

**UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE AUTOMAÇÃO E SISTEMAS**

Cassiano Valle Tartari

**ARQUITETURA HIERÁRQUICA DE COMUNICAÇÃO
PARA RASTREAMENTO DE VEÍCULOS BASEADA EM
REDES SEM FIO E SISTEMA GLOBAL DE
POSICIONAMENTO**

Florianópolis(SC)

2011

Cassiano Valle Tartari

**ARQUITETURA HIERÁRQUICA DE COMUNICAÇÃO
PARA RASTREAMENTO DE VEÍCULOS BASEADA EM
REDES SEM FIO E SISTEMA GLOBAL DE
POSICIONAMENTO**

Dissertação submetida ao Programa
de Pós-Graduação em Engenharia de
Automação e Sistemas para a
obtenção do Grau de Mestre.
Orientador: Prof. Carlos Barros
Montez, Dr.

Florianópolis(SC)

2011

Catálogo na fonte elaborada pela biblioteca da
Universidade Federal de Santa Catarina

A ficha catalográfica é confeccionada pela Biblioteca Central.

Tamanho: 7cm x 12 cm

Fonte: Times New Roman 9,5

Maiores informações em:

<http://www.bu.ufsc.br/design/Catalogacao.html>

Cassiano Valle Tartari

**ARQUITETURA HIERÁRQUICA DE COMUNICAÇÃO PARA
RASTREAMENTO DE VEÍCULOS BASEADA EM REDES SEM FIO
E SISTEMA GLOBAL DE POSICIONAMENTO**

Esta Dissertação foi julgada aprovada para a obtenção do Título de “Mestre”, e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia de Automação e Sistemas.

Florianópolis(SC), 03 de junho 2011.

Prof. Jose Eduardo Ribeiro Cury, Dr.
Coordenador do Curso

Banca Examinadora:

Prof. Carlos Barros Montez, Dr.
Presidente

Prof. Carlos Barros Montez, Dr.
Orientador

Prof. Frank Siqueira, Dr.

Prof. Jean Marie Farines, Dr.

Prof. Werner Kraus Jr., Dr.

Dedico todo o trabalho realizado nesse mestrado a minha família e amigos que sempre estiveram presentes dando suporte, e tendo a paciência de me suportar. Também dedico aqueles professores que se empenharam em sua tarefa árdua e pouco reconhecida/recompensada.

AGRADECIMENTOS

Prof. Carlos Barros Montez, pela preciosa consultoria em todos os aspectos. Pelo grande professor e grande pessoa que foi durante meu o meu mestrado.

Prof. Werner Kraus Junior, pela ajuda inestimável na estruturação do projeto, pelas ótimos conselhos e ensinados passados durante todo o meu mestrado e pela grande amizade existente.

Lurdes Bernadete Valle Tartari e Darci Antônio Tartari, meus pais, grandes incentivadores do meu estudo, exemplos de motivação para crescimento na vida e fornecedores de toda infra-estrutura necessária para que eu pudesse dedicar-me aos estudos.

A todos os meus amigos e colegas que fizeram parte da minha vida pessoal e acadêmica durante esse período de mestrado pois sem eles com certeza não teria forças suficientes para seguir em frente. Em especial aos amigos: Paulo Eduardo, Walter, Eduardo Saraiva, João Victor, Edvandro, Ríad, Toscano, Codas, Felipe e Tiago. Também gostaria de lembrar da Adele, grande amiga que sempre esteve presente para me ouvir e ajudar na tomada de decisões, amiga que considero como uma irmã.

Meus tios: Odilson e Cláudia que, além de parentes, são ótimas pessoas e de uma grande índole. Com eles formei uma enorme amizade e aprendi muito durante essa grande jornada. Não esquecendo de seus filhos, meus primos: Maria e Bruno (8 e 12 anos), os quais pude esquecer o quão séria é a vida e pude me divertir.

E a todos os professores que conheci, por terem dedicado um pouco do seu tempo e conhecimento para que eu pudesse chegar onde estou.

*A mente que se abre a uma nova ideia
jamais voltará ao seu tamanho original.*

Albert Einstein

RESUMO

As redes veiculares têm se tornado cada vez mais populares nos últimos anos, onde cada veículo constitui uma rede móvel sem fio. Esse crescimento deve-se ao fato do aumento pela exigência de mobilidade nos grandes centros. O acesso mais fácil à tecnologia tem permitido isso, visto que adquirir um veículo não é mais um ato para poucos. Com o intuito de otimizar o fluxo sem grandes modificações das malhas viárias estudos e inovações surgiram.

Neste trabalho foi feita uma proposta de uma arquitetura de comunicação hierárquica com o objetivo de combinar duas tecnologias de grande disseminação no mercado a fim de fornecer suporte a uma grande gama de aplicações de controle de tráfego urbano. Sendo a *WiFi*, a responsável pela comunicação de curtas distâncias e, a *WiMAX*, para comunicação de longa distância. Um estudo de caso, chamado *SORVES*, foi implementado em cima da arquitetura proposta, com o objetivo de monitorar visualmente veículos especiais (ambulâncias, viaturas dos bombeiros, etc.). Essa arquitetura, em sua instância mais simples, é composta dos seguintes elementos: um veículo, um *GPS*, uma unidade de processamento e um ponto *WiFi*, um *BS* e um *SS WiMAX* e uma câmera *PTZ*. Pode-se destacar no trabalho 2 contribuições: (1) comunicação *WiFi* entre veículo e ponto fixo na rodovia sem o estabelecimento de conexão; (2) a movimentação da câmera *PTZ* somente através da análise da posição enviada pelo veículo.

Palavras-chave: WiFi, WiMAX, câmera PTZ, redes veiculares, GPS

ABSTRACT

Vehicular networks have become increasingly popular in recent years where every vehicle is a mobile wireless network. This growth is due increasing demand for mobility in cities. The easier access to the technology has allowed it, since buying a car is no longer an act for a few people. So, networks studies and innovations have emerged to optimize the car flow without major changes in the infrastructure of the roads.

In this work a proposal is made for a hierarchical communication architecture in order to combine two technologies readily available in the market to provide support for a wide range of applications in urban traffic control. These technologies are *WiFi*, responsible for communication over short distances, the *WiMAX*, responsible for communication over long distances. A case study called *SORVES*, was implemented using this proposed architecture, in order to optically monitor special vehicles (ambulances, vehicles of firefighters, etc.). This architecture, in the simplest case, consists of the following elements: a vehicle, a *GPS*, a processing unit, a couple of *WiFi AP*, a *BS* and *SS WiMAX* and a camera *PTZ*. We highlight two contributions in this work: (1) the communication *WiFi* without establishing of a connection between the vehicle and a fixed point on the road, (2) the *PTZ* motion of the camera only by analyzing the position sent by the vehicle.

Keywords: WiFi, WiMAX, PTZ camera, vehicular networks, GPS

LISTA DE FIGURAS

Figura 1	Comunicação de veículos com os semáforos e destes com centrais de controle e gerência de tráfego.....	31
Figura 2	Estudo de caso da arquitetura hierárquica de comunicação proposta. A câmera <i>PTZ</i> acompanha visualmente o veículo de forma automatizada através da comunicação hierárquica com a central de controle.	32
Figura 3	Esquema ilustrativo das arquiteturas de redes veiculares.	42
Figura 4	Parte da pilha de protocolos do <i>IEEE 802.11</i>	47
Figura 5	Modelo de referência <i>OSI</i>	47
Figura 6	Arquitetura <i>ESS - Extended Service Set</i> do <i>IEEE 802.11</i> : conjunto de dois ou mais APs conectados a mesma rede cabeada. .	49
Figura 7	Arquitetura <i>IBSS - Independent Basic Service Set</i> do <i>IEEE 802.11</i> : rede sem fio formada por pelo menos duas estações.	50
Figura 8	Modo infraestruturado de operação do <i>IEEE 802.11</i>	51
Figura 9	Modo ad hoc de operação do <i>IEEE 802.11</i>	51
Figura 10	Formato geral do quadro <i>MAC</i> da <i>WiFi</i>	54
Figura 11	Modos de operação <i>LOS</i> e <i>NLOS</i> da <i>WiMAX</i>	59
Figura 12	Topologia padrão <i>IEEE 802.16</i>	61
Figura 13	Pilha de protocolos do <i>IEEE 802.16</i>	64
Figura 14	Comunicação de veículos com os semáforos e destes com centrais de controle e gerência de tráfego.....	68
Figura 15	Passos no estabelecimento de uma conexão <i>WiFi</i>	70
Figura 16	Alguns campos do pacote <i>beacon</i> do padrão <i>IEEE 802.11</i> .	72
Figura 17	Esquema ilustrativo da arquitetura hierárquica de comunicação.....	76
Figura 18	Arquitetura do veículo, através da qual as coordenadas são obtidas e transmitidas pela rede sem fio para as células de monitoramento.	80
Figura 19	Fluxo dos dados do estudo de caso da arquitetura hierárquica de comunicação. A numeração entre parênteses representa a seqüência de eventos.	82
Figura 20	Trigonometria para a rotação horizontal da câmera <i>PTZ</i> . Onde: α é o ângulo a ser calculado e d_i distância entre dois pontos.	85
Figura 21	Trigonometria para a rotação vertical da câmera <i>PTZ</i> .	

Onde: β é o ângulo a ser calculado, d e h distância entre dois pontos.	86
Figura 22 Esquemática dos elementos geométricos envolvidos na projeção de uma imagem no sensor de uma câmera através de sua lente.	87
Figura 23 Antenas <i>WiMAX</i> instaladas na UFSC para testes do <i>SORVES</i> . A antena <i>SS</i> ficou localizada no topo do <i>SeTIC</i> e a antena <i>BS</i> no topo da casa do estudante.	92
Figura 24 Antenas <i>WiMAX</i> . À esquerda a antena <i>SS</i> e à direita a antena <i>BS</i> .	93
Figura 25 Computador ligado a câmera <i>PTZ</i> realizando o papel da central de controle e monitoração, porém sem o uso da rede <i>WiMAX</i> . Os quadros <i>beacon</i> são coletados, tratados e transformados em comandos de movimentação da câmera para então receber a imagem focada pela câmera.	95
Figura 26 Câmera <i>PTZ</i> que equipa um ponto infraestruturado às margens da rodovia.	95
Figura 27 <i>Hardware</i> que equipa um veículo a ser rastreado. À direita, o roteador <i>WiFi</i> executando <i>Linux</i> embarcado; no centro, unidade de processamento responsável por coletar as coordenadas geográficas e transforma-las nos <i>SSID Frames</i> ; e, na direita, o <i>GPS USB</i> .	96
Figura 28 Roteador <i>WiFi</i> executando <i>Linux</i> embarcado. Através desse <i>firmware</i> é possível acessar e modificar a variável responsável pelo <i>SSID</i> do quadro <i>beacon</i> .	96
Figura 29 <i>GPS USB</i> responsável por fornecer as coordenadas geográficas.	97
Figura 30 Mapa com os pontos utilizados no teste do <i>SORVES</i> . As posições: 1, 2, 3 e 4 simulam o carro em movimento no sentido crescente da numeração atribuída.	98
Figura 31 Console com os quadros <i>SSID</i> formados e enviados pelos quadros <i>beacon</i> do roteador <i>WiFi</i> .	99
Figura 32 Captura dos quadros <i>beacon</i> e conseqüente extração de coordenadas para formação de comandos de movimentação para a câmera.	100
Figura 33 <i>Screenshot</i> do aplicativo responsável por obter imagens capturadas pela câmera.	101
Figura 34 Dependência entre os pacotes.	109
Figura 35 Diagrama de classe do pacote <i>camera</i> .	110
Figura 36 Diagrama de classe do pacote <i>gps</i> .	111

Figura 37 Diagrama de classe do pacote sniffer.	112
Figura 38 Diagrama de classe do pacote ssid.	112
Figura 39 Diagrama de classe do pacote outros.	113

LISTA DE TABELAS

Tabela 1 Estrutura de dados formada com as coordenadas obtidas do *GPS*. Tem por objetivo padronizar os dados enviados pela rede sem fio para os pontos infraestruturados às margens da rodovia. . . 80

LISTA DE ABREVIATURAS E SIGLAS

ABS	<i>Anti-lock Braking System</i>	67
AID	<i>Association Identifier</i>	71
AP	<i>Access Point</i>	53
API	<i>Application Programming Interface</i>	88
ASCII	<i>American Standard Code for Information Interchange</i> ..	64
ASR	<i>Anti-Slip Regulation</i>	67
BS	<i>Base Station</i>	58
BWA	<i>Broadband Wireless Access</i>	58
COM	<i>Communications - serial port</i>	43
CTS	<i>Clear To Send</i>	43
DCD	<i>Data Carrier Detect</i>	43
DS	<i>Distribution System</i>	48
DSL	<i>Digital Subscriber Line</i>	58
DSR	<i>Data Set Ready</i>	43
DSSS	<i>Direct-Sequence Spread Spectrum</i>	48
DTR	<i>Data Terminal Ready</i>	43
DVB	<i>Digital Video Broadcasting</i>	58
ESP	<i>Electronic Stability Program</i>	67
ESS	<i>Extended Service Set</i>	48
FDD	<i>Frequency Division Duplexing</i>	58
FFT	<i>Fast Fourier Transform</i>	61
FHSS	<i>Frequency-Hopping Spread Spectrum</i>	48
HR-DSSS	<i>High Rate Direct Sequence Spread Spectrum</i>	48
HTTP	<i>Hypertext Transfer Protocol</i>	42
IBSS	<i>Independent Basic Service Set</i>	48
IEEE	<i>Institute of Electrical and Electronics Engineers</i>	46
IETF	<i>Internet Engineering Task Force</i>	45
ISM	<i>Instrumentation, Scientific & Medical</i>	48
ITS	<i>Intelligent Transportation Systems</i>	29
LBS	<i>Location Based Services</i>	58
LLC	<i>Link Layer Control</i>	46
LOS	<i>Line of Sight</i>	58

MAC	<i>Medium Access Control</i>	46
MANET	<i>Mobile Ad Hoc Network</i>	41
MAN	<i>Metropolitan Area Network</i>	58
MBS	<i>Multicast and Broadcast Service</i>	58
MIB	<i>Management Information Base</i>	58
MIME	<i>Multipurpose Internet Mail Extensions</i>	64
MSDU	<i>Mac Service Data Unit</i>	54
MS	<i>Mobile Station</i>	58
NIC	<i>Network Interface Card</i>	53
NLOS	<i>Non-line of Sight</i>	58
NMEA	<i>National Marine Electronics Association</i>	41
OFDMA	<i>Orthogonal Frequency Division Multiple Access</i>	58
OFDM	<i>Orthogonal Frequency-Division Multiplexing</i>	48
OSI	<i>Open System Interconnection</i>	46
PCF	<i>Point Coordination Function</i>	51
PC	<i>Personal Computer</i>	43
PDU	<i>Protocol Data Units</i>	61
PMP	<i>Point-to-Multipoint</i>	58
QoS	<i>Quality of Service</i>	53
RI	<i>Ring Indicator</i>	43
ROHC	<i>Robust Header Compression</i>	58
RTS	<i>Request To Send</i>	57
SDU	<i>Service Data Units</i>	61
SIT	<i>Sistemas Inteligentes de Transporte</i>	39
SS	<i>Subscribe Station</i>	58
SSH	<i>Secure Shell</i>	42
SSID	<i>Service Set Identifier</i>	53
TDMA	<i>Time Division Multiple Access</i>	61
TDM	<i>Time-Division Multiplex</i>	61
UML	<i>Unified Modeling Language</i>	94
V2I	<i>Vehicle-to-Infrastructure</i>	41
V2V	<i>Vehicle-to-Vehicle</i>	41
VANET	<i>Vehicular Adhoc NETWORK</i>	41
VoIP	<i>Voice over Internet Protocol</i>	61

WAVE	<i>Wireless Access in the Vehicular Environment</i>	57
WEP	<i>Wired Equivalent Privacy</i>	53
WiMAX	<i>Worldwide Interoperability for Microwave Access</i>	31
WLAN	<i>Wireless Local Area Network</i>	46
WWW	<i>World Wide Web</i>	64

SUMÁRIO

1 INTRODUÇÃO	29
1.1 MOTIVAÇÃO	29
1.2 OBJETIVOS	31
1.3 METODOLOGIA	33
1.4 SUMÁRIO DA DISSERTAÇÃO	33
2 TRABALHOS RELACIONADOS	35
3 FUNDAMENTAÇÃO TEÓRICA	39
3.1 SISTEMAS INTELIGENTES DE TRANSPORTE	39
3.2 REDES VEICULARES	40
3.2.1 Arquitetura das Redes Veiculares	41
3.3 MEIOS DE COMUNICAÇÃO	42
3.3.1 Virtual Serial Port	42
3.3.2 SSH - Secure Shell	44
3.3.3 IEEE 802.11 - WiFi	45
3.3.4 IEEE 802.11p	57
3.3.5 IEEE 802.16 - WiMAX	58
3.3.6 HTTP - Hypertext Transfer Protocol	64
3.3.7 Sentenças NMEA - National Marine Electronics Association	65
3.4 SUMÁRIO	66
4 ARQUITETURA PROPOSTA	67
4.1 MOTIVAÇÃO DA ARQUITETURA	67
4.2 COMUNICAÇÃO <i>WIFI</i>	69
4.2.1 Procedimento de conexão do padrão IEEE 802.11 ..	70
4.2.2 Comunicação <i>WiFi</i> sem conexão	72
4.3 WIMAX	72
4.4 SUMÁRIO	73
5 ESTUDO DE CASO: <i>SORVES</i>	75
5.1 MOTIVAÇÃO	75
5.2 DESCRIÇÃO	75
5.3 <i>HARDWARE</i> E <i>SOFTWARE</i> UTILIZADOS	77
5.3.1 Hardware e equipamentos	77
5.3.2 Bibliotecas e APIs de Softwares	78
5.4 FLUXO DA INFORMAÇÃO	79
5.5 ACOMPANHAMENTO VISUAL POR CÂMERA <i>PTZ</i>	83
5.5.1 Cálculo da distância entre coordenadas geográficas .	83
5.5.2 Rotação horizontal	84

5.5.3	Rotação vertical	85
5.5.4	Zoom	86
5.5.5	Execução de Comandos	88
5.6	COMUNICAÇÃO <i>WIFI</i> SEM CONEXÃO	89
5.7	<i>WIMAX</i>	92
5.8	MODELAGEM DO PROTÓTIPO	93
5.9	TESTES DO PROTÓTIPO	94
5.10	CONSIDERAÇÕES DA IMPLEMENTAÇÃO	102
5.11	SUMÁRIO	102
6	CONCLUSÃO	103
6.1	REVISÃO DA MOTIVAÇÃO E OBJETIVO	103
6.2	VISÃO GERAL DO TRABALHO	103
6.3	CONTRIBUIÇÕES	104
6.4	TRABALHOS FUTUROS	105
	APÊNDICE A – Diagramas de classe	109
	Referências Bibliográficas	115

1 INTRODUÇÃO

Neste Capítulo são apresentadas a motivação e as contribuições pretendidas com esse trabalho. A estrutura do documento é apresentada na sequência.

1.1 MOTIVAÇÃO

Atualmente o transporte tem uma influência direta e uma importância vital no desenvolvimento econômico e social de uma sociedade moderna, onde há um aumento de exigência no nível da mobilidade crescente. É essa exigência de mobilidade que tem feito, nas últimas cinco décadas, com que o número de veículos aumente em circulação. Esse aumento resultou em uma saturação das vias que, principalmente em centro urbanos, não possuem mais espaço físico para a expansão. A ocorrência frequente de congestionamentos, acidentes e atrasos nos deslocamentos tem como consequências o aumento da poluição provocada pela emissão de gases, aumento dos ruídos o que levam a problemas de saúde, insegurança física e psicológica, diminuição da qualidade de vida da população.

Esta crescente demanda por serviços de transportes, seja de pessoas ou de carga, aliado aos elevados custos de construção de novas infra-estruturas tem levado gestores de sistemas de mobilidade e logística a buscar formas de gerenciamento eficiente dos recursos de transportes disponíveis. Nesse contexto, tem havido um rápido desenvolvimento de aplicações das tecnologias de informação e comunicação nos diferentes modos de transporte, dando origem à área conhecida por *ITS (Intelligent Transportation Systems)* (BAZZAN; KLÜGL, 2007). Exemplos de tais aplicações são a monitoração e o controle de tráfego em tempo real (LOUREIRO; GOMES; LEANDRO, 2002), operação automatizada de transporte público (SILVA, 2000), e integração de sub-sistemas diversos (gerência de construção e manutenção, gerência de tráfego, operação de fretes urbanos, etc.) (ALVES et al., 2009).

Um dos elementos centrais no rápido avanço dos *ITS* é o barateamento e a disponibilidade de tecnologias de comunicação sem fio, uma vez que as aplicações de transporte ocorrem em locais onde nem sempre se dispõe de linhas de comunicação com largura de banda suficiente para as demandas de comunicação. Considerando, ainda,

que há espectro de frequência disponível para aplicações não tarifadas tanto de curto como de longo alcance, torna-se interessante investigar o potencial de uso de tipos abertos de comunicação sem fio em aplicações de transportes.

Com base nas considerações acima, este trabalho investiga questões técnicas relativas ao emprego de tecnologias de comunicação sem fio para gerência de tráfego. Em particular, são examinadas as técnicas de *WiFi* (IEEE 802.11) (IEEE, 2010) e *WiMax* (IEEE 802.16) (IEEE, 2003) e seu potencial uso na monitoração e controle do tráfego urbano (ALVES FEHMI B. ABDESSLEM, 2008; CAVALCANTI, 2008). Um cenário de aplicação é mostrado na Figura 1, que ilustra a necessidade de comunicação de veículos com os semáforos e destes com centrais de controle e gerência de tráfego. Os protocolos sugeridos para este estudo foram escolhidos pela ampla disseminação de equipamentos e de documentação.

Através de um estudo de caso de um problema de rastreamento de veículo especial através de câmera de vídeo, são analisadas as características dessas tecnologias para avaliação de seu uso na comunicação entre equipamentos de campo e centrais de controle de tráfego.

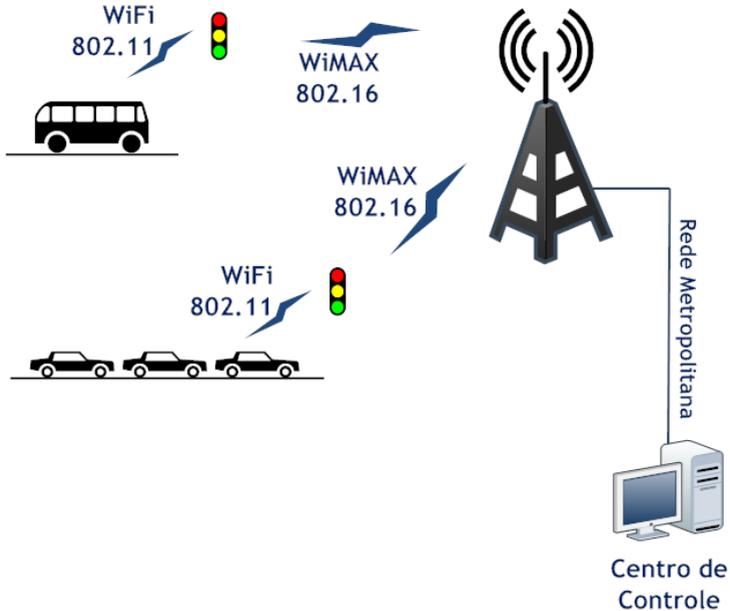


Figura 1: Comunicação de veículos com os semáforos e destes com centrais de controle e gerência de tráfego.

1.2 OBJETIVOS

Propor e testar uma arquitetura de comunicação hierárquica para aplicações de controle e monitoração de tráfego urbano (Figura 1). Essa arquitetura é composta por equipamentos que usam os protocolos 802.11 (*WiFi*), 802.16 (*WiMAX*) e 802.3 (*Ethernet*).

A arquitetura prevê uma organização hierárquica, cujas informações sobre os veículos monitorados são coletadas em células espalhadas pela cidade; sendo, então, reunidas e reenviadas para uma central de controle e monitoração remota.

Na Figura 2 é ilustrado graficamente um estudo de caso realizado sobre essa arquitetura. Pretende-se, através dessa arquitetura, rastrear veículos especiais como, por exemplo, ambulâncias, viaturas dos bombeiros etc. através de uma câmera com controle de *zoom*, movimentos horizontais e verticais (câmera *PTZ*). Também pretende-se estudar a comunicação entre veículo e câmera através do *WiFi*. Esses veículos serão acompanhados visualmente por

meio de informações de posicionamento geográfico enviados à câmera de uma maneira autônoma. Vários pontos fixos à beira da estrada, com boa visibilidade da via, estarão equipados com câmeras *PTZ*.

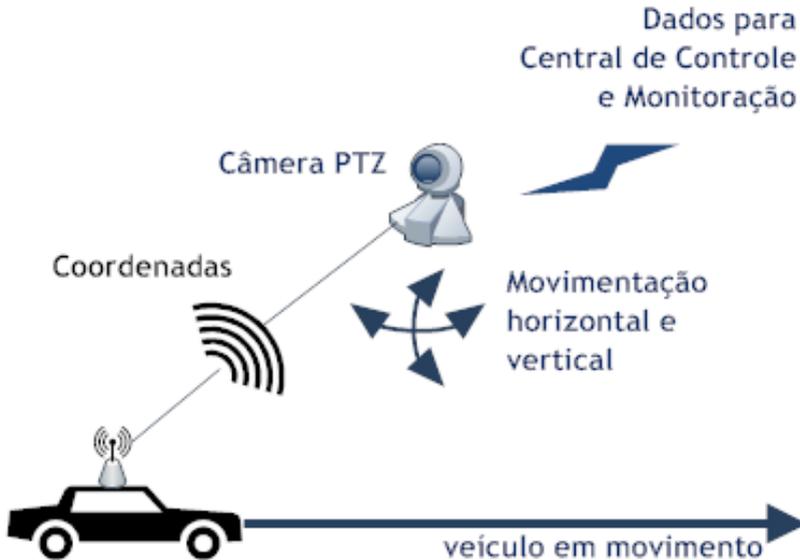


Figura 2: Estudo de caso da arquitetura hierárquica de comunicação proposta. A câmera *PTZ* acompanha visualmente o veículo de forma automatizada através da comunicação hierárquica com a central de controle.

A estrutura consiste de um *Access Point WiFi*(802.11) conectado a um roteador, a esse roteador também um câmera *PTZ* e um rádio *WiMAX*(802.16), todo o *gateway* realizado por *Ethernet*. Esse rádio *WiMAX* faz parte de uma antena *SS*(*Subscriber Station*) a qual se comunicará por *LOS*(*Light Of Sight*, linha visada) com uma antena *BS*(*Base Station*) que estará ligada a um servidor central. Também fazem parte da lista de equipamentos um *Access Point WiFi* móvel e um *GPS*. Através dessa arquitetura busca-se estudar a viabilidade do fluxo de dados para o uso no controle do tráfego urbano.

1.3 METODOLOGIA

Para mostrar a viabilidade da arquitetura foi criado um sistema que, através da análise dos pacotes recebidos por *WiFi*, contendo dados extraídos de um *GPS*, posicionará o emissor de pacotes no centro da cena de uma câmera. Essa câmera ficará fixada próxima a uma via em ponto estratégico de forma que o emissor possa se movimentar e a câmera acompanhar seus movimentos. Esse emissor de pacotes poderá ser desde uma simples pessoa com um celular com *GPS* e *WiFi* até um veículo equipado com esse hardware, cujo o objetivo primordial é acompanhar veículos especiais nas vias de tráfego. As imagens obtidas serão transmitidas para o servidor da central de monitoração utilizando *WiMAX*.

1.4 SUMÁRIO DA DISSERTAÇÃO

Essa dissertação está estruturada da seguinte forma. No Capítulo 2 foi feita uma revisão de todos trabalhos relacionados e que serviram como contextualizadores do que está sendo trabalhado na área.

O Capítulo 3 faz um embasamento teórico de assuntos importantes para o entendimento do trabalho desenvolvido como: os meios de comunicação utilizados: serial, *SSH*, *WiFi*, *WiMAX*, *HTTP* e *NMEA 0183*.

No Capítulo 4 é realizada a descrição da arquitetura proposta no trabalho e mostra o seu funcionamento. Nele são descritos todos os módulos do projeto, fluxo da informação e cálculos de movimentação da câmera.

Já no Capítulo 5 questões técnicas da implementação da arquitetura e desenvolvimento da aplicação de teste são abordadas.

Por último, o Capítulo 6, aborda uma revisão da motivação e objetivo, assim como uma visão geral do trabalho e suas contribuições, finalizando com trabalhos futuros.

2 TRABALHOS RELACIONADOS

A tecnologia IEEE 802.11 foi projetada para cenários de baixa mobilidade. A vantagem encontra-se na questão de que, independentemente de como os pontos de acesso *WLAN* são gerenciados, eles podem prover acesso à Internet e com um custo benefício efetivo. Porém esse acesso é fortemente limitado pela cobertura da geografia local e ambientes fechados. (OTT; KUTSCHER, 2004) lançaram um artigo que foi base para muitos outros trabalhos no que diz respeito a comunicação sem fio de usuários móveis. Nesse trabalho é realizada a primeira pesquisa detalhada a respeito da viabilidade de se fornecer conexão à rede e, conseqüentemente Internet, através do protocolo IEEE 802.11 para usuários móveis em veículos.

No trabalho de (OTT; KUTSCHER, 2004) foram feitas medições nas transmissões de grande quantidades de dados, tanto de envio como de recebimento, usando *UDP* e *TCP* em *SIT*. Essas medições foram feitas entre veículos, movendo-se em diferentes velocidades, e pontos de acesso próximos a rodovia. Foram também discutidas as limitações dessa comunicação em tais cenários para aplicações de alto nível.

(GASS; SCOTT; DIOT, 2006) mostraram que uma antena de um *laptop* pode suportar a comunicação da rede sem fio com o usuários em movimento com desempenho satisfatório. Também foi examinado o alcance da rede, isto é, o tempo e a distância quando o cliente pode se associar à rede, e o real alcance utilizável. Foi analisada a viabilidade do uso de aplicações correntes em tais cenários. Por último, foram realizados uma alta quantidade de testes do que em estudos anteriores para obter maior confiança nos resultados. Velocidades entre 5 mph a 75 mph foram testadas junto a um *AP* IEEE 802.11b. Também em 2006, (HEMPEL et al., 2006) executou testes parecidos porém com a comunicação feita entre um trem em movimento e um *AP*.

Outro trabalho (BYCHKOVSKY et al., 2006) averiguou a possibilidade de realizar conexões com a Internet somente através do acesso a *AP* de rede aberta encontrados na área metropolitana de Boston. Foram coletados dados a partir de 290 horas de alguns veículos dirigindo em condições típicas. Através de uma simples otimização de aquisição de *IP* foi possível obter alguns resultados relevantes. A duração média das conexões foi de 13s, a velocidade média de envio de dados foi de 30 KBytes/s, e a duração média entre conexões de sucesso foi de 75s. Como em outros trabalhos, a

conclusão foi de que é possível ter uma grande variedade de aplicações usando redes *WiFi* populares, principalmente as que permitem conexões intermitentes.

(NAVDA et al., 2007) estudou o uso de antenas direcionais e técnicas de direção de feixe para melhorar o desempenho das conexões IEEE 802.11 no contexto da comunicação entre veículos em movimento e *APs* fixos às margens da via. Para isso foi desenvolvida uma ferramenta chamada de *MobiSteer*. O objetivo dela é selecionar o melhor *AP* e combinação de feixes em cada ponto durante a condução do veículo dadas as informações disponíveis, para que a taxa de transferência possa ser maximizada. Extensivos testes foram realizados utilizando uma antena comercial composta por 8 antenas e comparados com resultados obtidos por uma antenas simples.

Também em 2007, (WELLENS; WESTPHAL; MAHONEN,) estudou o desempenho do IEEE 802.11a, 802.11b e 802.11g em comunicações entre veículos e também entre veículos e pontos estruturados às margens da rodovia. Uma conclusão importante obtida foi que a velocidade dos veículos tem um impacto insignificante até a velocidade testada de 180 km/h. Também foi mostrado que a adaptação da frequência do rádio pode ser melhorada ao reagir mais rapidamente às condições de mudança de canal e que a distância de carro para carro e disponibilidade de linha de comunicação de vista são os fatores de desempenho mais importantes.

(HADALLER et al., 2007), estudou o acesso à Internet por veículos móveis através da comunicação com *AP* à beira da via. Três importantes contribuições foram feitas: (1) Experimentalmente demonstraram que, na média, os protocolos atuais só alcançam 50% da taxa de transferência possível do cenário. (2) Eles quantificaram os efeitos dos problemas que causa essa perda de taxa de transferência. (3) Fizeram recomendações das melhores práticas para essas conexões oportunistas. A grande limitação desse trabalho foi que seus autores só executaram testes em um simples cenário: um veículo, uma velocidade, um ambiente, uma placa de rede sem fio e somente transferências de dados em uma via, *downlink*. Com relação aos problemas que causam a redução da taxa de transferência foram quantificados os seguintes percentuais: (a) Fase de acesso: 7,5% a 22,8% de redução na taxa de transferência devido ao processo de seleção de *AP*, tempo alto de gerenciamento de *MAC*, tempo de *ARP* e outros. (b) Fase de produção: até 75% menos de dados seriam transmitidos se fosse utilizado o algoritmo de seleção de taxa do *MAC* no *driver* do *AP* usado. E 16 a 23% menos dados foram transmitidos

devido à vagarosa adaptação da taxa *MAC* no lado do cliente.

(BALASUBRAMANIAN et al., 2007) adaptou o processo interativo de pesquisa na web e restabelecimento para as redes veiculares com acesso intermitente à Internet. Desenvolveram um sistema chamado *Thedu* no qual os usuários móveis fazem requisições a um *proxy* de Internet que pré carrega as páginas em seu servidor e as armazena. Então o usuário pode acessá-las assim que sua conexão com a Internet estiver disponível. Outra funcionalidade do *Thedu* é um conjunto de técnicas que são aplicadas para priorizar o *download* das páginas web pré carregadas evitando assim a perda de banda com respostas que normalmente são inúteis.

(ERIKSSON; BALAKRISHNAN; MADDEN, 2008a) desenvolveu um sistema chamado *Cabernet*. Trata-se de um sistema para troca de dados entre veículos e *AP* encontrados durante a movimentação do veículo usando redes abertas 802.11 (*WiFi*). Duas contribuições importantes podem ser citadas nesse trabalho, a primeira trata-se da implementação do *QuickWiFi*, que é uma otimização do processo de estabelecimento de conexão com o *AP*. Com esta ferramenta foi possível obter um tempo médio de conexão de 400 ms em oposição à média de 10 s quando se está usando o padrão puro IEEE 802.11. A segunda contribuição foi o *CTB* (*Cabernet Transport Protocol*) que melhora o desempenho do controle de congestionamento do *TCP* para conexões oportunísticas.

A motivação para a pesquisa de todos esses trabalhos citados focou-se na tentativa de otimização do tempo para que um cliente se associe a um *AP* através do IEEE 802.11. Por testes realizados em laboratório, constatou-se o mesmo tempo que foi obtido em muitos trabalhos, um tempo médio para conexão de 10 s. Em todos trabalhos citados onde houve otimização de *drivers* ou software não ficou claro como reproduzir a técnica e seus trabalhos não poderiam ser replicados. Uma exceção foi o trabalho de (CHANDRA et al., 2007), não citado acima, no qual em 2007 estudou a possibilidade de realizar uma comunicação de baixa banda sobre o IEEE 802.11 sem que houvesse o estabelecimento de uma conexão. Esse tipo de comunicação é ideal para os objetivos do projeto da dissertação, no qual apenas coordenadas geográficas e mais alguns identificadores são enviados pela rede sem fio.

Esta técnica de comunicação sem associação foi denominada de *beacon-stuffing*. Trata-se da troca de dados utilizando o quadro *beacon*, quadros que os *APs* utilizam para anunciar a sua presença. Alguns campos do quadro *beacon* são facilmente sobrecarregados e

assim dados possam ser transportados. No lado do cliente, os quadro de resposta, *Probe Response frames*, são sobrecarregados para enviar dados. Porém para a implementação total da ideia contida nesse trabalho seriam necessárias modificações em *drivers* de placas de rede. Como a comunicação do projeto da dissertação necessita de apenas um sentido do fluxo da informação, isto é, do veículo em movimento para pontos IEEE 802.11 fixos às margens da rodovia, uma técnica foi proposta e implementada neste trabalho. Em nossa proposta, apenas o campo do *SSID* é sobrecarregado para o transporte de dados. No Capítulo 4 será descrito em detalhes como esse tipo de comunicação foi implementado.

3 FUNDAMENTAÇÃO TEÓRICA

Este capítulo trata sobre temas e tecnologias necessárias ao entendimento do trabalho realizado. Começa com a definição de Sistemas Inteligentes de Transporte, seguida da definição de redes veiculares, junto da contextualização no cenário atual dessas redes. Também trata dos protocolos utilizados na arquitetura proposta e dos meios de comunicação utilizados.

3.1 SISTEMAS INTELIGENTES DE TRANSPORTE

A mobilidade tornou-se um aspecto primordial na vida da maioria dos cidadãos. Atualmente os congestionamentos possuem um alto custo a qualquer economia, podendo ter quilômetros de extensão dentro de um cidade e levar horas para percorrê-lo. No caso do transporte veicular, em particular, é notório que a demanda por mobilidade é uma das características da nossa sociedade. De fato, relatórios recentes da Organização das Nações Unidas e da União Europeia mostram que a demanda por serviços, comércio e viagens pessoais cresce ano a ano colocando desafios inéditos à área de transportes. O impacto direto e indireto dos congestionamentos em áreas urbanas e interurbanas é imenso e resulta em custos que podem atingir até 1% do PNB (FIGUEIREDO, 2005; BAZZAN; KLÜGL, 2007).

No Brasil, estes números não devem ser muito diferentes a se julgar pela seguinte notícia, retirada do portal de notícias G1 (edição online de 7 de agosto de 2008): “Lentidão chega a 194 km e SP continua em estado de atenção” (G1, 2008).

Nesse contexto surgiu a necessidade de automatizar a coleta de dados e processamento desses através de várias tecnologias. Esses sistemas foram então denominados genericamente de Sistemas Inteligentes de Transporte (SIT) e nessa área encontram-se as redes veiculares. Resumidamente, pode-se dizer que os SIT utilizam as tecnologias da informação, comunicação e controle para melhorar o desempenho e a eficiência das operações da rede de transporte e, além disso atravessam áreas como os transportes, a engenharia, as telecomunicações, o comércio eletrônico, as finanças e a indústria automobilística. Esta natureza multidisciplinar aumenta a complexidade do problema porque requer o interesse e cooperação

entre várias áreas (FIGUEIREDO, 2005).

Basicamente os SIT são compostos por condutores de veículos inteligentes e vias de comunicação (estradas) com o objetivo de proporcionar maior conforto, segurança e preservar o meio ambiente. Hoje em dia é relativamente aceita a hipótese de que os SIT estão entre os investimentos com melhor relação custo-benefício em transportes. Tais investimentos podem envolver desde sistemas avançados de informação ao motorista – difusão de informação via rádio, telefone e internet, painéis de mensagens, quiosques de informação, dispositivos instalados nos veículos e *personal assistants* (BAZZAN; KLÜGL, 2007). Por exemplo, os SIT tornam possível a implementação de um determinado número de regras e processos governamentais de uma forma mais econômica, ferramentas de aquisição de dados das vias de comunicação terrestres, melhoram a produtividade através da redução de tempos, dos custos de operação, do consumo de energia e do aumento da segurança (FIGUEIREDO, 2005).

3.2 REDES VEICULARES

As redes veiculares são formadas por sistemas de comunicação entre veículos. Cada veículo dessa rede constitui um nó. Os nós podem comunicar-se entre si ou com pontos infraestruturados às margens de ruas e estradas. Esses nós apresentam alta mobilidade e trajetórias que acompanham os limites das vias públicas de acesso (ALVES et al., 2009).

Redes veiculares estão entre os mais significativos e desafiadores sistemas modernos de comunicação. Tanto a academia quanto a indústria estão extremamente ativos nessa área de pesquisa e avanços fundamentais são esperados para ocorrer nos próximos anos. Um fator importante no sucesso dessas redes, como área de pesquisa, é o impacto que aplicações nesse contexto produzem no dia-a-dia das pessoas (ALVES et al., 2008).

As redes veiculares possuem uma série de desafios para sua adoção em larga escala. Dentre os principais desafios estão particularidades como a alta mobilidade dos nós, o dinamismo dos cenários e a escalabilidade em termos do número de nós. A perda de conectividade durante a transmissão dos dados e o tempo reduzido em que dois nós permanecem em contato são outros desafios. Nesse cenário, os protocolos criados para outras redes sem-fio, como as redes

móveis *ad hoc* (*MANETs*), não são adequados.

3.2.1 Arquitetura das Redes Veiculares

A arquitetura das redes veiculares define a maneira com é feita a organização dos nós e como é feita a comunicação entre eles. Atualmente, existem três arquiteturas principais: *ad hoc* puro (*Vehicular Ad hoc NETWORK* - VANET), infraestruturada ou híbrida (ALVES et al., 2008). Na arquitetura *ad hoc*, os veículos comunicam-se entre si sem a interferência de um elemento externo. Para isso, os veículos funcionam como roteadores de dados e encaminham esses dados através de múltiplos saltos entre os nós. Embora essa seja a configuração estrutural mais simples, ela tem como principal desvantagem a dependência com relação à densidade da rede para que haja conectividade e para que o fluxo de dados possa ocorrer.

Para evitar estes problemas de conectividade, a arquitetura infraestruturada trabalha com a ideia de nós estáticos distribuídos ao longo das vias. Esses nós estáticos centralizam todo o tráfego de dados da rede, servindo como nós intermediários das comunicações. A vantagem do modo infraestruturado é o aumento da conectividade e a possibilidade da comunicação com outras redes, como por exemplo, a Internet, através de um cabeamento ou até alguma tecnologia sem fio como a *WiMAX*. No entanto, a conectividade da rede só é garantida com um grande número de elementos fixos nas vias, o que pode inviabilizar a ideia devido ao possível alto custo.

Ainda existe a arquitetura híbrida que trata-se de um solução intermediária entre as duas anteriormente expostas: *ad hoc* puro e infraestruturada. Na arquitetura híbrida, uma infraestrutura bem menor é utilizada para aumentar consideravelmente a conectividade da rede e prover serviços como os de interconexão. Entretanto, há também a possibilidade dos veículos se comunicarem por múltiplos saltos. Nas redes veiculares, o modo *ad hoc* é conhecido por *V2V* (*Vehicle-to-Vehicle*) e o modo infraestruturado tem como sinônimo o termo *V2I* (*Vehicle-to-Infrastructure*). Atualmente, alguns pesquisadores referem-se às redes veiculares em geral como *VANETs*, mesmo quando existe infraestrutura. A Figura 3 ilustra as 3 arquiteturas comentadas.



Figura 3: Esquema ilustrativo das arquiteturas de redes veiculares.

3.3 MEIOS DE COMUNICAÇÃO

Nessa sessão será feita uma apresentação técnica dos meios de comunicação utilizados na arquitetura proposta na dissertação. Inicia-se com comunicação serial, seguida do protocolo de rede SSH (*Secure Shell*), *WiFi*, *WiMAX*, *HTTP* e terminando com as sentenças *NMEA*.

3.3.1 *Virtual Serial Port*

Uma *Virtual Serial Port* é uma emulação do padrão da porta serial. Essa porta é criada via *software* que habilita portas seriais extras no sistema operacional sem a instalação *hardware* adicional (como, por exemplo, cartões de expansão). Ao contrário de uma porta serial física, a virtual pode receber qualquer nome (COM255, VSP33, TTYS0 etc.). É possível criar um grande número de *Virtual Serial Ports* em um computador. A única limitação são os recursos, tais como a memória disponível no sistema e a capacidade de processamento, necessários para emular muitas portas seriais ao mesmo tempo.

Virtual Serial Port emula todas as funcionalidades da porta serial padrão, incluindo taxa de transmissão, bits de dados, bits de paridade e bits de parada. Adicionalmente elas controlam o fluxo de dados, emulando todos as linhas de sinais

(*DTR/DSR/CTS/RTS/DCD/RI*) e customização de pinagem. *Virtual Serial Ports* são comuns com *Bluetooth* e são a forma padrão que os sistemas operacionais usam para receber dados de módulos *GPS*.

Serial Port

Uma porta serial é uma interface do computador que transmite dados 1 bit por vez. Em um uso comum, o termo “porta serial” refere-se a portas que usam um protocolo assíncrono específico. Essas portas incluem as portas *RS-232* nos *PCs* e muitas portas seriais em sistemas embarcados. A maioria das portas seriais são *duplex*: elas podem tanto enviar como receber dados. Transmitir 1 bit por vez é ineficiente mas apresenta vantagens.

Nos *PCs*, aplicações acessam a maioria das portas seriais como as portas *COM*. Existem alguns dispositivos *USB* que funcionam como uma porta virtual *COM* que aplicações podem acessar da mesma maneira que uma porta física serial, como já descrito. Alguns dispositivos *WiFi* e *Ethernet* possuem a função de servidores seriais o que habilita aplicações a acessarem portas seriais pela rede.

Microcontroladores em sistemas embarcados podem usar portas seriais para se comunicar com outros sistemas embarcados e *PCs*. Os compiladores de linguagens para microcontroladores frequentemente fornecem bibliotecas com funções para simplificar a programação da porta-serial (AXELSON, 2007).

Essas são algumas das vantagens da programação de portas seriais assíncronas e portas *COM*:

- Portas seriais podem ser usadas para se trocar praticamente qualquer tipo de informação. Aplicações para portas seriais frequentemente envolvem leitura de sensores, relés, *displays*, ou outros dispositivos de entrada.
- O *hardware* é de baixo custo e facilmente acessível. *PCs* que não possuem portas seriais embutidas podem usar adaptadores *USB/serial*.
- Apenas os bits *Start*, *Stop* e um bit de paridade (opcional) são adicionados a cada *byte* transmitido. As interfaces seriais não interferem com os dados a serem transmitidos. Em contraste, *USB* e *Ethernet* usam protocolos sofisticados que definem o formato dos dados a serem transmitidos. *Hardware* ou *firmware*

necessitam implementar esses protocolos, adicionando complexidade que algumas aplicações não necessitam.

- Os sistemas operacionais fornecem os *drivers* para os dispositivos que precisam acessar as portas COM. As linguagens de programação fornecem também classes, bibliotecas e outras ferramentas para comunicação com portas COM.
- Um dispositivo *USB* acessado com uma porta *COM* não necessita ter um interface serial assíncrona. O dispositivo pode ter uma interface paralela ou outra interface como a aplicação necessitar.
- Tecnologias sem fio permitem transmissão de dados seriais (AXELSON, 2007).

No entanto, a comunicação serial apresenta também algumas limitações:

- Os computadores em cada extremidade precisam converter os dados seriais transmitidos para dados paralelos antes de enviá-los para o barramento de dados e *CPU*. A conversão é normalmente controlada automaticamente por *hardware*.
- A taxa máxima de transmissão especificada no padrão *RS-232* é de 20 kbps. Porém muitos circuitos de interface podem exceder essa taxa. O padrão *RS-485* suporta velocidades acima de 10 Mbps. Comunicações entre *PC* e as portas *USB Virtual COM* não são limitadas pelas taxas do padrão *RS-232* (AXELSON, 2007).

3.3.2 *SSH - Secure Shell*

O protocolo *SSH* fornece segurança no envio e recebimento de pacotes na rede. Toda a conexão é criptografada e há criação de um tunelamento cliente-servidor, onde não é possível se espionar as informações transmitidas (YLONEN, 1996).

O *Secure Shell* oferece ao usuário a capacidade de conectar-se remotamente a outro computador com segurança, tendo em vista que todos os dados utilizados na rede serão criptografados, impedindo a compreensão destes por outros usuários, ao contrário do *Telnet* que transmite em texto puro.

A primeira versão do protocolo *SSH*, o *SSH-1*, foi desenvolvido em 1995 por Tatu Ylönen, um pesquisador da *Helsinki University of*

Technology na Finlândia. Depois que a rede da universidade foi atacada por um espião de senhas (*Password-Sniffing*), Ylönen iniciou o desenvolvimento e os testes de um software que desse suporte ao protocolo *SSH-1* para uso próprio (BARRETT; SILVERMAN, 2001).

A *Internet Engineering Task Force (IETF)* posteriormente liberou o *SSH-2*, segunda versão do protocolo *SSH*, que melhorou a segurança e a funcionalidade do seu antecessor.

O protocolo *SSH* tem como principal finalidade o login remoto, porém pode ser utilizado como túnel criptográfico para outros propósitos, como copiar arquivos, criptografar conexões de e-mail e execução de programas remotos (SILVA; CASAGRANDE, 2010).

Arquitetura Cliente-Servidor *Secure Shell*

Um servidor *SSH* permite que vários clientes *SSH* conectem-se a ele. O servidor *SSH* executa um serviço de escuta, normalmente na porta 22 de uma conexão *TCP*. No entanto, estas e outras definições podem ser alteradas em um arquivo de configuração. O Cliente *SSH* precisa conhecer o endereço *IP* (ou *hostname*) do servidor *SSH* e a porta que ele está escutando, assim o cliente só precisa se autenticar para ter acesso à sessão.

O processo de conexão do *SSH* é efetuado em três passos: primeiro o cliente *SSH* envia o pedido de autenticação para o servidor *SSH*. Nesta primeira ligação, o cliente recebe uma chave de *host* que será utilizada nas próximas conexões para verificação de servidor; no segundo passo o servidor *SSH* determina se o cliente será autorizado a conectar-se com o servidor, verificando o usuário e senha que o cliente forneceu na requisição; se o servidor *SSH* autenticar o cliente e o mesmo estiver autorizado, a sessão *SSH* começa entre os dois *hosts* (SILVA; CASAGRANDE, 2010).

3.3.3 IEEE 802.11 - *WiFi*

O protocolo IEEE 802.11 e seus esquemas de transmissão são umas das realizações mais notáveis da normalização da tecnologia e protocolos de comunicação via redes sem fio. Um incontável número de dispositivos hoje são baseados nesse padrão. O protocolo começou como uma extensão sem fio para redes locais em 1997, e desde então tem sido gradualmente melhorada e estendida para uma tecnologia muito flexível e bem compreendida. O 802.11 foi construído para

sistemas de rádio frequência em um espectro sem licença, não existe nenhuma limitação virtual para o uso do 802.11: o espectro sem licença é frequentemente aceito no mundo todo, isto é, esses sistemas de rádio frequência podem ser utilizados em qualquer localidade e a qualquer hora. Por causa de sua simplicidade, o protocolo 802.11 é o padrão dominante para sistemas comerciais de rede sem fio. A comunidade de pesquisa frequentemente adota este padrão em seus experimentos e protótipos.

O *IEEE* publicou o padrão oficial IEEE 802.11 em 1997 com a especificação da camada de transporte e a camada *MAC* para redes locais sem fio (WLANs). Uma versão revisada com maior precisão foi lançada em 1999. No mesmo momento, 802.11a e 802.11b, os quais são os primeiros sub padrões a estender o 802.11, foram publicados em paralelo em 1999. O *IEEE Wireless Lan Edition* é uma compilação dos padrões 802.11, 802.11a e 802.11b (*IEEE*, 2003a). Atualmente o padrão 802.11 está dividido em muitos sub padrões, cada um endereçado particularmente. Através desses diversos conjuntos de melhoras incrementais, o 802.11 continua evoluindo em diferentes direções devido a demanda comercial, científica, médica, segurança pública e necessidades militares. Como resultado, por causa de sua flexibilidade, o padrão 802.11 é uma tecnologia sempre presente (WALKE; MANGOLD; BERLEMANN, 2007).

Pilha de protocolos do 802.11

Os protocolos usados por todas as variantes do 802, inclusive a *Ethernet*, têm certas características comuns em sua estrutura. Uma visão parcial da pilha de protocolos do *802.11* é dada na Figura 4. A camada física corresponde à camada física do modelo *OSI* (*Open System Interconnection* - Figura 5), mas a camada de enlace de dados em todos os protocolos 802 se divide em duas ou mais subcamadas. No 802.11, a subcamada *MAC* (*Medium Access Control*) determina como o canal é alocado, isto é, quem terá a oportunidade de transmitir em seguida. Acima dela, encontra-se a subcamada *LLC* (*Logical Link Control*), cujo trabalho é ocultar as diferenças entre as diversas variações do 802 e torná-las indistinguíveis no que se refere à camada de rede.

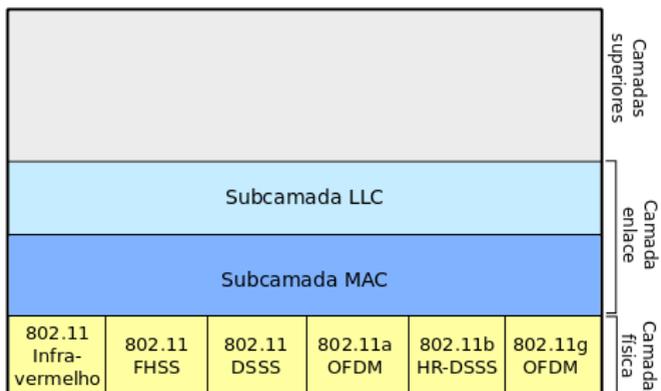


Figura 4: Parte da pilha de protocolos do *IEEE 802.11*.



Figura 5: Modelo de referência *OSI*.

O padrão 802.11 de 1997 especifica três técnicas de transmissão permitidas na camada física. O método de infravermelho utiliza quase a mesma tecnologia que os controles remotos dos televisores. Os outros dois métodos empregam rádio de alcance limitado, utilizando técnicas chamadas *FHSS* e *DSSS*. Ambas utilizam uma parte do espectro que não exige licenciamento (a banda *ISM* de 2,4 GHz). Todas essas técnicas operam a 1 ou 2 Mbps e com baixa potência, suficiente para evitar muitos conflitos. Em 1999, foram apresentadas duas novas técnicas para alcançar maior largura de banda. Essas técnicas são chamadas *OFDM* e *HR-DSSS*. Elas operam em até 54 Mbps e 11 Mbps, respectivamente. Em 2001, uma segunda modulação de *OFDM* foi introduzida, mas em uma banda de frequência diferente da primeira (TANENBAUM, 2003).

Arquitetura

A arquitetura do padrão 802.11 possui os seguintes componentes: estações (*STA*), pontos de acesso sem fio (*AP*), conjunto independente de serviços básicos (*IBSS*), conhecido também como *ad hoc*, sistema de distribuição (*DS - Distribution System*) e um conjunto estendido de serviços (*ESS - Extended Service Set*). As estações sem fio (*STA*) possuem um adaptador de rede que fornece conexão sem fio. Os pontos de acesso sem fio (*AP*) funcionam como uma ponte entre as estações sem fio e a rede de transporte existente.

Um *IBSS* é uma rede sem fio, formada com pelo menos duas *STAs*, usada quando o acesso ao sistema de distribuição (*DS*) não está disponível.

Um *BSS* é uma rede sem fio, formada por um simples ponto de acesso sem fio (*AP*) que suporta um ou mais clientes sem fio. Um *BSS* também é conhecido como uma rede sem fio infraestruturada. Todas as *STAs* em um *BSS* comunicam-se através do *AP*. O *AP* fornece a conectividade para a rede cabeada e a ponte quando uma *STA* comunica-se com outra *STA* ou um nodo no *DS*.

Um *ESS* é um conjunto de dois ou mais *APs* conectados a mesma rede cabeada que define a mesma rede lógica de um único segmento delimitada por um roteador (também conhecida como sub rede).

Os *APs* de múltiplos *BSSs* estão interconectados pelo *DS*. Isso permite mobilidade, pois *STAs* podem se mover de um *BSS* para outro. Os *APs* podem estar conectados a uma rede externa por uma rede sem fio, no entanto, na maioria das vezes estão conectados por cabos. O *DS* é o componente lógico usado para conectar *BSSs*. O *DS* faz a

distribuição de serviços para permitir a itinerância de *STAs* entre *BSSs* (TECHNET, 2003).

As Figuras 6 e 7 ilustram formas comuns de uso da arquitetura 802.11.

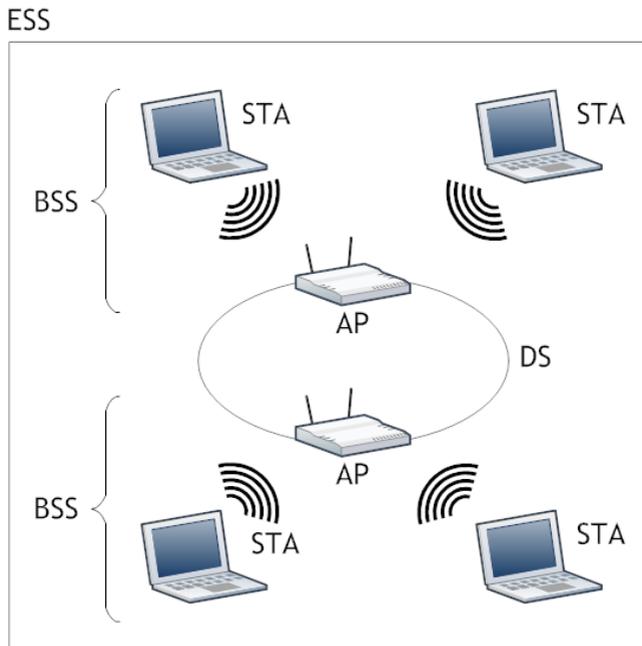


Figura 6: Arquitetura *ESS* - *Extended Service Set* do IEEE 802.11: conjunto de dois ou mais APs conectados a mesma rede cabeada.

Modos de operação

IEEE 802.11 define os seguinte modos de operação:

- Infraestruturado
- Ad hoc

Em ambos os modos, um *Service Set Identifier (SSID)*, também conhecido como nome da rede, identifica a rede sem fio. O *SSID* é um nome configurado no *AP* (no modo infraestruturado) ou em um cliente inicial (no modo ad hoc) que identifica a rede sem fio. O *SSID*



Figura 7: Arquitetura *IBSS - Independent Basic Service Set* do IEEE 802.11: rede sem fio formada por pelo menos duas estações.

é periodicamente anunciado pelo *AP* ou por um cliente inicial usando um quadro especial de gerenciamento do padrão 802.11 conhecido como quadro *beacon* (TECHNET, 2003).

As Figuras 8 e 9 ilustram os dois modos de operação:

Serviços

O padrão 802.11 estabelece que cada *LAN* sem fio compatível deve fornecer nove serviços. Esses serviços estão divididos em duas categorias: quatro serviços da estação e cinco serviços de distribuição. Os serviços da estação se relacionam à atividade dentro de uma única célula. Em contraste, os serviços de distribuição se relacionam ao gerenciamento da associação a células e à interação com estações situadas fora da célula.

Os cinco serviços de distribuição são fornecidos pelas estações base e lidam com a mobilidade das estações à medida que elas entram e saem das células, conectando-se e desconectando-se das estações base. São os serviços:

1. **Associação:** serviço usado pelas estações móveis para se

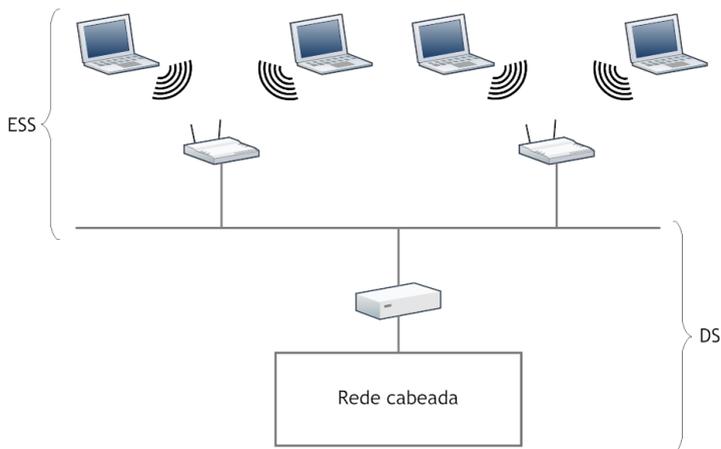


Figura 8: Modo infraestruturado de operação do IEEE 802.11.

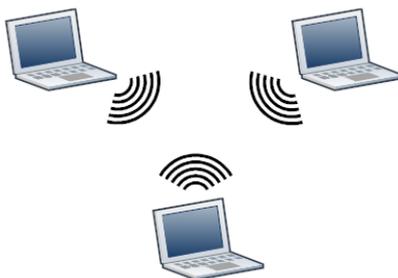


Figura 9: Modo ad hoc de operação do IEEE 802.11.

conectar às estações base. Usado geralmente logo após uma estação deslocar-se no interior do alcance de rádio da estação base. Ao chegar, ela anuncia sua identidade e seus recursos. Os recursos incluem as taxas de dados admitidas, a necessidade de serviços *PCF* (*Point Coordination Function*) e requisitos de gerenciamento da energia. A estação base pode aceitar ou rejeitar a estação móvel. Se for aceita, a estação móvel terá que se autenticar.

2. **Desassociação:** A estação móvel ou a estação base pode se desassociar, interrompendo assim o relacionamento. Uma estação deve usar esse serviço antes de se desligar ou sair, mas a

estação base também pode usá-lo antes de se desativar para manutenção.

3. **Reassociação:** Uma estação pode mudar sua estação base preferida usando esse serviço. Esse recurso é útil para estações móveis que se deslocam de uma célula para outra. Se for usado corretamente, não haverá perda de dados em consequência da transferência (*handover*).
4. **Distribuição:** serviço responsável por rotear os quadros enviados à estação base. Se o destino for local para a estação base, os quadros poderão ser enviados diretamente pelo ar. Caso contrário, eles terão de ser encaminhados pela rede fisicamente conectada.
5. **Integração:** Se um quadro precisar ser enviado por meio de uma rede que não seja 802.11, com um esquema de endereçamento ou um formato de quadro diferente, esse serviço cuidará da conversão do formato 802.11 para o formato exigido pela rede de destino.

Os quatro serviços restantes são serviços intra célula (ou intracelulares, isto é, se relacionam a ações dentro de uma única célula). Eles são usados depois que ocorre a associação, e são descritos da seguinte maneira:

1. **Autenticação:** uma estação deve se autenticar antes de poder transmitir dados visto que a comunicação é sem fio e portanto estações não autorizadas podem transmitir e receber dados. Após ocorrer a associação, ou seja, a estação móvel ser aceita pela estação base, a estação base envia um quadro especial para garantir que a estação móvel tem conhecimento da chave secreta (senha) que foi atribuída a ela. Para demonstrar o conhecimento da chave secreta, a estação móvel retorna à estação base o quadro especial criptografado. Se o resultado for correto, a estação móvel será completamente registrada na célula.
2. **Desautenticação:** quando uma estação autenticada anteriormente quer deixar a rede, ela é desautenticada. Depois da desautenticação, a estação não pode mais utilizar a rede.
3. **Privacidade:** para que as informações enviadas por uma LAN sem fio sejam mantidas confidenciais, elas devem ser criptografadas. Esse serviço administra a criptografia e a descriptografia. O algoritmo de criptografia atualmente especificado é o *RC4*, criado por *Ronald Rivest*, do *M.I.T.*

4. **Entrega de dados:** a transmissão de dados é o objetivo, e assim o 802.11 oferece naturalmente um meio para transmitir e receber dados. Como o padrão 802.11 foi baseado no padrão *Ethernet* ele também não oferece garantia de ser 100% confiável. As camadas mais altas é que devem se preocupar em oferecer confiabilidade através da detecção e correção de erros.

Uma célula 802.11 tem alguns parâmetros que podem ser inspecionados e, em alguns casos, ajustados. Eles se relacionam à criptografia, aos intervalos de *timeout*, às taxas de dados e assim por diante.

Formato dos Quadros

O padrão 802.11 define vários tipos de quadros que as estações (*NICs* e *APs*) usam para comunicação, assim como na gestão e controle da conexão sem fio. Todo quadro tem um campo que identifica a versão do protocolo 802.11, um campo com o tipo do quadro, e vários indicadores, como quando a criptografia *WEP* está ativa, gestão de energia está ativa, e assim por diante. Adicionalmente todos os quadros contêm o endereço *MAC* da estação remetente e destinatária (e *AP*), o número de sequência do quadro, o corpo do quadro e um campo de checagem de erro.

Os quadros de dados do 802.11 transportam protocolos e dados das camadas superiores dentro do corpo do quadro. Um quadro de dados, por exemplo, pode transportar o código *HTML* de uma página da *web* que um usuário esteja visitando. Outros quadros que estações usam para gestão e controle da conexão sem fio são transportados no corpo do quadro. Por exemplo, um quadro de aviso (*beacon frame*) contém o conjunto identificador do serviço (*SSID - Service Set Identifier*), *timestamp*, e outras informações importantes a respeito do *Access Point*.

Cada quadro consiste dos seguintes componentes básicos:

- Um cabeçalho *MAC* que inclui o controle do quadro, duração, endereço, e o número de sequência, e, para quadros de dados *QoS*, informação de controle *QoS*;
- Um campo de corpo do quadro com tamanho variável que contém informação específica a respeito do tipo e subtipo do quadro.
- Um campo de controle de erro que contém um *IEEE 32-bit CRC* (algoritmo de detecção de erro) (IEEE... , 2007).

comparando-o com o texto original enviado anteriormente. Com base na resposta da comparação feita o *AP* retorna com um quadro de autenticação contendo o resultado da autenticação.

- *Deauthentication frame*: Uma estação envia um quadro de desautenticação para outra estação caso ela deseje finalizar uma comunicação segura.
- *Association request frame*: a associação permite ao *AP* alocar recursos e sincronizar-se com o rádio. O rádio inicia o processo de associação enviando um pedido de associação para um *AP*. Esse quadro transporta informações sobre o rádio (por exemplo, taxas de dados suportadas) e o *SSID* da rede que ele deseja se associar. Após o pedido de associação ser recebido pelo *AP*, ele o analisa, e (se aceito) reserva memória e estabelece um *ID* de associação para o rádio em questão.
- *Association response frame*: um *AP* envia um quadro de resposta de autenticação do rádio contendo a notícia de aceitação ou rejeição em resposta à requisição de associação recebida. Se o *AP* aceita o rádio, o quadro inclui informações a respeito da associação, como as informações de taxas de dados suportadas e *ID* de associação. Caso o resultado da associação seja positivo, o rádio pode utilizar o *AP* para comunicar-se com outros rádios na rede e sistemas na área de distribuição (isto é, *Ethernet*) do *AP*.
- *Reassociation request frame*: caso o rádio se afaste da área de alcance do *AP* atualmente associado e encontre outro *AP* possuindo um sinal de aviso mais forte, o rádio irá enviar um quadro de reassociação para o novo *AP*. Então o novo *AP* coordena o encaminhamento de dados que ainda possam estar no *buffer* do *AP* anterior à espera de transmissão ao rádio em questão.
- *Reassociation response frame*: um *AP* envia um quadro de resposta de reassociação contendo a aceitação ou rejeição do pedido de reassociação enviado pelo rádio. Similar ao processo de associação, o quadro inclui informações a respeito da associação como taxa de dados suportados e *ID* de associação.
- *Disassociation frame*: uma estação envia um quadro de desassociação para outra estação caso deseje terminar uma

associação. Por exemplo, o rádio que desligar normalmente pode enviar um quadro de desassociação para alertar o *AP* que o rádio está se desligando. Então o *AP* desaloca a memória e remove o rádio de sua tabela de associação.

- *Beacon frame*: o *AP* periodicamente envia esse quadro para anunciar sua presença e transmite informações como: *SSID* e outros parâmetros a respeito do *AP* para rádios que estiverem no raio de alcance. Os rádios estão continuamente monitorando todos os canais 802.11 e escutando os quadros de aviso para formar uma base para escolha do melhor *AP* para se associar.
- *Probe request frame*: uma estação envia um quadro de pedido de sonda quando ela precisa obter informação de outra estação. Por exemplo, um rádio pode enviar um pedido de sonda para saber quais *APs* estão no seu alcance.
- *Probe response frame*: a estação irá responder com um quadro de resposta de sonda contendo informação de capacidade, taxas de dados suportadas, etc., logo após ela receber um quadro de pedido de sonda.

2. **Quadros de controle:** ajudam na entrega de quadros de dados entre as estações. A seguir os subtipos mais comuns de quadros de controle:

- *Request to Send (RTS) frame*: A função *RTS/CTS* é opcional e reduz as colisões de quadros quando estações ocultas (quando uma estação pode receber *frames* de duas outras, mas as duas estações transmissoras não conseguem receber *frames* uma da outra) têm associação com o mesmo *AP*. Uma estação envia um quadro *RTS* para outra estação como uma primeira etapa de um acordo necessário antes de enviar um quadro de dados.
- *Clear to Send (CTS) frame*: uma estação responde a um *RTS* com um *CTS*, fornecendo liberação para que a estação requerente envie quadros de dados. O *CTS* inclui um valor de tempo que faz com que todas as outras estações (incluindo as ocultas) adiem suas transmissões por um período de tempo necessário para que a estação requerente possa enviar seu quadro. Isso minimiza as colisões entre as estações ocultas, o que pode resultar em um fluxo maior se for implementado corretamente.

- *Acknowledgement (ACK) frame*: após receber um quadro de dados, a estação destinatária irá utilizar um processo de checagem de erro. Então essa estação irá enviar um quadro *ACK* se nenhum erro for encontrado. Caso a estação não receber o *ACK* após um período de tempo, a estação irá retransmitir o quadro.

3. **Quadros de dados**: obviamente, o principal propósito de uma rede sem fio é trocar dados. O padrão 802.11 define um quadro de dados cujo propósito é encapsular e carregar pacotes das camadas superiores.

3.3.4 IEEE 802.11p

Em 2004, o IEEE iniciou a padronização das comunicações em redes veiculares dentro do grupo de trabalho IEEE 802.11. O padrão é conhecido como IEEE 802.11p *WAVE*. A arquitetura *WAVE* (*Wireless Access in the Vehicular Environment*) é definida em seis documentos: IEEE P1609.1, IEEE P1609.2, IEEE P1609.3, IEEE P1609.4, IEEE 802.11 e IEEE 802.11p. O padrão IEEE 802.11p é uma extensão da família de protocolos IEEE 802.11. Ele se baseia principalmente na extensão “a” do IEEE 802.11, porém, opera na faixa *DSRC* de 5,9 GHz. O objetivo principal é fornecer comunicação a veículos com deslocamentos de até 160 Km/h. Outra capacidade deste padrão é a possibilidade de se criarem conexões *mesh* entre veículos.

O padrão IEEE 802.11p define as camadas físicas e de controle de acesso ao meio (*MAC*) para redes veiculares, e é baseado no padrão de redes locais IEEE 802.11a, que opera em uma faixa de frequências próxima à alocada para as redes veiculares. Além disso, a arquitetura *WAVE* designa uma família de padrões que não se restringe às sub camadas *MAC* e física. Os padrões da família IEEE 1609 definem outras camadas da pilha de protocolos, incluindo uma camada de rede alternativa à camada *IP*, características de segurança para aplicações *DSRC* e operação em múltiplos canais de comunicação (ALVES et al., 2009). Em 2011 espera-se o lançamento dos primeiro produtos comerciais do IEEE 802.11p que ajudar no trabalho desenvolvido nessa dissertação.

3.3.5 IEEE 802.16 - *WiMAX*

A primeira versão do padrão IEEE 802.16-2001, finalizada em Outubro de 2001 e publicada em 8 de Abril de 2002, definiu a especificação da interface *WirelessMANTM air* para redes metropolitanas sem fio (*MANs - Metropolitan Area Networks*). A intenção por trás da primeira versão do padrão foi definir a tecnologia de acesso a banda larga sem fio (*BWA - Broadband Wireless Access*) para usuários fixos, como uma alternativa as redes cabeadas, como a DSL (*Digital Subscriber Line*). Por essa razão, o IEEE 802.16 original define uma arquitetura de rede ponto-multiponto (*PMP - Point-to-Multipoint*) onde os recursos são compartilhados por um nodo central chamado de estação base (*BS - Base Station*) para um conjunto de estações assinantes (*SS - Subscribe Station*). Na verdade, o modo operacional *PMP* serve em um cenário fixo *BWA*, aonde vários assinantes se conectam a um provedor central de serviços que acessa redes externas, como a *Internet*, ou serviços, como transmissão de vídeo (*DVB - Digital Vídeo Broadcasting*) (GHOSH et al., 2005).

Desde a primeira versão, a camada *MAC* foi orientada a conexão e suportou qualidade de serviço (*QoS*). Além do mais, o padrão foi projetado para evoluir como um conjunto de interfaces aéreas baseadas em um protocolo *MAC* em comum, mas com especificações da camada física dependente do espectro utilizado e os regulamentos associados. O padrão, o qual foi aprovado em 2001, endereça frequências de 10 a 66 GHz em operações em linha visada (*LOS - Line of Sight*: Figura 11) usando uma única portadora de transmissão. Em 2003, uma nova versão do padrão, IEEE 802.16a-2003, foi publicada com suporte a operação em linha não visada (*NLOS - Non-line of Sight*: Figura 11) e frequências de 2 a 11 GHz. O padrão 802.16 pode ter velocidade aproximada de 70 Mbps e um alcance acima de 50Km (EKLUND et al., 2002; BACIOCCOLA et al., 2010).

Suporte à mobilidade

Um aprimoramento ocorrido durante o desenvolvimento do padrão deu origem ao IEEE 802.16-2004 que deu suporte para duas camadas físicas adicionais: *OFDM* (*Orthogonal Frequency Division Multiplexing*) e *OFDMA* (*Orthogonal Frequency Division Multiple Access*). Em 2005, uma nova versão do padrão foi lançada permitindo a combinação entre operações fixas e móveis em bandas licenciadas. O

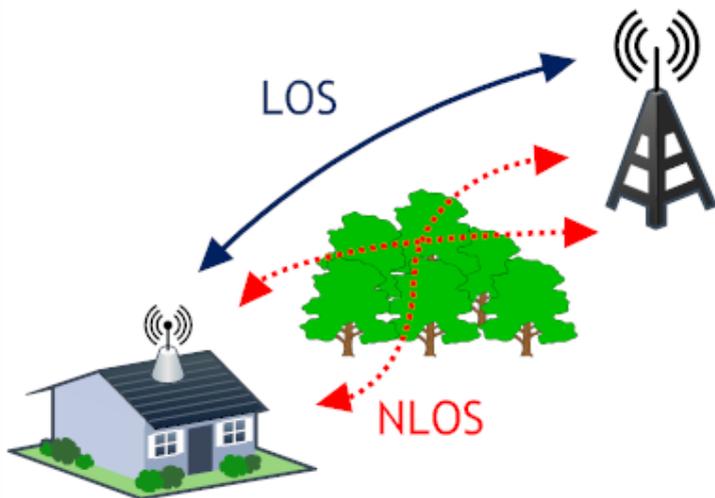


Figura 11: Modos de operação LOS e NLOS da *WiMAX*.

padrão citado, IEEE 802.16e-2005, foi definido como um aperfeiçoamento do IEEE 802.16-2004 e adicionou diversos recursos relacionados com operações móveis e estações móveis (*MS - Mobile Station*), incluindo economia de energia, modo inativo, *handover* (processo de troca de célula de um *MS* sem perda de conexão) e um aperfeiçoamento da camada física *OFDMA*. Depois do lançamento de 2005, o desenvolvimento do padrão continuou para definir a base de gestão de informação (*MIB - Management Information Base*) para as camadas *MAC* e física, IEEE 802.16f, e o plano de gestão e procedimentos, IEEE 802.16g. E para melhorar a co-existência de operações de licenças isentas, IEEE 802.16h, para introduzir as capacidades de retransmissão, IEEE 802.16j-2009, e para refinar os procedimentos de operações móveis das camadas *MAC* e física, IEEE 802.16-2009 (BACIOCCOLA et al., 2010).

O último padrão lançado é também conhecido como a versão 2009, e traz as seguintes mudanças principais:

- Operações móveis terminais *half-duplex* em *OFDMA* por divisão de frequência *duplex* (*FDD - Frequency Division Duplexing*).
- Balanceamento de carga.
- Compressão robusta de cabeçalho (*ROHC - Robust Header*

Compression).

- Mecanismo melhorado para alocação de recursos.
- Suporte para serviços baseados em localização (*LBS - Location Based Services*).
- Serviços de *multicast* e de *broadcast* (*MBS - Multicast and Broadcast Service*).

A mudança do IEEE 802.16-2009 também envolveu a incorporação das alterações do IEEE 802.16f e do IEEE 802.16g além de remover algumas características obsoletas, como o modo de malha (BACIOCCOLA et al., 2010).

Topologia

Entre todos os padrões definidos pode-se citar três topologias de rede existentes conforme descrito a seguir e ilustrado na Figura 12.

Ponto-a-ponto:

- Utilizadas duas antenas de rádio interligando dois pontos.
- Pouca facilidade de adição de novos nós na rede.
- Existe uma maior banda passante nesta solução.
- Exemplo: a matriz e a filial de uma empresa.

Ponto-multiponto (*PMP*):

- Células que podem utilizar antenas do tipo onidirecional (360°) ou setorial.
- O ângulo de abrangência da antena setorial pode ser de 30° , 60° , 90° ou 120° , dependendo da área de cobertura.
- Maior cobertura

Malha (*Mesh*):

- A arquitetura *mesh* é bem parecida com a arquitetura ponto-multiponto.
- O tráfego pode ser roteado através de outros assinantes, como também pode ocorrer diretamente entre os assinantes.

- Oferece redundância e maior confiabilidade.
- Mais dispendiosa, pois cada nó ou cliente da rede requer um roteador.

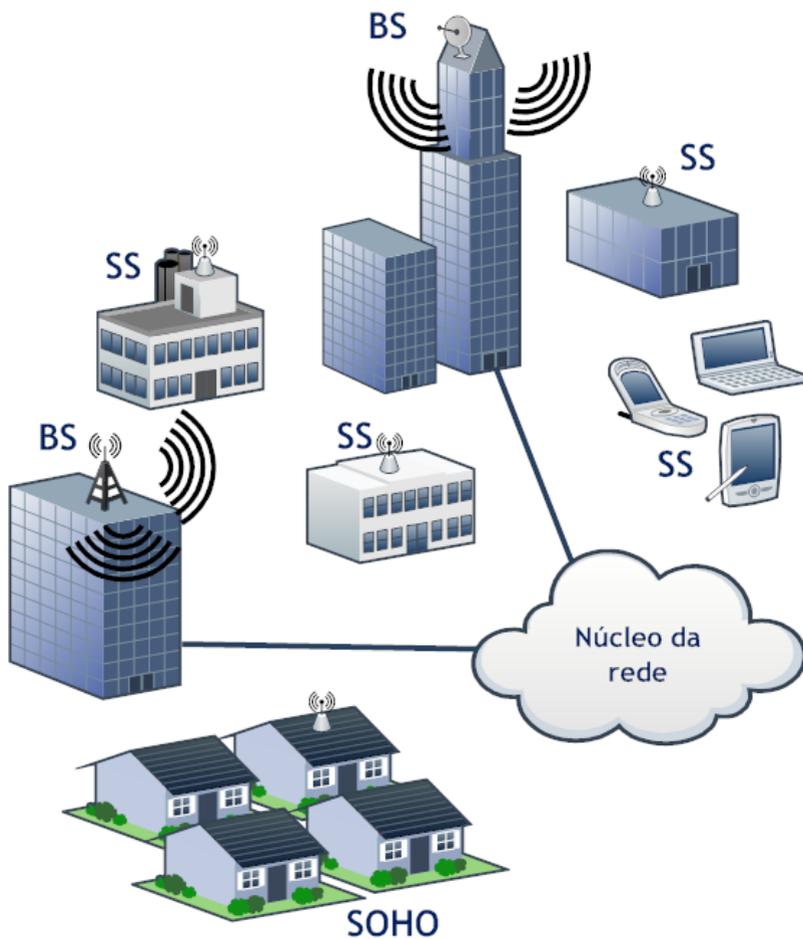


Figura 12: Topologia padrão IEEE 802.16.

1. Camada Física: o projeto da camada física do 2-11 GHz é impulsionado pela necessidade da operação *NLOS*, o que permite implantação e operação com baixo custo. O padrão IEEE 802.16a/d define três camadas físicas diferentes que podem ser usadas em conjunto com a camada *MAC* para fornecer uma conexão confiável. Essas especificações aéreas são:

- *WirelessMAN-SCa*: interface aérea que usa modulação *single-carrier*.
- *WirelessMAN-OFDM*: *256-carrier OFDM*. O acesso múltiplo de diferentes estações (*SSs*) é baseado em divisão por tempo (*TDMA - Time Division Multiple Access*).
- *WirelessMAN-OFDMA*: *2048-carrier OFDMA*. O acesso múltiplo é fornecido pelo acesso a um subconjunto de portadoras para um receptor individual, por isso essa versão é frequentemente conhecida por *OFD multiple access (OFDMA)*.

Dessas 3 interfaces, as duas baseadas em sistemas *OFDM* são mais adequadas para operações *NLOS* devido à simplicidade do processo de equalização para os sinais multi portadoras. Das duas interfaces aéreas baseadas em *OFDM*, *256-carrier WirelessMAN-OFDM* parece ser favorecida pela comunidade de fornecedores por razões como picos baixos na taxa média, cálculo mais rápido da transformada rápida de Fourier (*FFT - Faster Fast Fourier*) e requisitos menos rigorosos para sincronização de frequência quando comparado com o *2048-carrier WirelessMAN OFDMA*. Todos os perfis definidos atualmente pelo *WiMAX Forum* especificam a camada física *256-carrier OFDM*.

A fim de garantir a implementação global, o padrão IEEE 802.16 foi definido com uma largura de banda do canal variável. A largura de banda do canal pode ser um número inteiro múltiplo de 1.25 MHz, 1.5 MHz e 1.75 MHz com um máximo de 20 MHz. Essa grande largura de banda foi reduzida para poucas possibilidades pelo *WiMAX Forum*, o qual tem como primeira tarefa garantir a interoperabilidade entre implementações do padrão 802.16d por fornecedores (GHOSH et al., 2005).

2. Camada MAC: essa camada foi projetada para aplicações de acesso por difusão sem fio *PMP*. Ela foi desenvolvida para agrupar as requisições das aplicações de alta taxa de

transferência de dados com a variedade de requisições da qualidade de serviço (QoS). Os algoritmos de sinalização e alocação de largura de banda têm sido desenvolvidos para fornecer centenas de terminais por canal. O padrão permite que cada terminal seja compartilhado por múltiplos usuários. Os serviços requisitados pelos usuários finais podem ter requisições de latência e largura de banda, o que demanda flexibilidade e eficiência do protocolo da camada *MAC* em cima de um vasto intervalo de diferentes modelos de tráfego de dados. O sistema foi desenvolvido com a missão de incluir a multiplexação por divisão de tempo (*TDM - Time-Division Multiplex*) de voz e dados, conectividade *IP* e voz sobre *IP* (*VoIP - Voice over Internet Protocol*).

A camada *MAC* do IEEE 802.16 está dividida nas sub camadas de convergência específicas e *MAC* comum (Figura 13). As subcamadas de convergência específica são usadas para mapear o tráfego específico da camada de transporte para o *MAC*, que é suficientemente flexível para transportar qualquer tipo de tráfego. A subcamada de convergência comum é independente do mecanismo de transporte e responsável pela fragmentação e segmentação das unidades de dados dos serviços *MAC* (*SDU - Service Data Units*) em unidades do protocolo *MAC* (*PDU_s - Protocol Data Units*), controle de *QoS* e agendamento e retransmissão de *PDU_s MAC* (IEEE, 2009).

A largura de banda pedida e o mecanismo de concessão foram desenvolvidos para serem escalonáveis, eficientes e auto-corrigíveis. O sistema de acesso do 802.16 não perde a eficiência quando várias conexões por terminal estão presentes, múltiplos níveis de *QoS* e um grande número de usuários multiplexados estatisticamente. Isso tira proveito em cima da grande variedade de mecanismos de pedido. Enquanto a ampla alocação de banda e mecanismos de *QoS* são fornecidos pelo padrão, os detalhes do agendamento e gestão de reservas são deixados indefinidos, de tal forma que as diferenciações do produto podem ser alcançadas através de implementações de diferentes fornecedores (GHOSH et al., 2005; EKLUND et al., 2002).

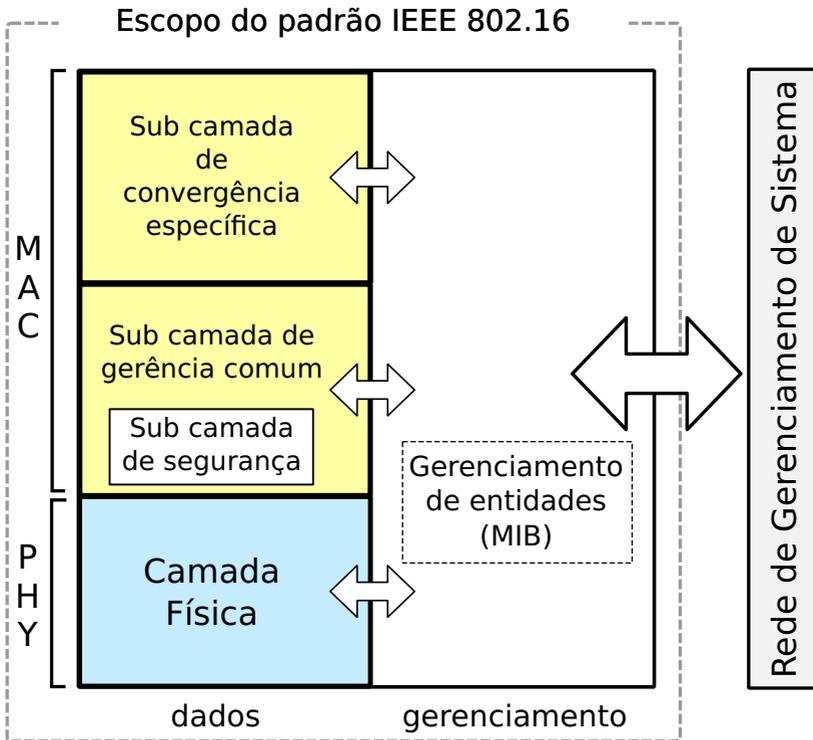


Figura 13: Pilha de protocolos do IEEE 802.16.

3.3.6 HTTP - Hypertext Transfer Protocol

O protocolo de transferência usado em toda a *World Wide Web* (*WWW*) é o *HyperText Transfer Protocol* (*HTTP*). Esse protocolo padroniza as mensagens que serão trocadas entre clientes e servidores. Cada interação consiste em um pedido *ASCII*, seguido por uma resposta *RFC 882* semelhante ao *MIME*. Todos os clientes e todos os servidores devem obedecer a esse protocolo. Ele está definido na *RFC 2616* (FORCE, 2011).

Normalmente um navegador comunica-se com um servidor estabelecendo uma conexão *TCP* para a porta 80 do servidor, mesmo não sendo obrigatório esse procedimento. A vantagem de usar o *TCP* é que nem o navegador e nem o servidor precisam se preocupar com a perda ou com confirmações. Quem se responsabiliza por tudo isso é o

TCP.

Em sua primeira versão — *HTTP 1.0* — depois de estabelecida uma conexão, uma única solicitação era enviada e uma única resposta era devolvida. Na seqüência, a conexão *TCP* era encerrada. Na época em que as páginas da *web* consistiam apenas de textos puros em *HTML* esse método era adequado. Porém, após alguns anos, as páginas da *web* evoluíram passando a ter um grande número de imagens associadas, tornando, então, o estabelecimento consecutivo de conexões *TCP* muito dispendioso.

Como conseqüente evolução, surgiu o *HTTP 1.1*, que admite conexões persistentes. Com elas, é possível estabelecer uma conexão *TCP*, enviar uma solicitação e obter uma resposta, e depois enviar solicitações adicionais e receber respostas adicionais na mesma conexão. O *overhead* relativo devido ao *TCP* é muito menor por solicitação *HTTP*. Também isso torna possível transportar as solicitações por *pipeline*, ou seja, enviar a solicitação 2 antes de chegar a resposta à solicitação 1.

3.3.7 Sentenças *NMEA - National Marine Electronics Association*

As sentenças *NMEA 0183* são especificações de dados e elétricas para comunicação de dispositivos eletrônicos de navegação, tais como anemômetros, ecolocalizadores, girocompassos, piloto automático, receptores GPS e muitos outros tipos de instrumentos (NMEA, 2011).

O padrão *NMEA 0183* usa *ASCII simples*, um protocolo de comunicação serial que define como os dados são transmitidos em uma sentença de um “locutor” a vários “ouvintes” em um momento. Através do uso de expansores de intermediários, um locutor pode ter uma conversa unidirecional com um número quase ilimitado de ouvintes, e usando multiplexadores, múltiplos sensores podem falar com uma porta de um único computador.

Na camada de aplicação, a norma também define o conteúdo de cada tipo de sentença (mensagem) para que todos os ouvintes possam analisar mensagens com precisão.

Exemplo de um tipo de sentença *NMEA 0183*:

```
$GPRMC,184628.600,A,2735.9962,S,04831.0864,W,0.02,255.34,070211,,A*67
```

As sentenças *\$GPRMC* são compostas obedecendo o seguinte padrão:

\$GPRMC,aaaaa,b,cccc.cccc,d,eeee.eeee,f,g.gg,hhh.hh,jjjjjj,kkk.k,l*mm

Onde:

- *aaaaaa* é a hora UTC no formato hhmmss.sss
- *b* é o estado (“A” = válido, “V” = inválido)
- *cccc.cccc* é a latitude no formato ddmn.mmmmm
- *d* é o indicador Norte/Sul (“N” = norte, “S” = sul)
- *eeee.eeee* é longitude no formato dddmm.mmmmm
- *f* é o indicador Leste/Oeste (“E” = leste, “W” = oeste)
- *g.gg* velocidade em Knots
- *hhh.hh* curso em graus
- *jjjjjj* é a data UTC no formato DDMMAA
- *kkk.k* variação magnética em graus
- *l* sentido da variação magnética (“E” = leste, “W” = oeste)
- **mm checksum*

3.4 SUMÁRIO

Este capítulo apresentou os conceitos necessários para o entendimento do trabalho, como a definição de sistemas inteligente de transporte abordando as redes veiculares. Também foi apresentado um embasamento técnico de todos os meios de comunicação usados durante o projeto, focando na parte teórica referente a implementação realizada. Entre os meios pode-se citar: comunicação serial, *SSH*, *WiFi*, *WiMAX*, HTTP e sentenças *NMEA*.

4 ARQUITETURA PROPOSTA

4.1 MOTIVAÇÃO DA ARQUITETURA

Os veículos automotores têm incorporado várias tecnologias conforme elas são disponibilizadas pelos fabricantes. Inicialmente todas essas tecnologias possuem um preço muito alto e são somente implementadas em veículos automotores de preço elevado. Pode-se citar algumas como freios *ABS*, controle de tração (*ASR*), controle de estabilidade (*ESP*), *airbag* etc. Apesar dessa incorporação de novas tecnologias, o congestionamento urbano continua a aumentar porque o número de veículos tem, também, aumentado.

Em geral, sistemas de segurança atuais são baseados em sensores e atuadores cada vez mais sofisticados, os quais captam sinais do ambiente e podem torná-los disponíveis ao condutor. No entanto, esses sistemas são restritos à interação entre veículo e condutor, isto é as informações permanecem no interior do veículo.

Através da rápida evolução dos dispositivos de comunicação sem fio está ocorrendo um grande crescimento das redes cuja principal característica é a possibilidade de comunicação sem uma infra-estrutura física. Nota-se que as redes móveis sem fio se destacam por permitirem a livre movimentação dos nós e rápida instalação (SILVA, 2010).

Atualmente as redes *WLAN (Wireless Local Area Network)* são uma solução poderosa e de ótimo custo benefício. No entanto, o acesso à rede está largamente limitado à cobertura local e frequentemente a ambientes internos. Um pouco menos difundido está o acesso em ambientes externos para usuários móveis, muitas vezes por causa do efeito colateral das *WLANs* no interior dos edifícios, ou em locais com pontos de acesso limitado como por exemplo em parques.

A recente consolidação de tecnologias de comunicação sem fio que seguem os padrões IEEE 802.11(*wifi*) (IEEE, 2010) e 802.16 (*WiMAX*) (IEEE, 2003) permite propor seu uso em monitoração e controle de tráfego urbano (ALVES FEHMI B. ABDESSLEM, 2008; CAVALCANTI, 2008). Criadas com diferentes propósitos de alcance, largura de banda e flexibilidade de uso (mobilidade, facilidade de configuração de nodos etc.), essas tecnologias podem ser combinadas para atender vários requisitos da gerência da operação do tráfego.

A arquitetura hierárquica de comunicação proposta nesse trabalho surge com o intuito de combinar duas tecnologias de grande

disseminação no mercado a fim de fornecer suporte a uma grande gama de aplicações de controle de tráfego urbano. As tecnologias usadas estão inseridas na área de redes, em particular, na comunicação sem fio. São elas:

- IEEE 802.11, mais popularmente conhecida como *WiFi*
- IEEE 802.16 conhecida como *WiMAX*

Sendo a *WiFi* utilizada para comunicações a curta distância e a *WiMAX* para comunicação a longa distância. Mais especificadamente, a comunicação a curta distância tem o objetivo de comunicação entre veículos e pontos infraestruturados às margens da rodovia e a comunicação de longa distância objetiva troca de dados entre os pontos infraestruturados e a central de controle de tráfego. A Figura 14 ilustra essa hierarquização na comunicação.

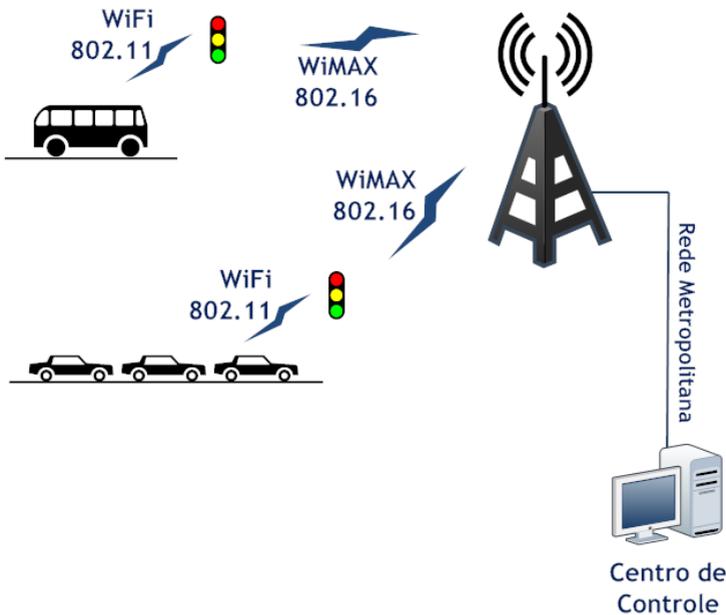


Figura 14: Comunicação de veículos com os semáforos e destes com centrais de controle e gerência de tráfego.

4.2 COMUNICAÇÃO *WIFI*

As redes sem fio *WiFi* tornaram-se populares em redes domésticas e pontos de acesso como restaurantes, aeroportos e restaurantes. Apesar de a tecnologia ter sido desenvolvida para utilização estática nada as impede de serem usadas em cenários móveis. Porém existem três razões que dificultam a implementação em redes veiculares.

1. As implementações atuais de cliente levam muito tempo—vários segundos— para sondar e se associar com um *AP*, adquirir um endereço *IP* e estabelecer uma conexão fim a fim em face as altas taxas de perda de pacotes nesse tipo de ambiente
2. Em geral protocolos de transferência de dados e controle de congestionamento não funcionam bem em períodos curtos de conexão.
3. Os algoritmos padrão de seleção de taxa de transferência são calibrados para usuários imóveis, resultando em uma performance sub ótima em aplicações veiculares.

Dentre todas as dificuldades encontradas durante a criação de toda a arquitetura do projeto pode-se destacar como sendo a comunicação *WiFi* um dos maiores desafios enfrentados devido aos simples fatos citados anteriormente. As redes *WiFi* foram projetadas inicialmente para cenários estáticos ou de baixa mobilidade. A partir do momento em que deseja-se implementá-la no cenário veicular nos deparamos com um cenário de grande mobilidade onde o tempo de conexão, qualidade do canal de comunicação, dentre outros fatores, tornam-se cruciais.

O padrão IEEE 802.11b foi inicialmente desenvolvido para baixa mobilidade em cenários internos, porém atualmente é uma das tecnologias mais usadas para experimentos de comunicação *VANET*. O 802.11b foi escolhido para compor nossa arquitetura porque se mostrou mais estável do que o 802.11g em testes realizados por outros pesquisadores onde taxas de transmissão mais altas foram obtidas, porém com alcance mais baixo (GONZÁLEZ et al., 2008; WELLENS; WESTPHAL; MAHONEN,).

O maior problema na implementação da rede *WiFi* para a comunicação entre pontos fixos às margens das vias de tráfego e os veículos em movimento está no estabelecimento da conexão. Na Figura 15 está ilustrado o processo de estabelecimento de conexão.

Geralmente, cada passo é composto de uma requisição seguida de uma resposta. O estabelecimento de conexão requisita no mínimo 13 quadros. Se nenhuma resposta é recebida em um tempo determinado, a requisição é retransmitida (ERIKSSON; BALAKRISHNAN; MADDEN, 2008b). Na Subseção 4.2.1 a seguir o processo de conexão será mais bem detalhado.

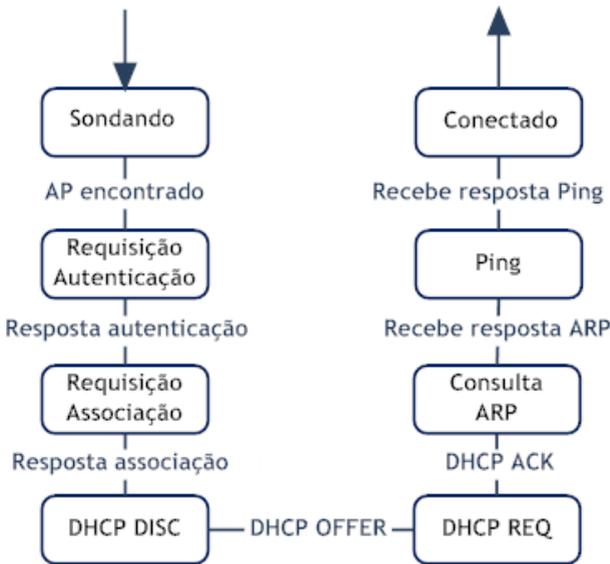


Figura 15: Passos no estabelecimento de uma conexão *WiFi*.

4.2.1 Procedimento de conexão do padrão IEEE 802.11

O processo de estabelecimento de conexão entre quaisquer nodos em uma rede *WiFi* está descrito na especificação do padrão IEEE 802.11 (IEEE, 2010). Esse processo consiste em 3 estágios consecutivos: sondagem e sincronização, autenticação e associação. No primeiro estágio o nodo encontra um canal do rádio, em que o *AP* está operando, define os parâmetros de conexão e faz a sincronização.

A sondagem pode ser feita no modo passivo ou ativo. No primeiro caso, o nodo escuta em cada canal do rádio e espera pela transmissão do quadro de aviso (*beacon frame*) para receber os parâmetros de configuração. Com a sondagem em cada um dos canais

do rádio, o nodo usuário transmite o quadro de consulta *probe request* e espera receber um quadro de resposta *probe response* no qual parâmetros de configuração também são transmitidos. Usando os parâmetros recebidos durante a sondagem, o nodo usuário faz uma sincronização com o *AP*. Durante o processo de sincronização, o nodo atribui valores de marca de tempo e identificador *BSSID*, recebido do *AP*.

Tendo finalizada a sondagem e sincronização, o nodo inicia o segundo estágio do estabelecimento de conexão: autenticação. O primeiro tipo de autenticação é o mais simples e permite que o nodo receba o estado da autenticação, se um *AP* também usa autenticação aberta. Quando a autenticação aberta é usada entre um nodo e um *AP* existe uma troca de 2 quadros de autenticação. O primeiro é a solicitação e o segundo a resposta a essa solicitação de autenticação.

Autenticação por meio de chaves compartilhadas pressupõe que o nodo e o *AP* tenham acesso ao protocolo *WEP*. Quando esse tipo de autenticação é usado, 4 quadros são trocados entre o nodo e o *AP*.

No estágio final do estabelecimento de conexão a associação é realizada por meio da entrega do *AID* (*Association Identifier*) ao nodo. Durante a associação, o nodo envia o quadro de requisição de associação e o *AP* retorna com o quadro de resposta de associação. Como resultado desse processo de troca de quadros, o *AID* é entregue ao nodo e o processo de conexão é finalizado.

Para que a comunicação realmente possa ocorrer, faltam as etapas de negociação de *IP* e verificação de conexão através do *ping*. De acordo com (BYCHKOVSKY et al., 2006) as implementações típicas do padrão IEEE 802.11 requerem muitos segundos para estabelecer uma conexão. Em seus estudos, *Bychkovsky et al.* mensuraram esse tempo em aproximadamente 11 segundos. Ele mostrou que o tempo médio para sondagem, associação, aquisição de *IP* e inicialização da aplicação levam respectivamente 750 *ms*, 560 *ms*, 1,83 *s* e 8 *s*.

Tal imposição temporal motivou a busca por maneiras de contornar esse problema surgindo então uma outra maneira de estabelecer a troca de dados entre um nodo e o *AP*. A Subseção 4.2.2 tratará do assunto que tornou-se um dos maiores focos durante o projeto.

4.2.2 Comunicação *WiFi* sem conexão

O artigo *Beacon-Stuffing: Wi-Fi Without Associations* (CHANDRA et al., 2007) trabalha uma abordagem alternativa para a comunicação *WiFi*, a sem conexão. Trata-se de uma comunicação de baixa largura de banda, ideal para o propósito do projeto, que habilita a comunicação entre *APs* e seus clientes sem associação, processo que dispende um tempo preciso no objetivo da aplicação do projeto. Essa comunicação se baseia em 2 observações chaves. A primeira, é que clientes recebem quadros de aviso (*beacon frames*) dos *APs* mesmo quando eles não estão associados a eles. A segunda, é que é possível sobrecarregar com dados campos no *beacon* e outros campos dos quadros de gerenciamento.

Os quadros *beacon* são utilizados para anunciar a presença da rede, então a ideia principal é sobrecarregar esses quadros para carregar informações adicionais. No entanto, os quadros *beacon* são tipicamente enviados com uma baixa taxa. O formato do quadro *beacon* do padrão 802.11 está ilustrado na Figura 16. *APs* comerciais permitem somente a modificação do *SSID* (texto legível pelo ser humano que identifica a rede) no quadro *beacon*, e essa será a técnica adotada na implementação da comunicação *WiFi* no projeto.

<i>Beacon Interval</i> (2 bytes)	<i>Time Stamp</i> (8 bytes)	SSID (32 bytes)	Taxas suportadas (8 bytes)	Informações de capacidade (2 bytes)	Elemento de informação (256 bytes)	<i>BSSID</i> (6 bytes)
----------------------------------	-----------------------------	------------------------	----------------------------	-------------------------------------	------------------------------------	------------------------

Figura 16: Alguns campos do pacote *beacon* do padrão IEEE 802.11.

4.3 WIMAX

Através do uso da comunicação *WiMAX*, um ponto fixo a beira da via pode comunicar-se com a central a quilômetros de distância. A complexidade da comunicação *WiMAX* é resolvida, em boa parte, através de um *gateway* entre os protocolos IEEE 802.11 e IEEE 802.16 com portas *ethernet*. No momento que o *AP* está conectado a este *gateway* (um roteador) *ethernet* e a este está ligado uma antena *WiMAX* a comunicação funciona normalmente como uma simples

rede *ethernet*.

4.4 SUMÁRIO

Este capítulo apresentou a arquitetura hierárquica proposta e implementada, explicando suas funcionalidades. Tratou também de um importante desafio durante a implementação: a comunicação *WiFi* sem associação. Finalmente foi abordada a questão com respeito ao canal de comunicação *WiMAX* usado.

5 ESTUDO DE CASO: *SORVES*

5.1 MOTIVAÇÃO

Atualmente, muitas rodovias e malhas viárias urbanas são monitoradas por câmeras comandadas por controladores. O estudo de caso proposto neste trabalho, *SORVES* (Software Rastreador Visual de Veículos Especiais Baseado em Redes Sem Fio e Sistema Global de Posicionamento), surge com o intuito de automatizar o monitoramento visual em aplicações *SIT*. Veículos especiais, isto é, selecionados a portarem equipamentos de processamento e comunicação, informam a sua posição a células de monitoramento às margens das vias de tráfego para que possam ser acompanhados visualmente. Essa arquitetura compõe-se de vários níveis de comunicação: mais internamente, a comunicação entre os equipamentos do veículo; um nível acima, uma comunicação sem fio entre veículo e células de monitoramento; e, no último nível, uma comunicação a longa distância entre essas células e a central de controle e monitoração.

5.2 DESCRIÇÃO

Trata-se um sistema rastreador óptico de veículos baseado em tecnologias sem fio e no sistema global de posicionamento (*GPS*) com o objetivo de testar a viabilidade da arquitetura hierárquica proposta. O sistema é composto por um veículo portando um computador equipado com um *GPS* e um roteador *WiFi*. Um programa executa uma rotina em laço infinito nesse computador coletando os dados fornecidos pelo *GPS*, esses dados são tratados e, junto de outras informações, é montado um quadro a ser enviado pela rede *WiFi* do roteador. Em pontos fixos na via, câmeras *PTZ* (*Pan-Tilt-Zoom*) ligadas a roteadores *WiFi* coletam esses dados transmitidos pelo veículo e enviam para o servidor central. O envio é feito através de uma antena *SS WiMAX*. O servidor recebe essa informação, trata-a e retorna para a câmera o que fazer. O *gateway* entre a rede *WiFi* e a rede *WiMAX* é feita por *Ethernet* e os roteadores são responsáveis por essa tarefa. Recebendo essa informação, a câmera move-se nos 3 graus de liberdade que possui, centralizando o veículo na imagem. Essa imagem é enviada de volta ao servidor para que seja usada em

algum sistema de monitoramento. A Figura 17 ilustra a arquitetura montada.

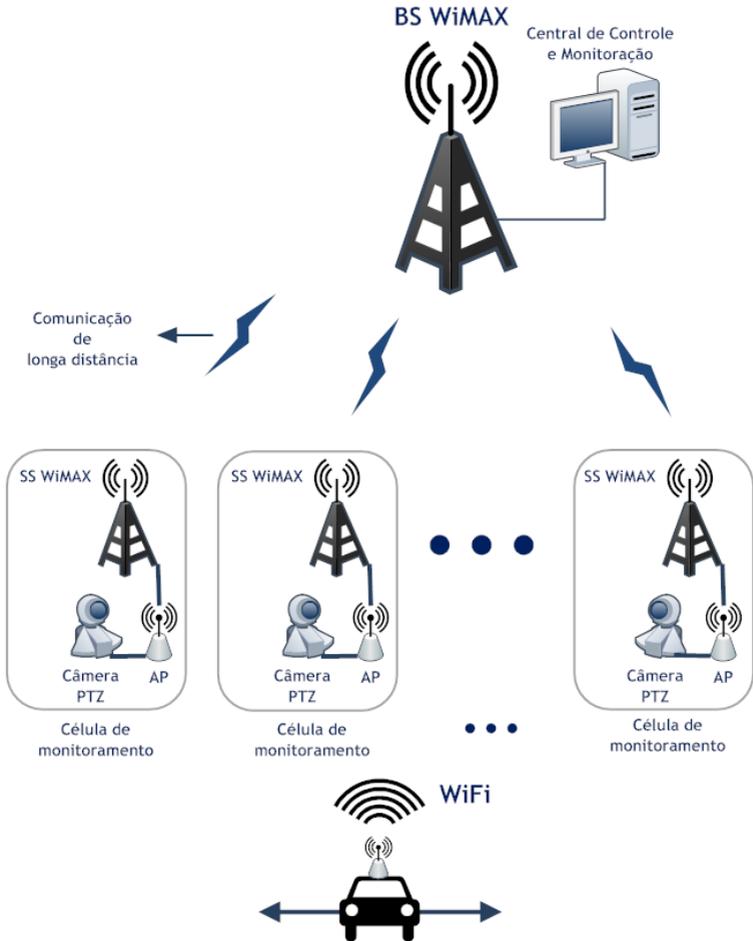


Figura 17: Esquema ilustrativo da arquitetura hierárquica de comunicação.

5.3 HARDWARE E SOFTWARE UTILIZADOS

Como protótipo, grande parte dos equipamentos e *hardware* usados foram escolhidos pela sua disponibilidade, adequando-os para os seus propósitos a fim de realizar testes com a arquitetura proposta. Durante toda a implementação do projeto surgiram necessidades que só puderam ser sanadas através do uso de bibliotecas externas.

5.3.1 *Hardware* e equipamentos

A arquitetura proposta teve seus componentes escolhidos por questões de grande disseminação no mercado, velocidades de comunicação, alcance, grande suporte, entre outros. O objetivo principal foi diminuir e automatizar o tempo de rastreamento visual de veículos, feito normalmente por operadores de câmera. O sistema foca-se no rastreamento de veículos especiais devido ao fato que esses estabelecem uma comunicação sem fio com o sistema. Tal comunicação fornecem informações a respeito de seus posicionamentos geográficos a fim de que possam ser localizados visualmente, como ilustrado na Figura 2.

Componentes:

- 1 SS *WiMAX*
- 1 BS *WiMAX*
- 2 roteadores *Ethernet*
- 1 câmera PTZ
- 1 servidor
- 1 notebook
- 1 *GPS mouse*
- 1 roteador *WiFi* com *Linux* embarcado.

O *AP WiFi* escolhido foi especificamente o *Cisco Linksys WRT54GL* devido a sua versabilidade para a instalação de *firmwares* de código aberto e grande capacidade de processamento e memória. Para a recepção dos pacotes enviados através dos quadros *beacon* por esse *AP* foi utilizada a placa *Intel® PRO/Wireless Network*

Connection 3945ABG(802.11a/b/g) no modo promíscuo de um *notebook*.

O *GPS USB* utilizado foi o *Qstarz GPS Nano BT-Q890* pela sua alta frequência de aquisição de coordenadas geográficas, 5 Hz. A câmera *IP* responsável pelo rastreamento visual do veículos especiais baseadas em informações de coordenadas geográficas emitidas por esses veículo foi uma *AXIS 214 PTZ Network Camera*.

Por fim para a comunicação *WiMAX* foram usadas 2 antenas da *Alvarion*[®] sendo uma *BS* e outra *SS*.

5.3.2 Bibliotecas e *APIs* de Softwares

Como *firmware* do *AP* foi utilizada a versão *DD-WRT v24-sp2*. Como sistema operacional optou-se pelo Ubuntu 10.04 pelo grande suporte e por ser *software* livre. Executando no sistema operacional a *IDE* de desenvolvimento *Eclipse Galileo* foi escolhida como *IDE* por seu conhecido suporte a programação *Java*, linguagem de programação utilizada para formalização do protótipo. A versão do *Java* utilizada foi a *Java*[™] *SE 6 Update 24*.

No entanto, apenas com o suporte nativo da linguagem de programação *Java* não foi possível implementar algumas funcionalidades. Para suprir esse necessidade bibliotecas de terceiros foram utilizadas. Segue abaixo a listagem delas e suas respectivas funções:

Bibliotecas

- *Java Communications 3.0 API*: é uma extensão *Java* que facilita a comunicação multi plataforma fornecendo o suporte às aplicações para o acesso a porta serial (RS-232). No protótipo, foi utilizada na comunicação entre o GPS e o computador, que se comunicam através de uma porta serial emulada via *USB*.
- *RXTX*: biblioteca utilizada em paralelo a *Java Communications* para a comunicação serial com o *GPS*.
- *Ganymed SSH-2 for Java*: é uma biblioteca o que implementa o protocolo *SSH-2* com *Java* puro. Ela permite a conexão com servidores *SSH*, suportando sessões *SSH*, encaminhamento de porta local e remoto, encaminhamento de fluxo local,

encaminhamento X11, SCP e SFTP. Essa biblioteca foi utilizada para a comunicação entre o computador e o *AP* para que o campo *SSID* do quadro *beacon* fosse constantemente alterado.

- *Jpcap*: é uma biblioteca *Java* para a captura e envio de pacotes na rede. Ela pode capturar pacotes *Ethernet*, *IPv4*, *IPv6*, *ARP/RARP*, *TCP*, *UDP*, e *ICMPv4*. Foi utilizada como interface para a captura de pacotes pelo computador com a placa de rede em modo promíscuo.

5.4 FLUXO DA INFORMAÇÃO

Inicialmente um programa é executado em laço infinito em um computador portátil dentro do veículo. Uma das funções desse programa é coletar as informações passadas pelo *GPS* em forma de sentenças *NMEA-0183 V3.01* (Sessão 3.3.7). O *GPS*, conectado através de uma porta *USB* que emula uma porta serial (Sessão 3.3.1) envia essas sentenças periodicamente com uma frequência de 5 Hz. O programa em laço infinito coleta as sentenças e as processa retirando as coordenadas. A partir desse momento um quadro é formado contendo as coordenadas e outras informações.

O *GPS* utilizado fornece várias sentenças *NMEA-0183* porém apenas as coordenadas geográficas tem interesse. Então, a sentença *GPRMC* pode ser usada. Segue abaixo um exemplo da sentença e suas coordenadas extraídas.

```
$GPRMC,184628.600,A,2735.9962,S,04831.0864,W,0.02,255.34,070211,,A*67
lat:2735.9963S
lon:04831.0862W
```

Como nas sentenças *GPRMC*, as coordenadas geográficas são fornecidas em *MinDec* (graus, minutos, minutos decimais) e o programa trabalha com graus decimais um algoritmo necessita ser executado para que a conversão seja feita. Por exemplo, dada a coordenada 79°56.93172W a conversão é feita seguindo os seguintes passos:

1. O número inteiro de graus é o mesmo fornecido (79)
2. Os graus decimais são os minutos decimais dividido por 60 ($56.93172/60 = 0.948862$)
3. Somam-se esses 2 valores obtidos ($79 + 0.948862 = 79.948862$)

4. Nega-se o número caso ele seja Sul (S) ou Oeste (W) (nesse caso Oeste (W), então, -79.948862)

Então, após as coordenadas terem sido convertidas para o formato usado no programa, um quadro é montado seguindo a estrutura conforme a Tabela 1.

Tabela 1: Estrutura de dados formada com as coordenadas obtidas do *GPS*. Tem por objetivo padronizar os dados enviados pela rede sem fio para os pontos infraestruturados às margens da rodovia.

Id do sistema	Id do veículo	Latitude	Longitude	Caracter de fim
6 bytes	1 byte	10 bytes	11 bytes	1 byte

Esse quadro é então enviado pelo roteador *WiFi* que encontra-se conectado ao computador portátil dentro do veículo. A arquitetura montada no veículo está ilustrada na Figura 18

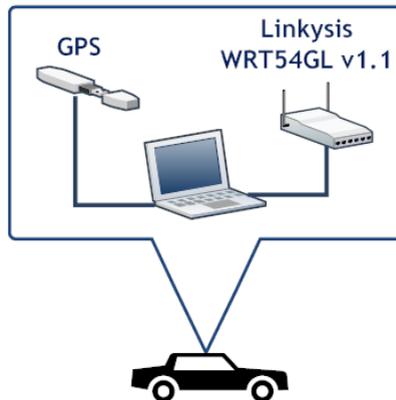


Figura 18: Arquitetura do veículo, através da qual as coordenadas são obtidas e transmitidas pela rede sem fio para as células de monitoramento.

Um ponto fixo na estrada equipado com um segundo roteador *WiFi* e uma câmera *PTZ* captura o pacote. Essa captura é realizada através de um programa que executa em laço infinito a procura dos

pacotes com as coordenadas do veículo. Tal programa roda no servidor central que se comunica com a câmera através de um rede *WiMAX* e depois *Ethernet*. Os quadros capturados são tratados e suas coordenadas enviadas para outro programa que as processa para transformá-los em comandos de *PTZ* para a câmera. Esses comandos são enviados para a câmera em forma de requisições HTTP (Subseção 3.3.6). Então a câmera executa os movimentos na seguinte ordem: movimento horizontal, a seguir vertical e logo depois *zoom*, focando o veículo emissor dos quadros com as coordenadas.

A imagem capturada pela câmera é então enviada de volta ao servidor através da rede *WiMAX*.

A Figura 19 ilustra o fluxo dos dados na arquitetura (a numeração entre parênteses informa a ordem na qual fluem os dados).

Algumas questões mais importantes serão abordados nas próximas sessões, como o cálculo dos valores de comando da câmera, envio e captura dos quadros pela *WiFi*.

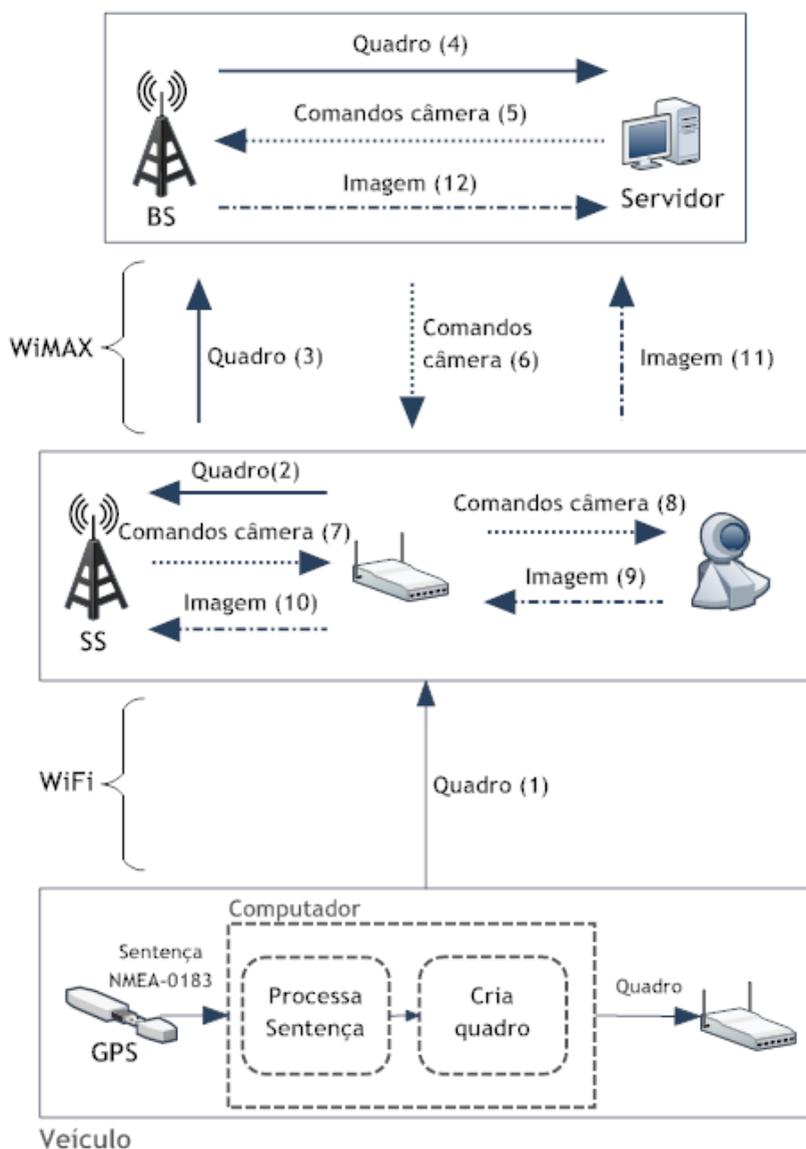


Figura 19: Fluxo dos dados do estudo de caso da arquitetura hierárquica de comunicação. A numeração entre parênteses representa a sequência de eventos.

5.5 ACOMPANHAMENTO VISUAL POR CÂMERA *PTZ*

Como descrito anteriormente, a câmera *PTZ* tem por objetivo acompanhar visualmente o assunto com base em suas coordenadas geográficas enviadas. No cenário idealizado para a arquitetura, cada câmera usada em sua célula local ficará fixada no topo de um poste ou em alguma posição estratégica em que tenha visão plena de toda a via sem possível obstrução de nenhum objeto. Esse acompanhamento visual se realiza através da variação dos parâmetros referentes aos 3 graus de liberdade que a câmera possui: rotação horizontal, rotação vertical e *zoom*. Os cálculos para a rotação horizontal e vertical foram baseados em fórmulas básicas da trigonometria e o cálculo da distância entre 2 coordenadas geográficas, enquanto o cálculo para a aplicação do *zoom* baseou-se em conceitos de óptica.

As equações para o cálculo da rotação horizontal e vertical retornam ângulos em radianos e a aplicação trabalha com ângulos em graus assim uma simples conversão é feita. A câmera aceita somente comandos que estejam no intervalo de $[-180^\circ, 180^\circ]$.

5.5.1 Cálculo da distância entre coordenadas geográficas

Para os cálculos de trigonometria a serem feitos, é necessário que as distâncias entre pontos sejam calculadas. Como os pontos utilizados são representados por coordenadas geográficas, precisamos utilizar um equacionamento específico. A fórmula desse cálculo é baseada na lei dos cossenos da trigonometria esférica e essa distância segue a linha geodésica, que é a curva de menor comprimento unindo dois pontos. Como o sistema de coordenadas terrestre é dividido em hemisférios, com os ângulos entre 0-90 e 0-180, faz-se necessário o ajuste na fórmula para estes ângulos limítrofes. Como as diferenças na altitude da superfície terrestre são insignificantes em relação ao raio da Terra, é possível ignorar esta variação sem comprometer o resultado do cálculo. Observando que como está sendo utilizado o raio médio, então os resultados para pontos próximos à linha do Equador serão subestimados e para pontos próximos aos polos serão superestimados.

O cálculo desta distância com as restrições citadas é feito através de (VENESS, 2010):

$$\begin{aligned}
 D = & ((\arccos(\cos(90 - Lat_1) \cos(90 - Lat_2) + \\
 & + \sin(90 - Lat_1) \sin(90 - Lat_2) \cos(|((360 + Lon_1) - \\
 & - (360 + Lon_2)|)))) 6371,004) 1000
 \end{aligned} \tag{5.1}$$

Onde:

- Lat_1 é a latitude do ponto 1
- Lon_1 é a longitude do ponto 1
- Lat_2 é a latitude do ponto 2
- Lon_2 é a longitude do ponto 2

Toda a expressão é multiplicada pelo raio médio da Terra e o resultado multiplicado por 1000 para a unidade da distância ser em metros.

5.5.2 Rotação horizontal

Com base na *Lei dos Cossenos* da trigonometria elaborou-se um sistema para o cálculo da rotação horizontal que a câmera deve realizar para o acompanhamento visual do assunto. Para que um triângulo imaginário seja formado, um ponto de calibração foi estabelecido em frente ao marco zero de movimentação horizontal da câmera. A Figura 20 ilustra toda a questão a respeito do ponto de calibração e trigonometria.

O ponto de calibração é posicionado em frente à câmera. Esse ponto fica em frente ao ponto representado pelo valor nulo do parâmetro de rotação horizontal. O ponto de calibração é estabelecido através de uma leitura de coordenadas geográficas feita por um *GPS* no lado oposto da via onde a câmera é instalada.

A posição da câmera também é registrada através da leitura de suas coordenadas geográficas realizada por um *GPS*.

Assim, podemos calcular o ângulo entre a reta, que a câmera faz entre ela e o ponto de calibração, e a reta que é formada entre ela e o veículo emissor de coordenadas. Na Figura 20 essas retas são representadas por d_2 e d_1 , respectivamente. O ângulo a ser calculado para o rotacionamento horizontal da câmera é o representado pela letra α na figura.

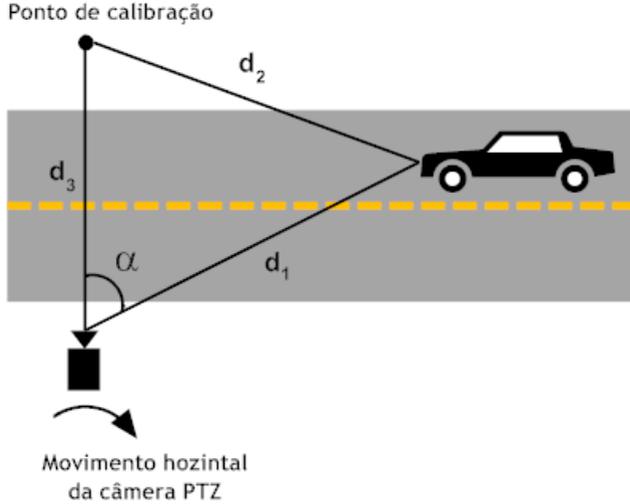


Figura 20: Trigonometria para a rotação horizontal da câmera *PTZ*. Onde: α é o ângulo a ser calculado e d_i distância entre dois pontos.

Baseado na notação atribuída na Figura 20, a equação para obtenção do ângulo α é feita através da *Lei dos Cossenos* e fica arranjada da seguinte maneira:

$$\alpha = \arccos\left(\frac{d_1^2 + d_3^2 - d_2^2}{2d_1d_3}\right) \quad (5.2)$$

Note que d_3 , posição da câmera e posição do ponto de calibração são valores constantes.

5.5.3 Rotação vertical

O equacionamento para o cálculo da rotação vertical da câmera torna-se mais simples nesse caso pois a reta formada pela normal que une o solo à câmera compõe um triângulo retângulo. A partir disso, podemos utilizar uma simples função trigonométrica, arco tangente. A Figura 21 ilustra o triângulo formado.

Baseado na notação atribuída na Figura 21, a equação para obtenção do ângulo β é dada por:

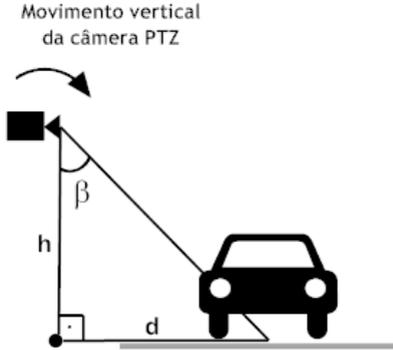


Figura 21: Trigonometria para a rotação vertical da câmera *PTZ*. Onde: β é o ângulo a ser calculado, d e h distância entre dois pontos.

$$\beta = \arctan\left(\frac{d}{h}\right) \quad (5.3)$$

5.5.4 Zoom

Para entender como o *zoom* é calculado faz-se necessário, uma explicação básica de óptica, mais especificamente sobre distância focal.

A distância focal de uma lente é definida como a distância em *mm* do centro óptico da lente até o ponto focal, o qual é localizado no sensor se o assunto (no infinito) estiver em foco. A lente da câmera projeta parte do cenário em seu sensor. O campo de visão é determinado pelo ângulo de visão da lente para fora do cenário e pode ser medido verticalmente e horizontalmente. Sensores maiores possuem um campo de visão maiores e podem capturar mais do cenário. O campo de visão associado a uma distância focal é geralmente baseado no filme de 35mm, dada a popularidade desse formato comparado aos outros.

Na fotografia de 35mm, lentes com uma distância focal de 50mm são chamadas de “normais” por que podem trabalhar sem redução ou ampliação e então criam imagens na maneira como se enxerga a cena a olho nu.

Uma mudança na distância focal permite a aproximação do assunto ou o afastamento dele e, portanto, um efeito indireto sobre a

perspectiva (AXIS, 2011).

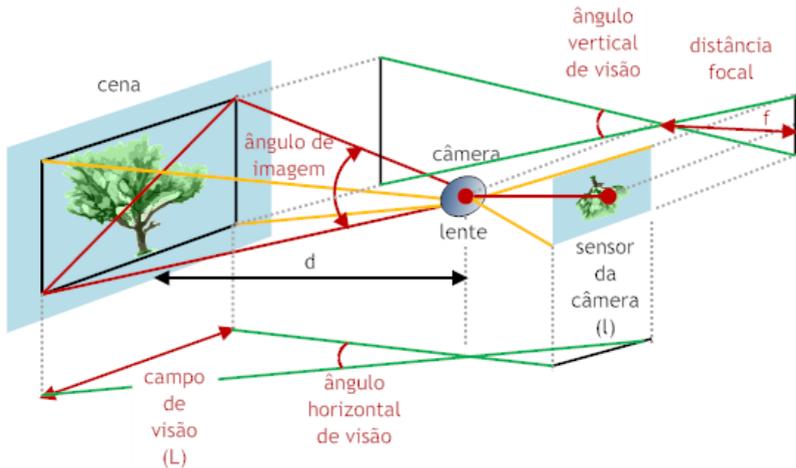


Figura 22: Esquemática dos elementos geométricos envolvidos na projeção de uma imagem no sensor de uma câmera através de sua lente.

A partir da distância focal pode-se calcular o *zoom* óptico de uma câmera por uma simples equação:

$$\text{Zoom óptico} = \frac{\text{distância focal máxima}}{\text{distância focal mínima}} \quad (5.4)$$

Na câmera *PTZ* usada, *Axis 214 PTZ*, o *zoom* óptico dela que possui lente 4.1-73.8mm é de 73.8/4.1 ou 18X.

A partir dessa fórmula e com base na Figura 22 obteve-se uma fórmula para o cálculo do *zoom* a ser aplicado no assunto com apenas 2 parâmetros de entrada. Esses parâmetros são a distância em que o assunto se encontra da câmera, calculado através da distância entre duas coordenadas (Equação 5.1), e a largura do campo de visão que deseja-se focar.

Com base nos seguintes características da câmera *PTZ*:

- A imagem fornecida pela câmera está na proporção 4:3
- Maior distância focal: 73,8mm
- Menor distância focal: 4,1mm

- Tamanho do sensor da câmera: 1/4"(3,6 x 2,7 mm)

E através de uma simples semelhança de triângulos contidos na Figura 22 podemos facilmente deduzir a fórmula para o cálculo da distância focal f .

$$\frac{\text{distância focal}}{\text{distância do assunto à câmera}} = \frac{\text{largura do sensor}}{\text{largura do campo de visão}} \quad (5.5)$$

Isolando-se a distância focal, temos que:

$$f = \frac{l}{L}d \quad (5.6)$$

Então, com o valor da distância focal calculado para uma certa distância do assunto à câmera podemos substituí-lo na Fórmula 5.4 e obtermos o *zoom* óptico necessário a ser aplicado. Como a interface da câmera nos permite o acesso a uma variável de *zoom* óptico, torna-se simples a emissão/execução do comando.

5.5.5 Execução de Comandos

A Câmera *Axis 214 PTZ* utilizada na arquitetura é uma câmera *IP*, que se comunica através de rede cabeada *Ethernet*. A fabricante da câmera fornece uma interface aberta de programação (*API*) com integração flexível, expansível e que pode ser usada em outros sistemas. Essa interface chama-se *VAPIX*[®].

O *VAPIX*[®] fornece funcionalidades para requisição de imagens, controle dos movimentos *PTZ* e acesso a outros parâmetros internos. Tudo baseado no protocolo *HTTP*.

Para enviar qualquer tipo de comunicação com a câmera é necessário primeiramente realizar uma autenticação *HTTP*. Por exemplo, para realizar uma rotação da câmera horizontalmente até o ângulo de 30° basta, após se autenticar, enviar a seguinte requisição:

```
http://<servername>/axis-cgi/com/ptz.cgi?pan=30
```

Onde <servername> é o endereço *IP* da câmera.

Então uma nova interface foi gerada via programação bom base no *VAPIX*[®] para controlar a câmera. Analisando as requisições foi possível identificar que o *VAPIX*[®] não tem um tratamento para

requisições consequentes em um curto período de tempo. Quando duas ou mais requisições são enviadas quase simultaneamente a câmera, ela randomicamente não executa até o fim certas requisições. Por exemplo, ao solicitar que ele execute o movimento de rotação vertical para o ângulo de 90° e antes de ela finalizar esse movimento ela for solicitada a rotacionar 180° , na horizontal existe a possibilidade de ela interromper o primeiro movimento para a execução do segundo.

A partir dessa observação implementou-se um método que coloca as requisições em uma fila e só às executa após um determinado tempo. Analisando a especificação técnica da câmera foi possível estipular esse tempo com base nas velocidades angulares fornecidas, $100^\circ/s$ e $90^\circ/s$, rotação horizontal e vertical respectivamente.

5.6 COMUNICAÇÃO *WIFI* SEM CONEXÃO

No *SORVES* as funções de equipamentos de comunicação *WiFi* são invertidos, fisicamente falando, pois o emissor de pacotes utiliza-se de um *AP* e o receptor pode ser desde um simples cliente como um *AP* com suas interfaces de rede em modo promíscuo. Como comentado anteriormente, o veículo é equipado com um *AP* que encontra-se constantemente em laço infinito coletando informações do *GPS* e compondo sentenças textuais a serem sobrecarregadas no campo de *SSID* do quadro *beacon*. O ponto fixo na beira da via encontra-se em modo promíscuo, isto é, sua interface de rede não fica associada a nenhum *AP* e passa a coletar todos os pacotes que transitam na rede *WiFi*.

No campo *SSID* do quadro *beacon*, uma estrutura foi definida para a organização dos dados. Essa estrutura com 32 *bytes* de comprimento foi denominada de *SSID Frame*, como ilustrado nas Tabelas 1 e 16. A estrutura resultante pode ser descrita como a seguir. No campo *Id do sistema* foram destinados 6 *bytes* para armazenar um identificador do projeto, como padrão o campo é preenchido com a sentença textual *SORVES*— o nome do nosso estudo de caso. Ao campo *Id do veículo* destinou-se apenas 1 *byte* o que restringe a uma representação limitada pela quantidade de caracteres que a tabela ASCII abriga, 128. Atualmente no projeto esse campo não possui nenhuma função pois o objetivo é rastrear apenas um veículo em especial por vez. Os campos *Latitude* e *Longitude* são destinados a armazenar as coordenadas geográficas do veículo representadas em graus decimais. Por último, existe o campo

Caracter de fim onde um caractere especial foi escolhido para marcar o fim do *SSID Frame*. Todos os campos são trabalhados em um alto nível, a sobrecarga do campo é feita somente através de caracteres *ASCII*, sendo assim, cada carácter representa 1 byte.

A cada segundo (frequência de captação de coordenadas geográficas pelo *GPS*) um *SSID Frame* é montado. O campo *SSID* do quadro *beacon* é sobrecarregado para ser enviado pelo *AP* em seu constante anúncio de presença.

Alteração de SSID do quadro *beacon*

Para o acesso a parâmetros de configuração do *AP* foi utilizada uma conexão *SSH*. Tal conexão só foi possível após a instalação de um novo *firmware* no *AP*. Esse *firmware* é baseado em um código aberto e no sistema operacional *Linux*, permitindo assim um acesso mais flexível ao hardware do *AP*. O tempo para mudança de *SSID* por *SSH* foi medido via programação e obteve o valor de $\approx 0,06$ s ficando então limitado pelo período de obtenção de coordenadas geográficas que é dado pelo *hardware* do *GPS* utilizado, 0,2s.

Captura de quadros *beacon*

No lado do ponto fixo à beira de estrada, equipado com a câmera e um *AP* em modo promíscuo, a interface *WiFi* fica constantemente à procura de quadros *beacon*. Encontrado um quadro, o aplicativo faz a busca no campo *SSID* pela sentença textual do *Id do Sistema*, após encontrada, essa sequência textual é quebrada a fim de parametrizar-se os valores do *Id do veículo*, *Latitude* e *Longitude*, valores constituintes do *SSID Frame*. Então, esses valores são enviados, processados e transformados em comandos de movimentação para a câmera.

Através de uma medição realizada pela ferramenta *Wireshark*, analisador de protocolo de rede, foi possível estimar a captura em um período de 1 quadro a cada ≈ 0.2 s. Como o *SSID* possui 32 bytes, estabelecemos uma transferência de ≈ 1280 bps. Essa taxa é suficientemente alta para a transmissão de coordenadas, visto que ainda possuímos a limitação temporal da mecânica para a movimentação dos 3 graus de liberdade da câmera *PTZ*. Na seção 5.5 foram abordadas essas questões de tempo da câmera.

AP com *Linux* embarcado

O *firmware* de código aberto escolhido para o AP foi o *DD-WRT* devido ao maior suporte e comunidade desenvolvedora encontrada na *web*. *DD-WRT* é um *firmware* (código de programação que um dispositivo executa) de código aberto compatibiliza-se a uma grande variedade de sistemas embarcados e roteadores *WLAN*. A ênfase principal recai sobre o fornecimento de uma manipulação o mais fácil possível enquanto suporta ao mesmo tempo um grande número de funcionalidades no contexto do *hardware* usado.

A interface gráfica é logicamente estruturada e operada em um navegador padrão, então mesmo pessoas que não são técnicos podem configurar o sistema através de simples passos.

Além do fácil manuseio, velocidade e estabilidade são também os focos de desenvolvimento do *DD-WRT*. Comparado aos programas pré instalados em muitos roteadores *WLAN*, o *DD-WRT* permite a operação confiável com maior clareza das funcionalidades o que também atende à demanda de profissionais.

Alguns parâmetros no AP foram estabelecidas com base em pesquisas como (ERIKSSON; BALAKRISHNAN; MADDEN, 2008b; BYCHKOVSKY et al., 2006; OTT; KUTSCHER, 2004; GONZÁLEZ et al., 2008; WELLENS; WESTPHAL; MAHONEN,). Pode-se destacar:

- Modo de operação: IEEE 802.11g
- Canal utilizado: 10 - 2.457 GHz
- Intervalo de quadros *beacon*: 10 ms

O modo IEEE 802.11b foi escolhido devido a maior taxa de transferência obtida nos testes realizados por (GONZÁLEZ et al., 2008; WELLENS; WESTPHAL; MAHONEN,). O canal fixo foi escolhido para diminuir o tempo de sondagem de quadros de *beacon*. O intervalo de quadros *beacon* foi escolhido com base no menor tempo que o *firmware* tem à disposição. Vale a pena citar que o *firmware* proprietário que o AP possuía anteriormente limitava o valor a 20 ms contra os 10 ms permitidos pelo *DD-WRT*. Com intervalo menor mais quadros *beacon* são transmitidos, portanto maior confiabilidade no envio das informações é obtido. Visto que, o envio de informações é limitado pela troca de *SSID* na comunicação *SSH*, como citado anteriormente.

5.7 WIMAX

Uma estrutura teste para comunicação *WiMAX* foi montada na Universidade Federal de Santa Catarina onde a antena *BS* ficou localizada no topo da casa do estudante e uma antena *SS* no topo do Superintendência de Governança Eletrônica e Tecnologia da Informação e Comunicação (*SeTIC*), separados por uma distância aproximada de 1 Km. Tais posições foram escolhidas a fim de estabelecer uma comunicação em *LOS*. A Figura 23 ilustra a posição das antenas instaladas na universidade e a Figura 24 ilustra as antenas, *SS* à esquerda e *BS* à direita.



Figura 23: Antenas *WiMAX* instaladas na UFSC para testes do *SORVES*. A antena *SS* ficou localizada no topo do *SeTIC* e a antena *BS* no topo da casa do estudante.



Figura 24: Antenas *WiMAX*. À esquerda a antena *SS* e à direita a antena *BS*

5.8 MODELAGEM DO PROTÓTIPO

A código fonte da aplicação gerada para testar a arquitetura proposta foi dividida nos seguintes pacotes e suas respectivas classes:

- camera
 - Camera
 - CameraFrame
 - ComandaCamera
 - Coordenadas
 - MyAuthenticator
 - PrincipalCamera
- gps
 - PrincipalGPS
 - GPSTokens
 - SerialCommGPS
 - ThreadProcessaSerial

- sniffer
 - Sniffer
 - SnifferThread
 - TrataPacote
- ssid
 - ModificaSSID
 - SSIDFrame
- outros
 - Constantes

As classes *ComandaCamera*, *Coordenadas*, *MyAuthenticator* e *PrincipalCamera* são responsáveis pelos cálculos e execução de movimentos da câmera *PTZ*. *Camera* e *CameraFrame* pela visualização das imagens obtidas pela câmera. *PrincipalGPS*, *GPSTokens*, *SerialCommGPS* e *ThreadProcessaSerial* tem o objetivo de obter as coordenadas geográficas do veículo. *Sniffer*, *SnifferThread* e *TrataPacote* realizam a captura dos quadros *beacon* para obtenção da posição geográfica do veículo. *ModificaSSID* e *SSIDFrame* tratam da estruturação do quadro *SSID* e da alteração do campo *SSID* do quadro *beacon* no roteador *WiFi*. Por fim, a classe *Constantes* possui apenas atributos de valores constantes usados na aplicação.

Para ilustrar graficamente as dependências, hierarquias e associações entre as classes digramas de classe do *UML* foram montados e estão representados no Apêndice A.

5.9 TESTES DO PROTÓTIPO

Alguns testes do *SORVES* foram realizados em laboratório. Em particular, a comunicação *WiFi* sem estabelecimento de conexão e a movimentação autônoma da câmera *PTZ* através da obtenção das coordenadas geográficas emitidas através da *WiFi*.

Abaixo as Figuras 25, 26, 27, 28 e 29 ilustram o *hardware* utilizado nesses testes.

A estrutura do prédio onde o laboratório está localizado não permite que o *GPS* obtenha sinal dos satélites para obter seu posicionamento geográfico. Assim, uma estrutura de dados foi utilizada para armazenar as coordenadas obtidas através do software

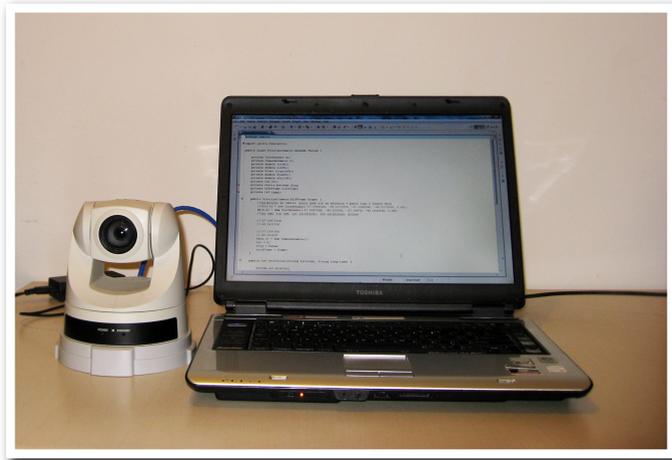


Figura 25: Computador ligado a câmera *PTZ* realizando o papel da central de controle e monitoração, porém sem o uso da rede *WiMAX*. Os quadros *beacon* são coletados, tratados e transformados em comandos de movimentação da câmera para então receber a imagem focada pela câmera.



Figura 26: Câmera *PTZ* que equipa um ponto infraestruturado às margens da rodovia.

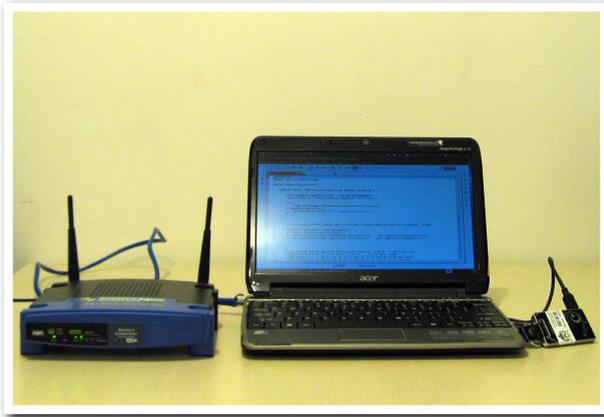


Figura 27: *Hardware* que equipa um veículo a ser rastreado. À direita, o roteador *WiFi* executando *Linux* embarcado; no centro, unidade de processamento responsável por coletar as coordenadas geográficas e transforma-las nos *SSID Frames*; e, na direita, o *GPS USB*.



Figura 28: Roteador *WiFi* executando *Linux* embarcado. Através desse *firmware* é possível acessar e modificar a variável responsável pelo *SSID* do quadro beacon.

Google Earth[®]. Tais coordenadas foram obtidas na Rua Delfino Conti, na frente do Centro Tecnológico da *UFSC*. A Figura 30 ilustra



Figura 29: *GPS USB* responsável por fornecer as coordenadas geográficas.

os pontos obtidos.

Inseridas essas coordenadas no *SORVES*, para emular o funcionamento do *GPS* e movimentação do carro, foi possível realizar a comunicação entre o *hardware*, que equipa um veículo, e o computador, que simula a central de controle e monitoramento. Esse computador está equipado de uma placa de rede *WiFi* e uma câmera *PTZ*, conforme a Figura 25 ilustra. A comunicação é realizada então pela rede *WiFi* sem estabelecimento de conexão: os *SSID frames* são transmitidos através do campo *SSID* do quadro *beacon* que é enviado pelo roteador *WiFi* (Figura 28). As Figuras 31 e 32 mostram o console de saída com os quadros *SSID* sendo formados e o quadros sendo capturados. A Figura 32 também mostra os comandos de movimentação formados para controle da câmera através da coordenadas extraídas dos quadros recebidos.

A Figura 33 é um exemplo da imagem obtida pelo aplicativo do *SORVES* responsável por capturar as imagens geradas pela câmera *PTZ*.

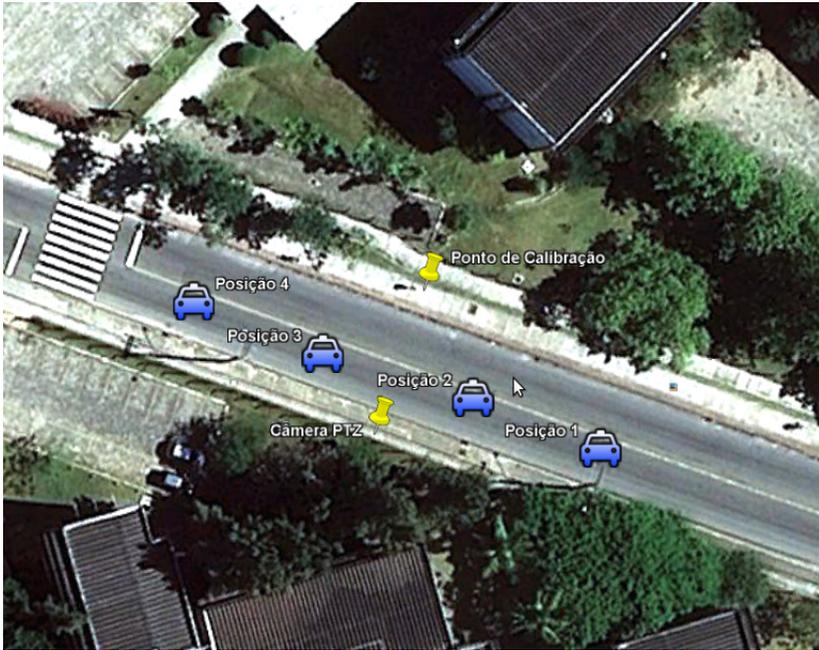


Figura 30: Mapa com os pontos utilizados no teste do *SORVES*. As posições: 1, 2, 3 e 4 simulam o carro em movimento no sentido crescente da numeração atribuída.

ExitCode: null

Latitude: -27.599764
Longitude: -48.517686
Setting SSID "SORVESa-27.599764-48.517686/"
ExitCode: null

Latitude: -27.599726
Longitude: -48.517830
Setting SSID "SORVESa-27.599726-48.517830/"
ExitCode: null

Latitude: -27.599682
Longitude: -48.517954
Setting SSID "SORVESa-27.599682-48.517954/"
ExitCode: null

Latitude: -27.599868
Longitude: -048.517262
Setting SSID "SORVESa-27.599868-048.517262/"
ExitCode: null" data-bbox="257 164 804 792"/>

```
<terminated> PrincipalGPS [Java Application] /usr/lib/jvm/java  
-----  
Latitude: -27.599807  
Longitude: -48.517564  
Setting SSID "SORVESa-27.599807-48.517564/"  
ExitCode: null  
-----  
Latitude: -27.599764  
Longitude: -48.517686  
Setting SSID "SORVESa-27.599764-48.517686/"  
ExitCode: null  
-----  
Latitude: -27.599726  
Longitude: -48.517830  
Setting SSID "SORVESa-27.599726-48.517830/"  
ExitCode: null  
-----  
Latitude: -27.599682  
Longitude: -48.517954  
Setting SSID "SORVESa-27.599682-48.517954/"  
ExitCode: null  
-----  
Latitude: -27.599868  
Longitude: -048.517262  
Setting SSID "SORVESa-27.599868-048.517262/"  
ExitCode: null
```

Figura 31: Console com os quadros *SSID* formados e enviados pelos quadros *beacon* do roteador *WiFi*.

```

<terminated> Sniffer [Java Application] /usr/lib/jvm/java-6-sun-1.6.0.24/bin/java (19/05/2011 16:26:39)
-----
Pacote: 1
  SSID: SORVESa-27.599807-48.517564/010300
  Latitude: -27.599807
  Longitude: -48.517564
-----
Feeding username and password for digest
For input string: "on"
REQUISICAO HTTP: http://169.254.144.218/axis-cgi/com/ptz.cgi?pan=-48
For input string: "on"
REQUISICAO HTTP: http://169.254.144.218/axis-cgi/com/ptz.cgi?tilt=0
REQUISICAO HTTP: http://169.254.144.218/axis-cgi/com/ptz.cgi?zoom=9992
Pacote: 2
  SSID: SORVESa-27.599764-48.517686/010300
  Latitude: -27.599764
  Longitude: -48.517686
-----
----- Camera -----
  Latitude: -27.599764
  Longitude: -48.517686
-----
For input string: "on"
REQUISICAO HTTP: http://169.254.144.218/axis-cgi/com/ptz.cgi?pan=61
Pacote: 3
  SSID: SORVESa-27.599726-48.517830/010300
  Latitude: -27.599726
  Longitude: -48.517830
-----
For input string: "on"
REQUISICAO HTTP: http://169.254.144.218/axis-cgi/com/ptz.cgi?tilt=-11
REQUISICAO HTTP: http://169.254.144.218/axis-cgi/com/ptz.cgi?zoom=1898
Pacote: 4
  SSID: SORVESa-27.599682-48.517954/010300
  Latitude: -27.599682
  Longitude: -48.517954
-----
----- Camera -----
  Latitude: -27.599682
  Longitude: -48.517954
-----
For input string: "on"
REQUISICAO HTTP: http://169.254.144.218/axis-cgi/com/ptz.cgi?pan=78
Pacote: 5
  SSID: SORVESa-27.599868-048.517262/010300
  Latitude: -27.599868
  Longitude: -048.517262
-----
For input string: "on"
REQUISICAO HTTP: http://169.254.144.218/axis-cgi/com/ptz.cgi?tilt=-5
REQUISICAO HTTP: http://169.254.144.218/axis-cgi/com/ptz.cgi?zoom=6173

```

Figura 32: Captura dos quadros *beacon* e consequente extração de coordenadas para formação de comandos de movimentação para a câmera.

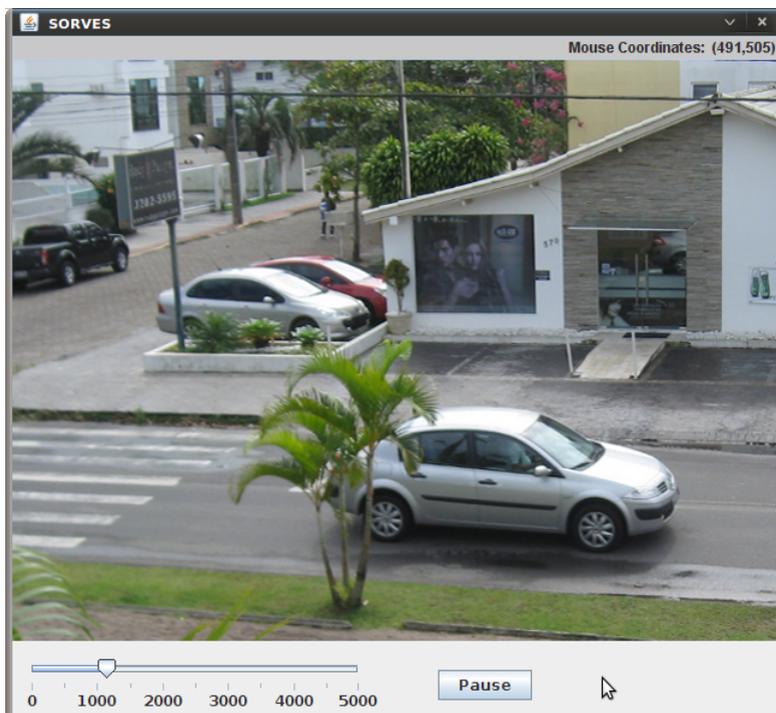


Figura 33: *Screenshot* do aplicativo responsável por obter imagens capturadas pela câmera.

5.10 CONSIDERAÇÕES DA IMPLEMENTAÇÃO

Relembrando, podemos destacar duas importantes contribuições nesse trabalho. A primeira diz respeito a comunicação *WiFi* sem estabelecimento de conexão no cenário de redes veiculares. A segunda trata da movimentação da câmera *PTZ* através da análise das coordenadas geográficas enviadas pelo veículo.

Em relação a comunicação *WiFi* podemos traçar um comparativo com outras implementações, as quais levam em média 10 s para estabelecer uma conexão. De todos trabalhos pesquisados podemos destacar (BALASUBRAMANIAN et al., 2007), o qual através de otimizações de *drivers* e *software*, obteve um tempo para estabelecimento de conexão de ≈ 400 ms. O *SORVES* trabalha com uma outra técnica adaptada para redes veiculares onde não existe o estabelecimento de conexão, porém essa técnica permitiu apenas uma comunicação com baixa taxa de transferência, ≈ 1280 bps. Em trabalhos, como o de (BYCHKOVSKY et al., 2006), obtiveram-se taxas de transferência de ≈ 30 KBytes/s.

Na movimentação da câmera *PTZ* não foi possível fazer uma comparação pois não se encontrou trabalhos que abordassem a movimentação da câmera com base em análise de coordenadas geográficas.

5.11 SUMÁRIO

Neste capítulo foram abordadas questões técnicas para a composição do estudo de caso *SORVES*. Foram listados os equipamentos especificadamente utilizados e *softwares* que deram apoio no desenvolvimento do *SORVES*. Tratou também de grandes desafios durante a implementação como as questões na comunicação *WiFi* sem associação, *WiMAX* e cálculos de óptica. Questões referentes a posicionamento geográfico, como o cálculo da distância entre duas coordenadas geográficas e manuseio de informações de baixo nível emitidas por um *GPS*, também foram discutidos. Também foi ilustrado o diagrama de classes do código fonte do *SORVES*. Por último, foi feito um relato de um teste realizado em laboratório abordando a movimentação da câmera e a comunicação *WiFi* sem o estabelecimento de conexão.

6 CONCLUSÃO

6.1 REVISÃO DA MOTIVAÇÃO E OBJETIVO

Com o rápido avanço dos dispositivos de comunicação sem fio devido ao seu baixo custo de implementação e popularização das tecnologias, novas implementações tem surgido conforme a tecnologia se aperfeiçoa. Recentemente, com a consolidação dos padrões de rede sem fio IEEE 802.11 e 802.16 e também do aumento da necessidade por soluções para mobilidade urbana, criou-se espaço para o desenvolvimento de aplicações de monitoramento e controle de tráfego urbano de fácil implementação, isto é, sem necessidade de grandes investimentos em infra estrutura nos atuais centros urbanos. Formalizadas com diferentes propósitos de alcance, largura de banda e flexibilidade de uso (mobilidade, facilidade de configuração de nodos, etc.), essas tecnologias podem ser combinadas para atender vários requisitos da gerência da operação do tráfego.

Então, nesse trabalho a meta foi desenvolver uma arquitetura hierárquica de comunicação para o monitoramento visual automatizado de veículos especiais. Para isso baseou-se na comunicação sem fio dos protocolos IEEE 802.11 e 802.16; para o monitoramento visual: uma câmera *PTZ*; e para a automatização do processo: coordenadas geográficas emitidas pelo veículo em movimento. Essa coordenadas são convertidas pelo sistema em comandos para movimentação da câmera e conseqüente centralização do veículo na cena captada. Para mostrar a viabilidade da arquitetura, uma ferramenta denominada *SORVES* foi desenvolvida e avaliada.

6.2 VISÃO GERAL DO TRABALHO

Com o intuito de investigar questões técnicas relativas ao emprego de tecnologias de comunicação sem fio para gerência de tráfego foi examinada uma hierarquização de protocolos de comunicação sem fio envolvendo tecnologias de grande disseminação atual no mercado. Em especial, são estudadas as técnicas de *WiFi* (IEEE 802.11) (IEEE, 2010) e *WiMax* (IEEE 802.16) (IEEE, 2003) e seu potencial uso na monitoração e controle do tráfego urbano (ALVES FEHMI B. ABDESSLEM, 2008; CAVALCANTI, 2008). Um

cenário de aplicação é mostrado na Figura 1, que ilustra a necessidade de comunicação de veículos com os semáforos e destes com centrais de controle e gerência de tráfego. Para a comunicação entre veículos e pontos infraestruturados, comunicação de curta distância, foi usado o *WiFi*; para a comunicação entre esses pontos e uma central de controle e monitoramento, comunicação de longa distância, foi utilizado o *WiMAX*. O *gateway* entre esses protocolos é realizado através de portas *ethernet* de um roteador, como discutida no Capítulo 4.

Um estudo de caso foi desenvolvido para testar a arquitetura proposta. Trata-se do sistema denominado *SORVES*(Software Rastreador Visual de Veículos Especiais Baseado em Redes Sem Fio e Sistema Global de Posicionamento). Esse sistema tem como objetivo a automatização do processo de monitoramento visual de veículos especiais. Esse monitoramento é baseado em uma câmera *PTZ* que faz a movimentação em três direções diferentes (horizontal, vertical e *zoom*) para centralizar o veículo na imagem captada. Para essa movimentação da câmera, coordenadas geográficas são enviadas via *WiFi* para o ponto fixo às margens da rodovia assim, através do uso da geometria analítica e noções básicas de óptica esses movimentos (horizontal,vertical e *zoom*) são calculados.

6.3 CONTRIBUIÇÕES

Duas grandes dificuldades foram encontradas e superadas. A primeira e mais complexa, trata da comunicação *WiFi* sem estabelecimento de uma conexão. A segunda, trata dos cálculos envolvidos para a movimentação da câmera.

Para a comunicação sem estabelecimento de conexão foi utilizada a seguinte estratégia: o veículo a ser monitorado porta um conjunto de equipamentos composto por uma unidade de processamento de dados(nos testes, um *notebook*), um *GPS* e um roteador *WiFi*. As coordenadas geográficas atuais que representam a posição atual do veículo são obtidas pelo *notebook* em um laço infinito. Nessa informação um identificador do veículo e do sistema são anexados. Então uma sentença de caracteres *ASCII* é formada. Essa sentença é atribuída ao campo *SSID* (nome legível da rede) do quadro *beacon*. Tal quadro tem por objetivo anunciar a rede do roteador do veículo e sua transmissão não possui um destinatário. O período de emissão desse quadro é de 10 ms (tempo mínimo imposto

pelo hardware). A outra extremidade, a receptora, coleta esse quadro, contendo as coordenadas e identificadores atribuídos ao campo *SSID*, em pontos fixos às margens da rodovia (*APs*), os quais estão em um modo de constante captura de quadros *WiFi* a transitar no ambiente. Identificado os quadros com o *ID* do sistema, as coordenadas contidas nesse quadro são extraídas e convertidas em comandos para movimentação da câmera.

A segunda contribuição trata da movimentação horizontal, vertical e de *zoom* da câmera através da análise da posição atual do veículo obtida por coordenadas geográficas. Para o cálculo da movimentação horizontal e vertical foi usada a *Lei dos Cossenos*. No movimento horizontal, um triângulo no plano horizontal é formado pelas coordenadas geográficas da câmera, ponto de calibração localizado em frente à câmera no outro lado da rodovia, e pelo posição atual do veículo. No movimento vertical, um triângulo reto no plano vertical é formado pela posição da câmera, do veículo e da altura que a câmera se encontra do solo. Já o movimento de *zoom* óptico é feito através de noções de básicas de óptica, onde a distância obtida pelo cálculo da diferença das posições da câmera e do veículo junto com características da câmera, como tamanho do sensor e distância focal, são parâmetros do cálculo.

Essas duas contribuições foram abordadas em maiores detalhes no Capítulo 4.

6.4 TRABALHOS FUTUROS

Muitos aspectos podem ser melhorados nesse trabalho. Iniciando pelo aumento da complexidade da aplicação desenvolvida que atualmente só suporta o acompanhamento de um único veículo emitindo sua posição na via. O hardware presente no veículo em movimento também pode ser otimizado. Atualmente ele está equipado por um roteador *WiFi*, um *GPS* e um *notebook*.

Todo o sistema em si está sintetizado em apenas uma instância, isto é, só funcionará para 1 veículo comunicando-se com 1 ponto fixo, equipado com 1 *AP* e 1 câmera *PTZ* às margens da rodovia, que transmite os dados para 1 central através de 1 antena *WiMAX BS* a uma *SS*.

Outro ponto que poderia ser melhor explorado é a comunicação *WiFi* entre o veículo e o *AP*. Uma modificação de *drivers* das placas de redes para explorar melhor os campos dos quadros *beacon* assim

como dos quadros emitidos pelo cliente, quadros de resposta (*probe request frame*). Com isso teríamos uma comunicação com maior taxa de transferência e nos 2 sentidos, cliente para servidor e servidor para cliente.

A comunicação *WiFi* no sistema não necessita de uma grande confiabilidade dos dados, visto que uma mesma posição do veículo é enviada consecutivas vezes e que existe a limitação temporal imposta pela movimentação da câmera *PTZ*. Porém, se houvesse a necessidade de utilizar essa comunicação *WiFi* sem estabelecimento de conexão para uma outra aplicação técnicas de confiabilidade deveriam ser implementadas.

APÊNDICE A – Diagramas de classe

Representado nas Figuras 34, 35, 36, 37, 38 e 39 estão os diagramas de classe. Eles foram montados para ilustrar as dependências, associações e hierarquia entre classes e pacotes.

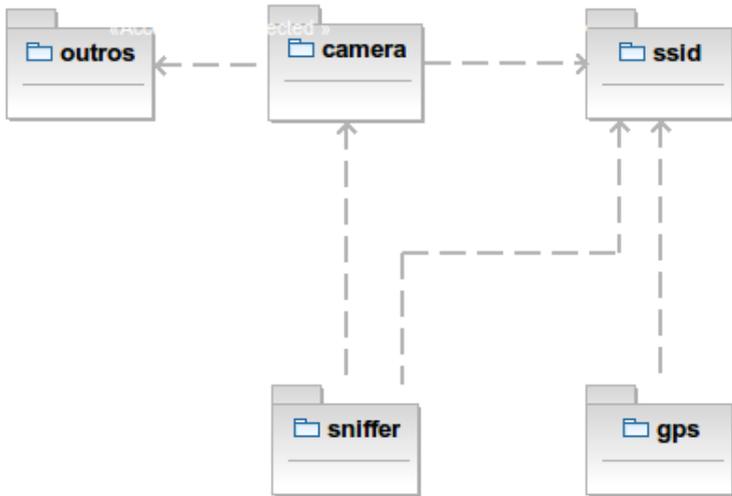


Figura 34: Dependência entre os pacotes.

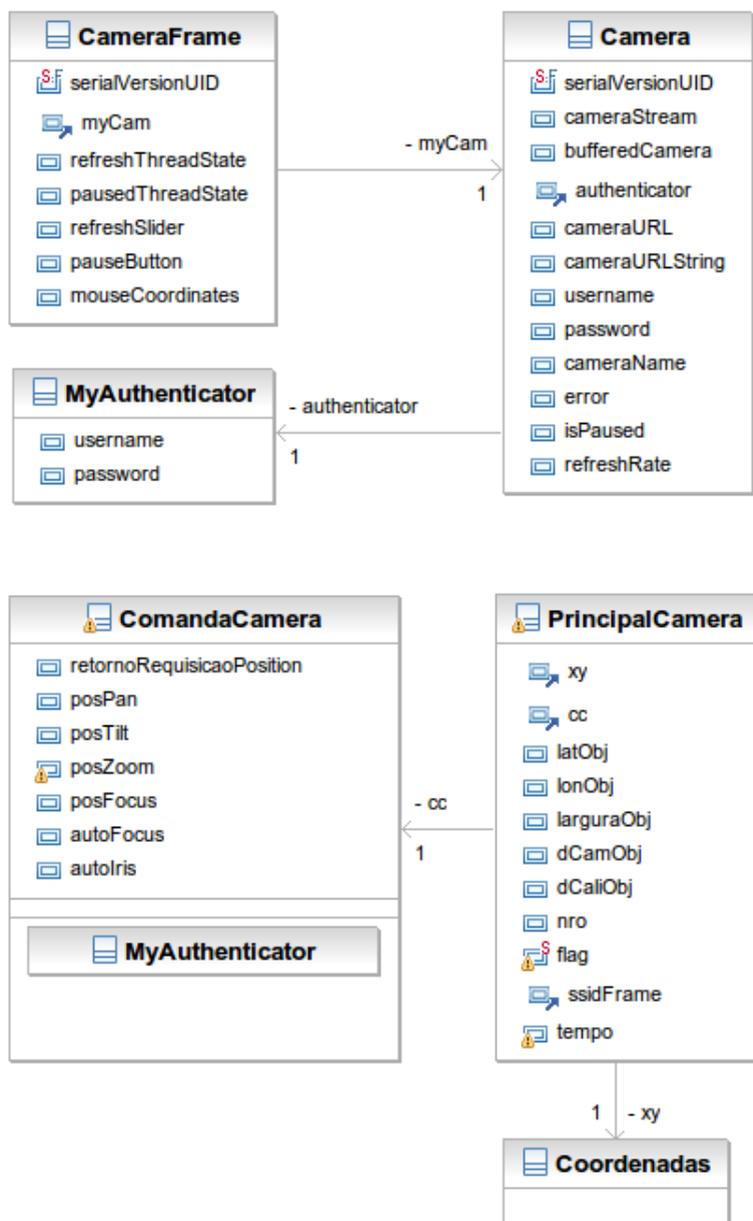


Figura 35: Diagrama de classe do pacote camera.

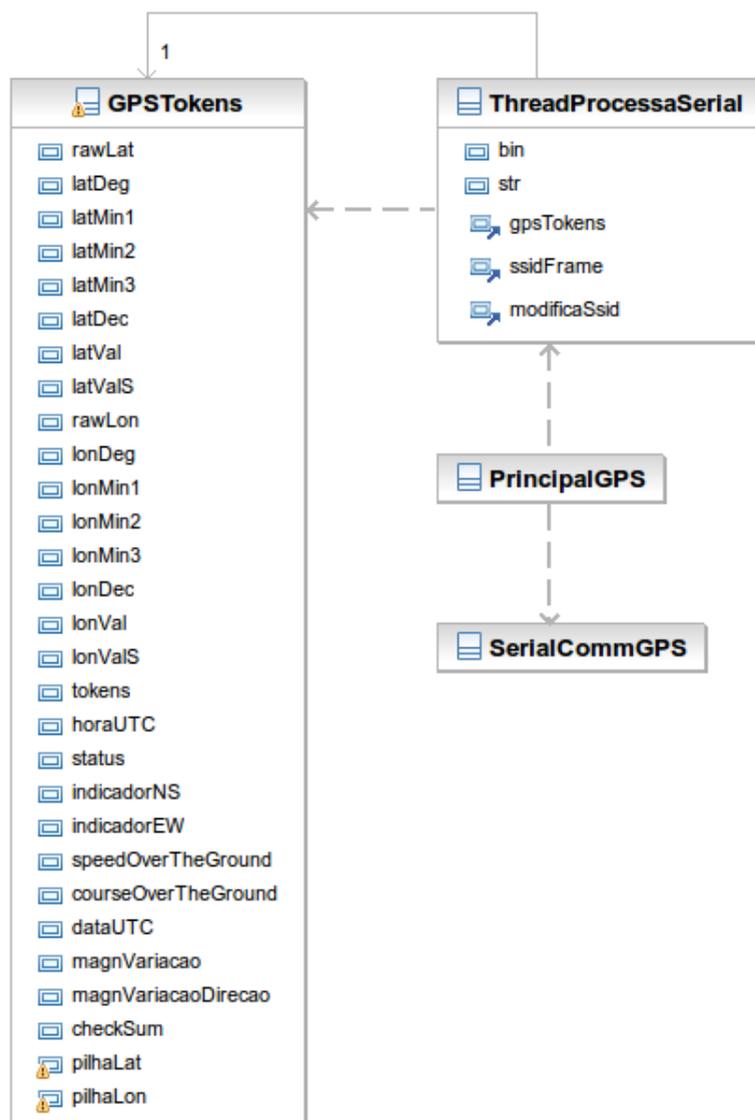


Figura 36: Diagrama de classe do pacote gps.

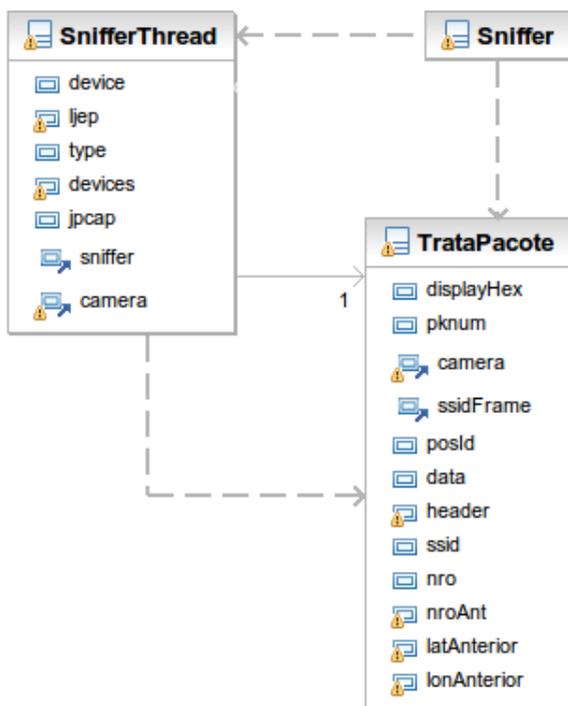


Figura 37: Diagrama de classe do pacote sniffer.

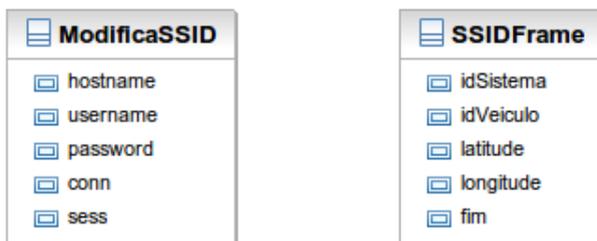


Figura 38: Diagrama de classe do pacote ssid.



Figura 39: Diagrama de classe do pacote outros.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES FEHMI B. ABDESSLEM, S. R. C. M. E. M. C. L. H. M. K. C. M. G. R. M. D. d. A. e. O. C. M. B. D. Rafael dos S. Uma análise experimental da capacidade de redes ad hoc veiculares. *XXVI Simpósio Brasileiro de Telecomunicações - SBrT'08*, 2008.

ALVES, R. et al. Uma análise experimental da capacidade de redes ad hoc veiculares. *XXVI SIMP OSIO BRASILEIRO DE TELECOMUNICAÇÕES SBrT2008*, 2008.

ALVES, R. et al. Redes veiculares: Princípios, aplicações e desafios. *Minicursos do Simpósio Brasileiro de Redes de Computadores, SBRC*, 2009.

AXELSON, J. *Serial Port Complete: COM Ports, USB Virtual COM Ports, and Ports for Embedded Systems*. 2nd. ed. [S.l.]: Lakeview Research, 2007. ISBN 193144806X, 9781931448062.

AXIS. *Sobre o vídeo em rede*. Mar 2011. <<http://www.axis.com>>.

BACIOCCOLA, A. et al. Ieee 802.16: History, status and future trends. *Computer Communications*, Elsevier, v. 33, n. 2, p. 113–123, 2010. ISSN 0140-3664.

BALASUBRAMANIAN, A. et al. Web search from a bus. In: *ACM. Proceedings of the second ACM workshop on Challenged networks*. [S.l.], 2007. p. 59–66.

BARRETT, D. J.; SILVERMAN, R. E. *SSH, The Secure Shell: The Definitive Guide*. Sebastopol, CA, USA: O'Reilly & Associates, Inc., 2001. ISBN 0596000111.

BAZZAN, A.; KLÜGL, F. Sistemas inteligentes de transporte e tráfego: uma abordagem de tecnologia da informação. *Anais das Jornadas de Atualização em Informática*, 2007.

BYCHKOVSKY, V. et al. A measurement study of vehicular internet access using in situ wi-fi networks. In: *Proceedings of the 12th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2006. (MobiCom '06), p. 50–61. ISBN 1-59593-286-0. <<http://doi.acm.org/10.1145/1161089.1161097>>.

CAVALCANTI, S. R. *VEER: Um Algoritmo de Seleção de Pares em Redes AD-HOC Veiculares*. Dissertação (Mestrado) — Universidade Federal do Rio de Janeiro, COPPE, 2008.

CHANDRA, R. et al. Beacon-stuffing: Wi-fi without associations. IEEE Computer Society, Los Alamitos, CA, USA, 2007.

EKLUND, C. et al. Ieee standard 802.16: a technical overview of the wirelessmair air interface for broadband wireless access. *Communications Magazine, IEEE*, v. 40, n. 6, p. 98–107, jun. 2002. ISSN 0163-6804.

ERIKSSON, J.; BALAKRISHNAN, H.; MADDEN, S. Cabernet: vehicular content delivery using WiFi. In: ACM. *Proceedings of the 14th ACM international conference on Mobile computing and networking*. [S.l.], 2008. p. 199–210.

ERIKSSON, J.; BALAKRISHNAN, H.; MADDEN, S. Cabernet: vehicular content delivery using wifi. In: *Proceedings of the 14th ACM international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2008. (MobiCom '08), p. 199–210. ISBN 978-1-60558-096-8. <<http://doi.acm.org/10.1145/1409944.1409968>>.

FIGUEIREDO, L. *Sistemas inteligentes de transporte*. Tese (Doutorado) — Universidade do Porto, 2005.

FORCE, I. E. T. *Internet Engineering Task Force*. May 2011. <<http://www.ietf.org/>>.

G1. *Lentidão chega a 194 km e SP continua em estado de atenção*. Ago 2008. <<http://g1.globo.com>>.

GASS, R.; SCOTT, J.; DIOT, C. Measurements of in-motion 802.11 networking. IEEE Computer Society, 2006. ISSN 1550-6193.

GHOSH, A. et al. Broadband wireless access with wimax/802.16: current performance benchmarks and future potential. *Communications Magazine, IEEE*, v. 43, n. 2, p. 129–136, fev. 2005. ISSN 0163-6804.

GONZÁLEZ, V. et al. Experimental demonstration of the viability of ieee 802.11b based inter-vehicle communications. In: *Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities*. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer

Sciences, Social-Informatics and Telecommunications Engineering), 2008. (TridentCom '08), p. 1:1–1:7. ISBN 978-963-9799-24-0. <<http://portal.acm.org/citation.cfm?id=1390576.1390578>>.

HADALLER, D. et al. Vehicular opportunistic communication under the microscope. In: ACM. *Proceedings of the 5th international conference on Mobile systems, applications and services*. [S.l.], 2007. p. 206–219.

HEMPEL, M. et al. A wireless test bed for mobile 802.11 and beyond. In: ACM. *Proceedings of the 2006 international conference on Wireless communications and mobile computing*. [S.l.], 2006. p. 1003–1008. ISBN 1595933069.

IEEE. Ieee standard for local and metropolitan area networks — part 16: Air interface for fixed broadband wireless access systems—amendment 2: Medium access control modifications and additional physical layer specifications for 2-11 ghz. *IEEE Std 802.16a-2003 (Amendment to IEEE Std 802.16-2001)*, 2003.

IEEE. Ieee standard for local and metropolitan area networks part 16: Air interface for broadband wireless access systems. *IEEE Std 802.16-2009 (Revision of IEEE Std 802.16-2004)*, p. C1 –2004, 29 2009.

IEEE. Ieee standard for 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 amendment 6: Wireless access in vehicular environments. *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)*, p. 1 –51, 15 2010.

IEEE Standard for 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. *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, p. C1–1184, 12 2007.

LOUREIRO, C.; GOMES, M.; LEANDRO, C. Avaliação do desempenho nos períodos de pico do tráfego de interseções semaforizadas com controle centralizado em tempo fixo e real. In:

Anais do XVI Congresso de Pesquisa e Ensino em Transportes. [S.l.: s.n.], 2002. p. 365–376.

NAVDA, V. et al. MobiSteer: using steerable beam directional antenna for vehicular network access. In: ACM. *Proceedings of the 5th international conference on Mobile systems, applications and services*. [S.l.], 2007. p. 192–205.

NMEA. *National Marine Electronics Association - NMEA*. Mar 2011. <<http://www.nmea.org/>>.

OTT, J.; KUTSCHER, D. Drive-thru internet: Ieee 802.11b for "automobile" users. In: *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*. [S.l.: s.n.], 2004. v. 1, p. 4 vol. (xxxv+2866). ISSN 0743-166X.

SILVA, D. Sistemas inteligentes no transporte público coletivo por ônibus. Universidade Federal do Rio Grande do Sul. Escola de Engenharia. Programa de Pós-Graduação em Engenharia de Produção., 2000.

SILVA, R.; CASAGRANDE, R. Redes de Computadores- Gerenciamento de servidores Linux, a partir de dispositivos celulares com suporte a J2ME, utilizando protocolo de comunicação SSH. *Anais SULCOMP*, n. 0, 2010.

SILVA, R. F. *Caracterização da Mobilidade Veicular e o seu Impacto nas Redes Veiculares Tolerantes a Atrasos e Desconexões*. Dissertação (Mestrado) — Programa de Pós-Graduação em Engenharia de Sistemas e Computação, COPPE, da Universidade Federal do Rio de Janeiro, 2010.

TANENBAUM, A. S. *Redes de Computadores*. trad. 4 ed. Rio de Janeiro: Elsevier, 2003.

TECHNET, M. *How 802.11 Wireless Works*. Mar 2003. <<http://technet.microsoft.com>>.

VENESS, C. *Internet Engineering Task Force*. May 2010. <<http://www.movable-type.co.uk/scripts/latlong.html>>.

WALKE, B. H.; MANGOLD, S.; BERLEMANN, L. *IEEE 802 Wireless Systems: Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistence*. 1., Auflage. ed. Wiley & Sons, 2007. Gebundene Ausgabe. ISBN 0470014393. <<http://www.worldcat.org/isbn/0470014393>>.

WELLENS, M.; WESTPHAL, B.; MAHONEN, P. Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios. In: IEEE. *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*. [S.l.]. p. 1167–1171. ISBN 1424402662. ISSN 1550-2252.

YLONEN, T. SSH-secure login connections over the Internet. In: *Proceedings of the 6th USENIX Security Symposium*. [S.l.: s.n.], 1996. p. 37–42.