto de estudos anteriores mas com diferentes focos e utilização [29] [30]. Vários grupos vêm trabalhando há alguns anos nisso, mas com o enfoque um pouco diferente, pois o intuito no passado era solucionar os problemas daquela época, ou seja, a limitação de distância, problemas de pontes (*Bridges*) e roteamento [19] [26], necessidades de expansão da infraestrutura, etc. Todos esses trabalhos, sem sombra de dúvida, serviram de base e ajuda para o desenvolvimento das interfaces de rede sem fio Wi-Fi IEEE 802.11 virtuais que se tem hoje. O foco, hoje, é a conexão simultânea com várias redes.

No mundo globalizado que se vive hoje, os sistemas, as aplicações e as pessoas precisam estar conectadas permanentemente à Internet e a uma variedade de redes de comunicação, com vários dispositivos, simultaneamente. O ideal, devido a esse contexto, seria ter um único dispositivo com uma única interface de rede e um único programa que permitisse fazer diversas conexões com diversos protocolos usados simultaneamente, tornando o sistema simples de usar e fácil de instalar e operar, conseguindo desta forma o nível de estabilidade e confiabilidade desejadas.

Existem inúmeras tecnologias de suporte às Redes de Equipamentos sem Fio de Uso Pessoal sendo que elas têm uma característica particular em comum que é a estrutura em camadas e uma divisão dos seus componentes em módulos bem definidos que com certeza possibilitam a troca e a combinação desses elementos mesmo que eles sejam de padrões e tecnologias diferentes.

Com o crescimento das técnicas de virtualização devemos ter, novas soluções de comunicação que vão, com certeza, facilitar o desenvolvimento das comunicações do futuro, por isso, escolheu-se para os testes desta dissertação a análise da solução de virtualização da interface de rede 802.11 que permite simultaneamente estar conectado a duas redes locais com endereços, características e controles totalmente independentes [28].

4.1 A interface 802.11 My WiFi

Aqui se apresenta alguns detalhes sobre a solução usada nestes testes na qual se usa interfaces de redes 802.11[9] abrindo novos caminhos para as redes sem fio pessoais WPAN [10]. A WPAN é uma rede sem fio pessoal onde os equipamentos, notebooks, câmeras, impressoras, etc., se comunicam diretamente se a necessidade de um ponto de acesso AP e a WLAN é a rede sem fio onde os equipamentos sempre se comunicam usando um ponto de acesso AP. A solução escolhida para os testes foi a “*My Wi-Fi Technology – MWT*” [31] que permite operar com conexão simultânea uma rede sem fio WLAN e uma rede pessoal sem fio WPAN a qual permite ter conectados e em uso até oito dispositivos (câmeras fotográficas, impressoras, Tocadores MP3, etc.,) de uso pessoal.

O MWT é uma solução integrada de - *firmware* - micro-código (*hardware*) e - *software- programa (driver)*, como ilustrado na figura 19, a qual permite a uma única interface de rede sem fio (placa de rede Wi-Fi modelo 5100 ou 5300) operar como se fossem duas placas independentes: uma para se conectar à infra-estrutura de rede sem fio AP – *Access Point* - e a outra para se estabelecer a rede pessoal sem fio, WPAN.

Como é uma solução desenvolvida no programa (*driver*) da placa de rede sem fio do notebook e mais algumas alterações no micro-código (*firmware*) da placa, não há o custo adicional de mais uma placa para a implementação da solução, e além disso, mantém todos os benefícios do 802.11, endereçamento IP, Qualidade de Serviços, WPS – *Wi-Fi Protected Setup* – Configuração Protegida WiFi, segurança forte WPA2, o padrão 802.11i, serviços de voz, de vídeo, de *streaming* além de todos os outros.

Figura 19 - My Wi-Fi Placa de Rede + Programas (*driver*) [31]

Fonte: Intel Wi-Fi Technology [31]

Essa solução é implementada usando-se as técnicas de virtualização, fazendo com que uma placa de rede Wi-Fi opere como se fossem duas e dessa forma, o Sistema Operacional visualiza dois endereços MACs virtuais, um é usado para se conectar à infra-estrutura de rede WLAN como STA e o outro é usado para estabelecer a conexão à rede pessoal sem fio WPAN. Todos os dispositivos Wi-Fi que estiverem no raio de alcance verão dois endereços MACs, isto é, duas interfaces de rede diferentes, como se fossem dois dispositivos diferentes e independentes.

A conexão com a rede sem fio pode ser feita na modalidade de operação de compartilhamento de banda, nela todos os dispositivos conectados à rede sem fio compartilham a mesma banda e o mesmo canal ou a modalidade de conexão sem compartilhamento de banda em que todos os dispositivos se conectam à rede sem fio em bandas e canais diferentes. Ex.: um dispositivo conecta-se usando um canal da banda de 5.2GHz enquanto outro pode estar conectado a um canal da banda de 2.4GHz ou, ainda, pode existir o modo misto que consiste no uso das duas modalidades simultaneamente.

Como se tem duas redes com endereços MAC e IP diferentes pode-se configurar os serviços de roteamento entre as duas redes sem fio, a WLAN e a rede pessoal sem fio, WPAN e também pode-se configurar e oferecer os serviços de filtro de pacotes - *fire wall* entre as duas redes.

Os dispositivos (equipamentos) que estiverem na área de cobertura podem ser associados tanto à rede sem fio WLAN, quanto à rede pessoal sem fio, WPAN, de maneira dinâmica podendo ser movimentados de uma rede para a outra como se fossem duas redes físicas distintas.

A solução foi descrita usando-se a extensibilidade da arquitetura de software, e como se pode ver na figura 20, cada uma das duas interfaces virtuais, WLAN e WPAN, possuem uma pilha independente de acesso aos protocolos TCP/IP, e uma pilha comum a todos os serviços TCP/IP (DHCP etc.) e compartilha um MUX *Driver* para poder compartilhar o programa de acesso ao hardware *Miniport Driver* e o acesso ao dispositivo físico (placa de rede Wi-Fi).

Figura 20 - Arquitetura do My Wi-Fi

Fonte: Intel my Wi-Fi Technology [31]

Como a solução foi descrita em camadas independentes, é possível escrever programas que adicionem novas funcionalidades e serviços para as redes sem fio de uso pessoal.

Qualquer dispositivo compatível com o padrão 802.11 opera de modo transparente com essa solução, já que ela foi descrita totalmente dentro dos padrões do IEEE 802.11.

A associação dos dispositivos na WLAN / WPAN pode ser feita manualmente fornecendo:

- 1) o endereço Wi-Fi – SSID;
- 2) o tipo de segurança;
- 3) o tipo de autenticação;
- 4) o nível de criptografia e a chave de criptografia, ou automaticamente, pelo uso do WPS, especificado pelo Wi-Fi Alliance que simplifica a associação de dispositivos à WPAN e que pode ser feita simplesmente pressionando um botão e fornecendo o PIN do dispositivo, quanto aos padrões de segurança, a solução aceita os padrões especificados pelo IEEE 802.11[9].

4.2 Equipamentos e Programas usados durante os testes

Equipamentos:

- 1) *notebook* com interfaces: IrDA, Bluetooth, placa de rede wi-fi 802.11 a/b/g Wifi, placa de rede ethernet 802.3, modem, USB e *FireWire* IEEE1394;
- 2) controle remoto para IrDA;
- 3) *mouse*, celular e fone de ouvido com interface sem fio Bluetooth;
- 4) máquina fotográfica, Porta-Retratos (*Picture Frame*) e Tocador de MP3 Zune com interface Wi-fi;
- 5) concentrador (hub) de dispositivos USB;
- 6) controlador de Ponto de Acesso para Internet (*Access Point*) com interface 802.11 a/b/g;
- 7) analisador de protocolos de redes sem fio;
- 8) *notebook* Lenovo T61 com processador Core 2 Duo T7300 de 2GHz, com 2GB de memória e placa de rede sem fio Intel 4965AGN com sistema operacional Windows XP da Microsoft;
- 9) *notebook* Clevo M740T com processador Core 2 Duo P7350 de 2GHz com 2GB de memória e placa de rede sem fio Intel 5300, com sistema operacional Windows 7 da Microsoft;
- 10) *netbook* modelo G10IL1 com processador Atom N270 de 1.6GHz e um 1GB de memória com placa de rede sem fio Realtek RTL8187SE com sistema operacional Windows 7 da Microsoft;
- 11) AP ponto de acesso Cisco Linksys “*Wireless Broadband Router with 4 port Switch*” modelo WRT54G;

Todos esses equipamentos, possuem interfaces de rede sem fio, compatíveis com o padrão 802.11.

Programas:

- 1) sistema Operacional Windows 7 Ultimate;
- 2) windows Media Center;
- 3) microsoft Office;
- 4) Intel Proset/Wireless Drivers para implementação do My Wifi e
- 5) *drivers* e programas dos equipamentos acima descritos.

4.3 Descrição do teste

Para os testes escolheram-se produtos de mercado e o laboratório foi preparado e montado de forma que os ensaios e a coleta dos dados se aproximassem do mundo real. A análise dos dados é usada para avaliar a tecnologia para que se tenha no fim um conjunto de informações que permita visualizar a viabilidade, as vantagens e desvantagens da tecnologia e para que isso leve a conclusão deste trabalho.

Foram feitas diversas medições em diferentes condições para se obter resultados mais precisos e de maior qualidade, visando atingir os objetivos propostos. Já que o meio ambiente tem grande influência nas redes sem fio, o laboratório deve ser montado, para fazer os testes, em ambientes diferentes, se possível.

4.4 Descrição Geral dos Testes

O objetivo dos testes é verificar a viabilidade prática da solução, analisar não apenas como funciona o compartilhamento da rede sem fio, como também se esse compartilhamento não provoca algum problema de desempenho na rede sem fio.

Quanto à modalidade de conexão, no teste, a rede sem fio usada foi a de modalidade de operação de compartilhamento de banda *single band mode* na qual, tanto os dispositivos conectados à rede sem fio, quanto os que estão conectados à rede pessoal sem fio compartilham a mesma banda e mesmo canal, isto é, se o *notebook* estiver conectado ao AP no canal 1 na frequência de 2.4GHz, os dispositivos da WPAN também estarão conectados no canal 1 na frequência de 2.4GHz.

4.5 Observações sobre o ambiente de Testes

Sempre que se trabalha com rede sem fios operando com radio frequências é importante avaliar o ambiente quanto a possíveis interferências, ruídos e barreiras. Isto é feito realizando-se antes do início do projeto um “*site survey*”, isto é, uma

pesquisa do ambiente. Quando foi iniciadoo laboratório desta dissertação foi experimentadovários ambientes e foi detectado que a virtualização da interface de rede sofre, da mesma forma que as redes não virtualizadas, em locais onde existem muitas redes e dispositivos a dificuldades de transmissão e com isso uma perda de desempenho.

Foi realizado um teste em um ambiente com grande concentração de redes sem fio e com alto tráfego e interferência e houve uma grande perda de desempenho.

Os ensaios aqui descritos foram realizados em vários ambientes domésticos, já que se trata de WPAN, com algumas redes sem fio presentes e alguns dispositivos operando na frequência livre de 2.4 GHz, mas dentro dos padrões de normalidade, sem grandes interferências e nestes ambientes não houve quantidade significativa de erros ou interferências o que permitiu obter bons resultados de desempenho.

4.5.1 Testes de Compatibilidade e Aderência

Para testar a compatibilidade e funcionalidade dos equipamentos quanto à aderência ao padrão 802.11 foram feitos testes na rede pessoal sem fio, WPAN, de transferências de fotos diretamente de máquinas fotográficas, Nikon e Samsung (esta segunda com cartão WI-FI da Eye-Fi), transferências de fotos e vídeos para um porta-retratos Digital (Picture Frame) da Dlink, transferência de fotos e músicas para um reprodutor de MP3 Zune da Microsoft e iTunes da Apple, e impressão de fotos numa impressora com interface de rede sem fio da HP Photo Smart C4700 series, todos estes testes funcionaram perfeitamente não tendo ocorrido nenhum tipo de erro.

4.5.2 Testes de Desempenho

Para os testes de desempenho estabeleceu-se como linha base (tempos base) a cópia de arquivos (vídeos) de disco para disco no *notebook* Clevo M740T, fazendo-se 10 interações para cada cópia, usando-se arquivos em disco de

diferentes tamanhos: 1MB, 3MB, 4MB, 5MB, 12MB, 25MB, 26MB, 47MB, 54MB, 100MB, 250MB, 500MB e de 1GB.

Para poder fazer a comparação, usou-se os mesmos arquivos e o mesmo número de interações descritas acima mais:

Executou-se a cópia dos arquivos do *notebook* Clevo M740T para o *netbook* G10IL1 (disco a disco) usando-se a rede sem fio WLAN, isto é, usando-se a infraestrutura de rede gerenciada pelo AP;

Os mesmos arquivos foram transferidos do *notebook* Clevo M740T para o *netbook* G10IL1 por meio da rede pessoal sem fio, WPAN, uma cópia direta, sem passar pelo AP;

Repetiu-se a cópia descrita no item b. Desta vez, porém, foi realizada enquanto existia tráfego constante na infra-estrutura WLAN. Este tráfego foi a execução repetitiva (opção t) de comandos ping de 1500 bytes do *notebook* Clevo M740T para o *notebook* Lenovo T61 e vice-versa, no tráfego por intermédio do AP.

5 RESULTADOS DOS TESTES

A tabela 6 mostra os tempos de cópia de arquivos de disco a disco dentro do mesmo *notebook*, isto é, uma cópia de arquivos dentro do mesmo equipamento sem usar a rede.

Tabela 6 - Cópia de disco-a- disco dentro do mesmo *notebook*

		PC Disco		
54 MB	100 MB	250 MB	500 MB	1000 MB
140	234	1.497	7.644	14.585
124	234	733	7.550	14.616
140	296	1.326	7.222	14.024
156	234	624	7.534	15.490
124	234	1.435	7.675	15.802
124	249	1.638	7.410	15.209
156	249	1.482	7.363	15.319
156	234	1.404	7.488	15.568
140	246	1.267	7.486	15.077

Tamanho em MB vs tempo em mm:ss.ms

A tabela 7 mostra os tempos de cópia de arquivos de um *notebook* a outro *notebook* usando a infra-estrutura de rede sem fio 802.11 WLAN passando pelo ponto de acesso AP.

Tabela 7 – Cópia de arquivos usando a WLAN

		AP		
54 MB	100 MB	250 MB	500 MB	1000 MB
40.014	1:14.287	3:10.335	6:14.244	12:25.883
40.092	1:15.051	3:09.789	6:13.807	12:26.320
40.045	1:13.897	3:10.460	6:14.525	12:26.866
40.216	1:14.614	3:09.696	6:15.570	12:26.897
40.560	1:13.788	3:11.053	6:13.792	12:26.819
40.248	1:14.739	3:10.148	6:13.499	12:27.833
39.811	1:14.708	3:11.630	6:17.146	12:30.610
40.045	1:15.160	3:10.897	6:13.402	12:29.830
40.129	1:14.531	3:10.501	6:14.498	12:27.632

Tamanho em MB vs tempo em mm:ss.ms

A tabela 8 mostra os tempos de cópia de arquivos de um *notebook* a outro *notebook* usando a rede sem fio pessoal WPAN sem passar pelo ponto de acesso AP.

Tabela 8 – Cópia de arquivos usando a WPAN

		My Wi-Fi		
54 MB	100 MB	250 MB	500 MB	1000 MB
19.110	40.060	1:29.606	2:54.283	5:06.959
19.016	35.193	1:29.599	2:53.129	5:06.866
19.234	35.521	1:29.497	2:53.441	5:07.427
19.016	35.349	1:29.715	2:53.831	5:08.254
18.907	35.287	1:29.715	2:53.316	5:08.998
18.876	35.287	1:29.653	2:53.534	5:08.005
18.938	35.380	1:29.918	2:53.160	5:07.708
18.985	35.271	1:29.559	2:53.581	5:07.193
19.010	35.919	1:29.658	2:53.534	5:07.676

Tamanho em MB vs tempo em mm:ss.ms

A tabela 9 mostra os tempos de cópia de arquivos de um *notebook* a outro *notebook* usando a rede sem fio pessoal WPAN sem passar pelo ponto de acesso AP, mas com tráfego constante na WLAN – AP.

Tabela 9 - Cópia de arquivos usando a WPAN com tráfego na WLAN

		My Wi-Fi + AP		
54 MB	100 MB	250 MB	500 MB	1000 MB
19.375	35.848	1:30.604	2:57.247	5:11.281
19.219	35.911	1:30.339	2:55.313	5:09.393
19.266	36.114	1:30.355	2:55.381	5:09.361
19.063	35.724	1:40.167	2:55.625	5:09.845
19.172	35.833	1:29.559	2:55.328	5:09.658
19.172	35.193	1:29.918	6:58.455	5:09.409
19.110	35.552	1:30.090	2:56.841	5:09.143
19.172	35.131	1:29.824	2:55.562	5:09.518
19.194	35.663	1:31.357	3:06.219	5:09.701

Tamanho em MB vs tempo em mm:ss.ms

5.1 Comparativos dos Resultados dos Testes de Desempenho

No gráfico 1 tem-se a comparação entre os tempos obtidos na cópia de disco a disco efetuada usando a rede pessoal sem fio WPAN e a cópia de disco a disco usando a rede local 802.11 WLAN através do ponto de acesso AP. Como pode se ver o tempo de cópia na WPAN é menor por que não há a retransmissão dos pacotes pelo ponto de acesso.

Gráfico 3 – Comparativo WPAN e a WLAN.

No gráfico 2 tem-se a comparação entre os tempos obtidos na cópia de disco a disco efetuada usando a rede pessoal sem fio WPAN e a cópia de disco a disco usando também a WPAN, mas com tráfego constante, ping de 1500 bytes, nos dois sentidos na rede local 802.11 WLAN através do ponto de acesso AP, como pode se verificar não houve uma perda de desempenho.

Gráfico 4 - Comparativo WPAN e WLAN com tráfego constante.

Como se pode verificar pelos dados obtidos nos testes, o desempenho da rede pessoal sem fio, WPAN, é melhor do que o da rede sem fio WLAN, por não ter de passar pelo AP (Ponto de Acesso) o que elimina um tempo de recepção/transmissão. Mesmo havendo tráfego na rede sem fio WLAN, não há um aumento significativo nos tempos de transmissão na rede pessoal sem fio, WPAN.

Isso demonstra a viabilidade desta tecnologia em ambientes residenciais e comerciais. A rede sem fio de infra-estrutura WLAN atingiu nos testes de laboratório a vazão média de 80 MBytes por minuto, enquanto a rede pessoal sem fio, WPAN, atingiu uma vazão média de 199 MBytes por minuto.

O teste deste laboratório permitiu uma avaliação positiva das redes Wi-Fi virtualizadas, a vazão oferecida por esse tipo de rede, que no laboratório foi praticamente o dobro da WLAN é totalmente compatível com as necessidades dos ambientes residenciais e comerciais de pequeno porte e o baixo custo e a

simplicidade para sua adoção fazem prever um crescimento acelerado da sua utilização.

Com se pode observar com os recursos atuais, já é possível se pensar na virtualização das interfaces de rede sem fio, nas redes sem fio pessoais WPANs, soluções que com certeza vão permitir um avanço muito grande nos equipamentos residenciais e pessoais também conhecidos por CE – *Consumer Electronics Devices* - Dispositivos Eletrônicos de Consumo.

Verifica-se também que este esquema de virtualização das interfaces de rede poderá servir de base para o desenvolvimento de trabalhos futuros, como o das redes sem fio inteligentes [14] e da agregação de dispositivos (*Device Agregation*) de uma rede sem fio pessoal.

6 CONCLUSÃO

Este trabalho permitiu comparar as principais tecnologias propostas para comunicação sem fio de curta distância genericamente conhecidas por WPAN e WLAN.

As principais alternativas, no momento são a tecnologia Wi-Fi e Bluetooth. A quantidade de equipamentos que usam essas tecnologia, 2 bilhões do caso do Wi-Fi e 3 Bilhões no caso do *Bluetooth*, é bem superior a das outras alternativas e o fato de escala favorece a redução de custos das interfaces mais usadas.

Os estudos apresentados nesse trabalho demonstrou a possibilidade de virtualizar diferentes tipos de interface em uma única interface física. Essa possibilidade compreende dois aspectos fundamentais:

- a) A funcionalidade da interface virtualizada. A solução estudada é compatível com as aplicações e com o hardware hoje usados em computadores de uso pessoal.
- b) O desempenho de 199 Mbytes por minuto da rede virtualizada com as tecnologias de transmissão sem fio disponíveis é compatível com as necessidades de banda das aplicações de acesso a Internet e de transferência de arquivos comuns nos ambientes residenciais e pessoais que na Wlan é de 80 Mbytes por minuto.

A economia de escala, multiplicada pelo efeito da virtualização das interfaces, leva a conclusão que as tecnologias Wi-Fi e Bluetooth deverão dominar o mercado de WLAN e WPAN nos próximos anos.

Tantos as WLANs quanto as WPANs continuam sendo tecnologias muito importantes para os trabalhos atuais e futuros de pesquisa e desenvolvimento nos Centros de Pesquisa e nas Universidades.

Podemos citar: “Interfaces de Redes Inteligentes”, “Agregação de Dispositivos em Redes Sem Fio”, Reconhecimento de Contextos em Redes”, “Aprendizados de Comportamentos e Uso de Redes”, “Reconhecimento de Pessoas e Objetos por Características e Comportamento na Rede”.

REFERÊNCIAS

- [1] SEGREDOS DOS CELULARES, “**Número de celulares no mundo pode chegar a 4 bilhões até o fim do ano**”, <http://www.celulares.etc.br/numero-de-celulares-no-mundo-pode-chegar-a-4-bilhoes-ate-o-fim-do-ano.html> , acesso em: 20 de agosto de 2009.
- [2] MARKET RESEARCH COM, “**Consumer Electronics Association (CEA) Market Research**”, <http://www.marketresearch.com/publisher/2340.html> , acesso em: 20 de agosto de 2009.
- [3] UNITED NATIONS MILLENNIUM DEVELOPMENT GOALS,, “**2008 Goals Report**”, www.un.org/millenniumgoals , acesso em: 10 de setembro de 2009.
- [4] FCC Regultaions, (1989), “Unlicensed ISM band”, <http://www.fcc.gov> , acesso em: 07 de maio de 2009.
- [5] Darren Waters, BBC (2008), “The best gadgets of CES 2008”, <http://news.bbc.co.uk/2/hi/technology/7173582.stm> , acesso em: 20 de agosto de 2009.
- [6] GRALLA, P. ., “**How Wireless Works**”, Ed. QUE, 2002 .
- [7] IEEE 802, (2010) “LAN/MAN Standards Committee”, <http://www.ieee802.org/> , acesso em :20 de maio de 2010.
- [8] IrDA, (2010), “**Infrared Data Association**”, <http://www.irda.org/> , acesso em: 05 de maio de 2009.
- [9] IEEE 802.11, (2010), “**Wireless Local Area Networks**“, <http://www.ieee802.org/11/index.shtml> , acesso em: 20 de maio de 2010.
- [10] IEEE 802.15, (2010), “**Working Group for WPAN**”, <http://www.ieee802.org/15/> , acesso em 20 de maio de 2010.
- [11] MALONEY , S. , “**Intel Trends & Vision Session**”, apresentação no IDF – Intel Development Forum., spring 2009
- [12] ISO 8802-11, (2010), “**Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications**”, http://www.iso.org/iso/catalogue_detail.htm?csnumber=39777 , acesso em: 20 de maio de 2010.
- [13] Wi-Fi, (2010), “**Wi-Fi Alliance**”, <http://www.wi-fi.org/> , acesso em: 20 de maio de 2010.

- [14] Kahn, K.,(2008), **“Redefining Mobility: Carry Small, Live Large”**. Research@Intel, USA <http://blogs.intel.com/research/2008/03/> , acesso em: agosto de 2009.
- [15] Geier, J., **“Wireless LANs Implementing Interoperable Networks”**, Ed. Macmillan, (1999).
- [16] Haykin, S; Moher, M., **“Sistemas Modernos de Comunicações Wireless”**, Ed. Bookman, (2008).
- [17] Nichols, R K., Lekkas P C., **“Wireless Security Models, Threats, and Solutions”**, Ed. Mcgraw-Hill, (2002).
- [18] Prasad, R; Deneire, L.,**“From WPANs to Personal Networks Technologies and Applications”**, London: Ed. Artech House, (2006).
- [19] Prasad, R; Muños, L., **“WLANs and WPANs towards 4G wireless”**, London: Ed.Artech House, (2003).
- [20] Sikora, A., **“Wireless Personal and Local Area Networks”**, Ed. Wiley, (2003).
- [21] Tanenbaum, A S., **“Redes de Computadores”**, Ed. Elsevier, (2003).
- [22] SIG Bluetooth,(2010), **“Bluetooth SIG Membership Website”** <https://www.bluetooth.org/apps/content/> , acesso em: 05 de junho de 2009.
- [23] Zigbee (2010), **“Zigbee alliance”**, <http://www.zigbee.org/> , acesso em: 10 de junho de 2009.
- [24] Pinheiro, J M S., **“As Redes com Zigbee”**, Ed. Suporte Eletronica, (2008).
- [25] Kinney P., **“Zigbee Tecnology: Wireless Control that Simply Works”**, Ed. Kinney Consulting LLC, (2003).
- [26] Misic J., Misic V. B., **“Wireless Personal Area Networks Performance, Interconnections and Security with 802.15.4”**, Ed. Wiley, (2008).
- [27] Zhao F., Gibas L., **“Wireless Sensor Networks an Information Processing Approach”**, Ed. Morgan Kaufmann, (2004).
- [28] Nickel, R. (2009), **“The second Wi-Fi revolution”** – Technology@intel, http://blogs.intel.com/technology/2009/01/the_second_wi-fi_revolution.php agosto de 2009 , acesso em: 10 setembro de 2009.
- [29] Chandra, R.; Bahl, P.; Bahl P., **MultiNet: Connecting to Multiple IEEE 802.11 Networks Using a Single Wireless Card**. IEEE Infocom, Hong Kong, http://www.cs.cornell.edu/people/ranveer/multinet_infocom.pdf , acesso em: 15 de outubro de 2009.

- [30] Chandra, R., **MultiNet: Connecting to Multiple IEEE 802.11 Networks Using a Single Wireless Card**
<http://www.cs.cornell.edu/people/ranveer/multinet/multinet/MultiNet.html> , acesso em 15 de outubro de 2009.
- [31] **Intel My Wi-Fi Technology – Tech Brief. Intel**
http://download.intel.com/network/connectivity/products/wireless/Intel_R_My_WiFi_Technology_Tech_Brief.pdf , acesso em: 10 janeiro de 2010.
- [32] Marguerite Reardon, - January 6, 2010 CNET – Highlights from CES 2010.
- [33] Kurose J F., Ross, K W., **“Redes de Computadores e a Internet”**, Ed. Pearson, (2006)..
- [34] Fiorese, V., **“Wireless Introdução às Redes de Telecomunicação Móveis Celulares”**, Ed. Brasport, (2005)..

GLOSSÁRIO

Área: A medida de uma superfície; superfície plana determinada; Extensão de terreno; Campo de ação, esfera, domínio.

POS: *Personal Operating Space* – Espaço de Operação Pessoal é o espaço ocupado pela pessoa que tipicamente se estende até 10 metros ao seu redor esteja a pessoa parada ou em movimento.

Rede: conjunto dos meios de comunicação ou de informação (telefone, telégrafo, rádio, televisão, jornais, revistas, etc.) ou o conjunto das vias (e do equipamento) de transporte ferroviário, rodoviário, aéreo, etc. que pela sua estrutura se assemelha a uma rede e se difundem em áreas mais ou menos consideráveis.

Rede Pessoal: conjunto de meios, métodos, informações, utensílios ou ferramentas interligados entre si logicamente por pertencerem e serem usados sempre pela mesma pessoa, isto é coisas que uma pessoa usa no seu dia- a- dia.

Rede: usada dentro da área pessoal é uma rede de dispositivos nós (incluindo telefone e dispositivos assistentes digitas), ligados a um computador e que estão perto da pessoa, o dispositivo pode ou não pertencer a pessoa em questão. As pesquisas sobre as PANs são tipicamente alguns poucos metros. Essas redes podem ser usadas para permitir a comunicação entre dispositivos, entre pessoas e dispositivos, pessoa a pessoa e também para servir de ponto de saída para outras redes.

Rede *Ad-Hoc*: Este termo em Latim significa “para isto”. Nas redes sem fio *ad hoc* significa uma rede na qual não existe uma topologia pre-definida, e onde não se tem controle centralizado. Os dispositivos de uma rede ad hoc se comunicam sem conexão formando a rede somente naquele momento sendo que alguns dos dispositivos participam dela apenas durante a duração da comunicação, e somente quando eles estão na área de alcance da rede.

Rede de Equipamentos sem Fio de uso Pessoal: com alcance até 10 m.(WPAN-*wireless personal área network*)

WiMAX – *Worldwide Interoperability for Microwave Access* - Interoperabilidade Mundial para Acesso por Microondas. O Forum WiMAX é uma organização liderada pela indústria sem fins lucrativos criada para certificar e promover a compatibilidade e interoperabilidade dos equipamentos de rede sem fio para banda larga baseados nos padrões IEEE 802.16 e ETSI HiperMAN.

Wi-Fi – *Wireless Fidelity* – Fidelidade em Rede Sem Fio. Do termo Hi-Fi - *High Fidelity* – Alta Fidelidade que por se tratar de redes sem fio foi adaptado para Wi-Fi. É uma organização sem fins lucrativos com o objetivo de promover a adoção de um padrão mundial único para as redes locais sem fio de alta velocidade WWW.wi-fi.org. A denominação Wi-Fi, surgiu no WECA - *The Wireless Ethernet Compatibility Alliance* – Aliança para Compatibilidade das Redes sem Fio Ethernet (*Wi-Fi Alliance*) em 1999.

ZigBee– *Zig Zag Bee* – Zigue zague das Abelhas. A aliança ZigBee é uma associação de empresas montada em 2002, que trabalham juntas, para criar uma rede sem fio de dispositivos dispersos e seguros, de baixo custo, baixo consumo, com monitoramento e controle e acredita-se que recebeu este nome porque sua arquitetura em malha lembra o Zigue Zague das Abelhas. No IEEE foi montado o grupo de estudos 802.15.4 que em maio de 2003 homologou a primeira versão do padrão.

APÊNDICES

APENDICE A - Estrutura do Grupo IEEE 802.11.

Para poder entender melhor a evolução do padrão e a tendência futura descrevemos a seguir a estrutura dos Grupos que compõem o 802.11 e os assuntos tratados em cada um deles, as datas de formação e de conclusão [9].

TG – *Working Group* - Todo Grupo de Trabalho no IEEE é composto pelas comissões permanentes - SC, grupos de tarefa - TG, grupos de estudo SG e grupos para fins específicos – *Ad-Hoc*.

TG – *Task Group* – Grupo de Tarefa - Sempre que há um novo assunto a ser discutido e tratado, um novo grupo de tarefa é formado, e fica responsável por pesquisar, estudar, avaliar, e validar o assunto e se for o caso especificar novos padrões, recomendações ou alterações de normas existentes o que é sempre feito através de um documento chamado de PAR – *Project Authorization Request* – Requerimento de Autorização de Projeto que deve ser devidamente aprovado para que o TG tenha início.

SG - *Study Group* – Os grupos de estudo são formados para investigar se existe no mercado interesse de se colocar alguma coisa específica nas normas.

SC - *Standing Committee / Ad-Hoc Committee* – Os grupos permanentes ou para fins específicos se reportam diretamente ao presidente do WG e executam trabalhos de apoio em áreas específicas.

Grupos de Tarefa TG – *Task Group* do IEEE 802.11:

Grupo TG MAC 1997 - *Medium Access Control* – Controle de Acesso ao Meio - desenvolve um método de controle de acesso ao meio comum para todas as redes sem fio para a área local em conjunto com o TG PHY.

Grupo TG PHY 1997 - *Physical Layer* – Camada Física – trabalha com três especificações de camada física para atender as aplicações que usam comunicação via luz infravermelho, comunicação com ondas de rádio de 2.4 GHz usando FHSS – *Frequency Hopping Spread Spectrum* - Espalhamento Espectral por Salto de Frequências e com ondas de rádio 2.4 GHz usando DSSS – *Direct Sequence*

Spread Spectrum - Espalhamento Espectral de Sequência Direta com velocidades de 1 e 2 Mbps em conjunto com o TG MAC.

Grupo TGA – 802.11a 1999 – desenvolve as especificações de camada física para atender as aplicações que usam comunicação com ondas de rádio UNII - *Unlicensed National Information Infrastructure* – Infra estrutura de Informação Nacional não licenciada banda de 5 GHz velocidade de 54 Mbps.

Grupo TGB – 802.11b 1999 - desenvolve as especificações de camada física para atender as aplicações que usam comunicação com ondas de rádio 2,4 GHz de alta velocidade 11 Mbps.

Grupo TGC – 802.11c 1998 – este grupo teve como finalidade escrever o padrão para O MAC de *Bridges* – Controle de acesso ao Meio para Pontes nas redes sem fio.

Grupo TGD – 802.11d 2001 – o TGD foi responsável por alterar o padrão para atender os requisitos de legislação dos países do mercado onde o padrão atual não os atendia.

Grupo TGE – 802.11e 2005 – o grupo “e” definiu as alterações na camada MAC de modo a incluir a QoS – *Quality of Services* - Qualidade de Serviços e TXOP *Transmission Opportunity* - Oportunidade de Transmissão para atender as aplicações com requisitos de qualidade de serviços.

Grupo TGF – 802.11f 2003 – neste grupo foram definidas as recomendações para a implementação do protocolo IAPP – *Inter-Access Point Protocol* – Protocolo para Intercomunicação entre Pontos de Acesso e sobretudo permitir e facilitar a intercomunicação de equipamentos de diferentes fabricantes.

Grupo TGG – 802.11g 2007 – foi no grupo g que foi feito o projeto de alta velocidade, o projeto pretendia atingir 20 Mbps, mas hoje temos o 802.11g chegando a 11 Mbps, 22 Mbps ou 54 Mbps.

Grupo TGH – 802.11h 2003 – extensão do padrão com o gerenciamento tanto para ambientes fechados – *indoor* e para ambientes abertos *outdoor* da seleção automática de canais para a frequência de 5 GHz quanto do consumo de energia permitindo no protocolo a medição e reporte.

Grupo TGI – 802.11i 2004 – aprimoramento dentro do padrão do processo de autenticação, criptografia e segurança. WEP- *Wired Equivalent Privacy* – Privacidade Equivalente ao Fio, TKIP - *Temporal Key Integrity Protocol* - Protocolo

de Integridade com Chaves Temporais, AES - *Advanced Encryption Standard* – Padrão de Criptografia Avançado.

Grupo TGj – 802.11j – 2004 – aprimoramento do padrão de 4,9 e 5 GHz para atender as normas estabelecidas no Japão.

Grupo TGk – 802.11k – 2008 – este grupo ficou responsável por definir os recursos necessários para a medição dos parâmetros de rádio para possibilitar as camadas superiores o gerenciamento e desenvolvimento de serviços como por exemplo; o deslocamento entre pontos de acesso – *Roaming* entre outros.

Grupo TGl – 802.11l – o grupo l não é usado atualmente pois foi reservado.

Grupo TGma – 802.11ma – 2007 – grupo formado para revisar e atualizar o padrão.

Grupo TGmb – 802.11ma – em atividade – Grupo formado para revisar e atualizar o padrão.

Grupo TGn – 802.11n – 2009 – definir o padrão para a rede sem fio de altíssima velocidade procurando atingir mais do que 100 Mbps, o padrão definiu velocidades de até 600 Mbps.

Grupo TGo – 802.11o – Não usado – reservado.

Grupo TGp – 802.11p – em atividade – grupo formado para definir o padrão de redes sem fio a ser usado nos veículos em movimento como por exemplo carros de passeio.

Grupo TGq – 802.11q – não usado – reservado.

Grupo TGr – 802.11r – 2008 – grupo formado para definir os procedimentos para permitir o rápido deslocamento entre pontos de acesso – *fast roaming*.

Grupo TGs – 802.11s – ativo – grupo formado para definir os procedimentos para o conjunto de serviços estendidos – ESS *Extended Service Set* para topologias em malha dentro do sistema de rede sem fio distribuídos WDS *Wireless Distribution System* para permitir mensagens com endereçamento único - *Unicast*, para grupos *Multicast* e mensagens abertas para todos *Broadcast* com auto configuração *self-configuration* para topologias com mensagens através de múltiplos pontos de acesso *multi-hops*.

Grupo TGt – 802.11t – ativo – desenvolver a metodologia e formação de medição dos parâmetros de teste e performance para permitir que as camadas superiores e as aplicações possam de forma segura prever a performance da rede e

os tempos de viagem das mensagens tanto em ambientes de teste quanto de produção.

Grupo TGu – 802.11u – ativo – definir um protocolo avançado para troca de mensagens com outras redes através do ar - *internetworking with external networks* e também permitir o desenvolvimento de aplicações que utilizem este serviço de comunicação nas camadas superiores.

Grupo TGv – 802.11v – ativo – definir protocolos, mensagens e mecanismos de gerenciamento centralizado e distribuído que permitam acessar, monitorar, configurar e atualizar as estações conectadas, AP MIB – *Access Port Management Information Base* - Porta de Acesso a Base de Informações de Gerenciamento.

Grupo TGw – 802.11w – 2009 – definir mecanismos de proteção para permitir a integridade dos pacotes de gerenciamento incluindo os pacotes de controle, de autenticação e associação.

Grupo TGx – 802.11x – não é usado – reservado.

Grupo Tgy – 802.11y – 2008 – define os mecanismos de operação para o uso e compartilhamento da faixa de frequências de 3650 a 3700 MHz nos Estados Unidos da América.

Grupo TGz-802.11z – ativo – desenvolver os mecanismos para utilização do novo DLS *Direct Link Setup* – Ativação de Enlace Direto e permitir que as estações que estejam com seção ativa no DLS entrem em estado de *Power save mode* - economia de energia.

Grupo TGaa – 802.11aa – ativo – especifica as melhorias que devem ser feitas no Controle de Acesso ao Meio para atender as necessidades emergentes para o tráfego de áudio e vídeo – streaming áudio and vídeo, sem afetar os outros tipos de tráfegos.

Grupo TGab – 802.11ab – não é usado – reservado.

Grupo TGac – 802.11ac – ativo – definir os protocolos e mecanismos para implementar altas velocidades de transmissão usando frequências acima de 6 GHz.

Grupo TGad – 802.11ad – ativo – especifica as alterações que tem que ser feitas nas camadas físicas e de controle de acesso ao meio para trabalhar com frequência de 60 GHz, banda típica de 57 a 66 GHz e com isso implementar velocidades acima de 1 Gbps

Grupo TGae – 802.11ae – ativo – define os mecanismos necessários para implementar gerenciamento e priorização de pacotes para permitir melhorias no QoS.

Grupo TGaf – 802.11af – ativo – especifica as alterações que devem ser feitas no padrão para permitir o acesso e compartilhamento a TV *White Space* – Espaço Branco (Não definido – não licenciado).

Grupos de Estudo:

Grupo de Estudo QSE – Dissolvido – Grupo formado para estudar as especificações da Qualidade de Serviços - *Quality of Services* – 802.11e as especificações feitas no WMM - *Wi-Fi Alliance Wi-Fi Multimídia* – para verificar a possibilidade de convergência e a padronização dos serviços de QoS.

Grupo de estudo QoS *Management Frames* – Finalizado – estudar os mecanismos para a implementação de gerenciamento e priorização dos frames, aprovado no 802.11ae – Tgae.

Grupo de estudo TV *White Space* – grupo de estudo formado para estudar a viabilidade de operação da TV *White Space* dentro do padrão, aprovado no 802.11af – Tgaf.

Grupo de estudo VHT *Very High Throughput* – estudar a possibilidade de aumentar a velocidade além da conseguida pelo padrão 802.11n 600 Mbps, aprovado 802.11ad – Tgad.

Grupo de estudo VTS – *Video and Audio Streaming* – estudar as mudanças necessárias no padrão para permitir a transmissão de sinais de alta qualidade de áudio e vídeo, aprovado 802.11aa – Tgaa.