



VLADIMIR PÍCCOLO BARCELOS

**ANÁLISE E EXPERIMENTAÇÃO DO PADRÃO
IEEE 802.11P EM REDES VEICULARES
HÍBRIDAS**

LAVRAS - MG

2014

VLADIMIR PÍCCOLO BARCELOS

**ANÁLISE E EXPERIMENTAÇÃO DO PADRÃO IEEE
802.11P EM REDES VEICULARES HÍBRIDAS**

Dissertação apresentada à Universidade Federal de Lavras, como parte das exigências do Programa de Pós-Graduação em Ciência da Computação, área de concentração em Redes de Computadores e Sistemas Embarcados, para a obtenção do título de Mestre.

Orientador

Dr. Luiz Henrique Andrade Correia

LAVRAS - MG

2014

**Ficha Catalográfica Elaborada pela Coordenadoria de Produtos e
Serviços da Biblioteca Universitária da UFLA**

Barcelos, Vladimir Pícolo.

Análise e experimentação do protocolo IEEE 802.11P em redes
veiculares híbridas / Vladimir Pícolo Barcelos. – Lavras : UFLA,
2014.

104 p. : il.

Dissertação (mestrado) – Universidade Federal de Lavras, 2014.

Orientador: Luiz Henrique Andrade Correia.

Bibliografia.

1. VANET. 2. V2X. 3. NS-2. 4. Hardware. 5. Desempenho de
VANETs. I. Universidade Federal de Lavras. II. Título.

CDD – 004.6

VLADIMIR PÍCCOLO BARCELOS

**ANÁLISE E EXPERIMENTAÇÃO DO PADRÃO IEEE
802.11P EM REDES VEICULARES HÍBRIDAS**

Dissertação apresentada à Universidade Federal de Lavras, como parte das exigências do Programa de Pós-Graduação em Ciência da Computação, área de concentração em Redes de Computadores e Sistemas Embarcados, para a obtenção do título de Mestre.

APROVADA em 28 de fevereiro de 2014.

Dr. Wilian Soares Lacerda UFPA

Dr. Daniel Fernandes Macedo UFMG

Dr. Luiz Henrique Andrade Correia

Orientador

LAVRAS - MG

2014

Dedico este trabalho ao meu Pai.

AGRADECIMENTOS

A Deus e minha família. Agradeço ao meu Orientador pela integral disponibilidade, valioso aprendizado e convivência. Obrigado Luiz pela paciência e atenção especial. À DGTI, que forneceu a maioria dos equipamentos necessários para a realização deste trabalho. Aos amigos Amarante, Wykret e Drury, pelo auxílio no desenvolvimento dos trabalhos. A todos os colegas de mestrado, pelo apoio e troca de experiências. Agradeço as agências de fomento CAPES e FAPEMIG, pelo apoio durante a realização dos trabalhos.

RESUMO

Redes veiculares *ad hoc* (*Vehicular Ad Hoc Networks* – VANETs) são caracterizadas por redes de comunicação de dados entre veículos, nas quais são trocadas informações sobre segurança do trânsito (como comunicação de acidentes) e/ou dados de propósito geral (como acesso à internet ou aplicações de entretenimento). É um tema desafiador que apresenta muitos problemas em aberto, por se tratarem de redes extremamente heterogêneas e dinâmicas, com características específicas. A maioria das pesquisas englobam apenas simulações, devido à disponibilidade restrita e alto custo de dispositivos comerciais que operam no padrão IEEE 802.11p, voltado para VANETs. Este trabalho propõe um dispositivo de comunicação customizável, de custo reduzido, capaz de suportar o padrão IEEE 802.11p e um link 3G de redundância. Além disso, um algoritmo de seleção do melhor link disponível é proposto para garantir que o veículo esteja conectado o maior tempo possível. Análises de desempenho do dispositivo e do padrão IEEE 802.11p foram realizadas por meio de simulações no NS-2 e por experimentos práticos. Resultados mostraram que o dispositivo foi capaz de realizar comunicações entre veículos, garantindo conectividade durante todo o tempo, quando o algoritmo de seleção do melhor link foi utilizado. Além disso, foi possível verificar que redes ajustadas conforme o padrão IEEE 802.11p podem ser utilizadas em comunicações veiculares. Nos cenários avaliados, foi possível verificar, tanto por meio de simulações quanto por meio de experimentações que, quanto maior o tamanho do pacote transmitido, maiores são a vazão, perda de pacotes e latência. Além disso, a velocidade de deslocamento dos nós impactou de forma negativa na vazão, latência e taxa de perda de pacotes. Atrasos menores que 100 ms foram obtidos usando-se o protocolo IEEE 802.11p. O mesmo não foi possível no link 3G durante os experimentos. O padrão IEEE 802.11p comprovou ser viável para aplicações de segurança e o link 3G para aplicações gerais insensíveis à latência.

Palavras-chave: redes veiculares, IEEE 802.11p, VANET, V2X, hardware 802.11p.

ABSTRACT

In vehicular ad hoc networks (VANETs) vehicles and other fixed devices can exchange information about traffic safety (such as accident reporting) and/or general purpose data (such as Internet access or entertainment applications). It's a challenging theme that has many open issues, for considering extremely heterogeneous and dynamic networks, with specific characteristics. Most researches encompass only simulations due to limited availability of IEEE 802.11p compatible devices. The IEEE 802.11p standard defines the physic and medium access control layers exclusively for VANETs. The cost of comercial devices also turns practical experiments prohibitive. This work proposes a low cost customizable device that supports the IEEE 802.11p and a 3G redundant link. Furthermore, an algorithm for selecting the best available link is proposed to ensure that the vehicle remains connected for the longest time possible. A performance analysis of both the device and the IEEE 802.11p standard was performed by means of NS-2 simulations and by practical experiments. Results showed that the device was able to perform communication between vehicles, guaranteeing connectivity for the entire time when the link selection algorithm was used. In addition, it was possible to verify that networks adjusted according to the IEEE 802.11p standard may be used in vehicular communications. Experiments and simulations showed that, in the evaluated scenarios, the greater the size of the transmitted packet, higher the throughput, packet loss and latency. Furthermore, node speeds had a negative impact on throughput, latency and packet loss rate. Delay values shorter than 100 ms were obtained using the IEEE 802.11p standard. The same was not possible with the 3G link during the experiments. The IEEE 802.11p standard showed to be feasible for emergency VANET applications. The 3G link may be used by general applications, in which latency is irrelevant.

Keywords: V2X, VANET, IEEE 802.11p, IEEE 802.11p hardware

LISTA DE FIGURAS

Figura 1	(a) Comunicação em um único salto. (b) Comunicação em múltiplos saltos.....	22
Figura 2	Ilustração de comunicações <i>ad hoc</i> entre veículos (V2V), veículos para infraestrutura (V2I) e comunicações híbridas (V2X).....	37
Figura 3	Os padrões IEEE 1609 da arquitetura WAVE e suas relações com o padrão IEEE 802.11p.....	37
Figura 4	Difusão normal.....	37
Figura 5	Difusão utilizando MPRs	38
Figura 6	Percurso de um pacote OGM.....	38
Figura 7	Foto de satélite do ambiente real utilizado nas simulações e experimentos.	47
Figura 8	Sequência de utilização das ferramentas para elaboração das simulações de VANETs.....	49
Figura 9	Routerboard modelo RB433AH.....	52
Figura 10	Routerboard modelo RB411U.....	52
Figura 11	Arquitetura geral dos dispositivos.....	53
Figura 12	Cartão miniPCI IEEE 802.11a/b/g da Mikrotik, modelo R52.....	55
Figura 13	Interface de geração do arquivo de configuração do sistema a ser compilado.....	57
Figura 14	Ferramenta RouterBOOT que configura a inicialização das RouterBoards.....	58
Figura 15	Validação da VANET por meio do RouterOS.....	60
Figura 16	Cenário utilizado nas simulações de avaliação das latências.....	65
Figura 17	Latência média no último nó a receber a informação (51 nós).....	68
Figura 18	Latência média no último nó a receber a informação (151 nós).....	68
Figura 19	Latência média da infraestrutura localizada no ponto <i>D</i> (51 nós).....	70
Figura 20	Latência média da infraestrutura localizada no ponto <i>D</i> (151 nós).....	70
Figura 21	Latência média da infraestrutura localizada no ponto <i>E</i> (51 nós).....	71

Figura 22	Latência média da infraestrutura localizada no ponto <i>E</i> (151 nós).....	71
Figura 23	Vazão média (51 nós).....	74
Figura 24	Vazão média (151 nós).....	75
Figura 25	Taxas máximas de transferência obtida proporcionada pelo protocolo IEEE 802.11p.	76
Figura 26	Posição dos nós utilizados nos testes dos protocolos de roteamento.	77
Figura 27	Latência média dos protocolos de roteamento OLSR e BATMAN.....	78
Figura 28	Média de perda de pacotes utilizando os protocolos de roteamento OLSR e BATMAN.....	79
Figura 29	Latência média das comunicações V2V, usando exclusivamente o padrão IEEE 802.11p.	81
Figura 30	Média da taxa de perda de pacotes em comunicações V2V, utilizando exclusivamente o padrão IEEE 802.11p. ...	83
Figura 31	Vazão média em comunicações V2V, usando exclusivamente o padrão IEEE 802.11p.	84
Figura 32	Latência média das comunicações V2X, usando exclusivamente o padrão IEEE 802.11p.	85
Figura 33	Taxa média de perda de pacotes, utilizando exclusivamente o padrão IEEE 802.11p em comunicações V2X.	86
Figura 34	Vazão média utilizando exclusivamente o padrão IEEE 802.11p em comunicações V2X.	87
Figura 35	Latência média das comunicações, utilizando o 3G como link redundante.	89
Figura 36	Média da taxa de perda de pacotes, utilizando o 3G como link redundante.	90
Figura 37	Vazão média utilizando o 3G como link redundante.	92

LISTA DE TABELAS

Tabela 1	Especificações da camada física do padrão IEEE 802.11p...	25
Tabela 2	Equivalência de priorização de mensagens em redes veiculares.	26
Tabela 3	Parâmetros Específicos de Priorização de Mensagens.	26
Tabela 4	Software utilizado na elaboração e execução de simulações em VANETs.	48
Tabela 5	Custo médio estimado para cada modelo de equipamento. .	61
Tabela 6	Especificação resumida do ambiente simulado.	67

LISTA DE SIGLAS

2G	Segunda Geração
3G	Terceira Geração
3GPP	<i>3rd Generation Partnership Project</i>
4G	Quarta Geração
AC	<i>Access Class</i>
ACK	<i>Acknowledgement</i>
AIFS	<i>Arbitration Inter-Frame Space Number</i>
AODV	<i>Ad Hoc On-Demand Distance Vector Routing</i>
ASL	Algoritmo de Seleção do Link
BATMAN	<i>Better Approach To Mobile Ad-hoc Networking</i>
CA	<i>Collision Avoidance</i>
CCH	<i>Control Channel</i>
CSMA	<i>Carrier Sense Multiple Access</i>
CTS	<i>Clear to Send</i>
DCC	Departamento de Ciência da Computação
DCF	<i>Distributed Coordination Function</i>
DSDV	<i>Destination-Sequenced Distance Vector</i>
DSRC	<i>Dedicated Short-Range Communications</i>
EDCA	<i>Enhanced Distributed Channel Access</i>
EDGE	<i>Enhanced Data rates for GSM Evolution</i>
EUA	Estados Unidos da América
FCC	<i>Federal Communications Commission</i>
FDMA	<i>Frequency Division Multiple Access</i>
GCDC	<i>Grand Cooperative Driving Challenge</i>
GSM	<i>Global System for Mobile Communications</i>
GPRS	<i>General Packet Radio Service</i>
HSPA	<i>High Speed Packet Access</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
LTE	<i>Long Term Evolution</i>
MAC	<i>Media Access Control</i>
MOVE	<i>MObility model generator for VEhicular networks</i>
MPR	<i>Multipoint Relaying</i>
NAV	<i>Network Allocation Vector</i>
NS-2	<i>Network Simulator</i>
IMT	<i>International Mobile Telecommunications</i>
ISM	<i>Instrumentation, Scientific and Medical</i>

ITU	<i>International Telecommunication Union</i>
OBE	<i>On Board Equipament</i>
OBU	<i>On Board Unit</i>
OGM	<i>Originator Message</i>
OLSR	<i>Optimized Link State Routing</i>
oTCL	<i>object Tool Command Language</i>
QoS	<i>Quality of Service</i>
RREP	<i>Route Reply</i>
RREQ	<i>Route Request</i>
RSE	<i>Road-Side Equipment</i>
RSU	<i>Road-Side Unit</i>
RSSI	<i>Received Signal Strength Indication</i>
RTS	<i>Request to Send</i>
SCH	<i>Service Channel</i>
SUMO	<i>Simulation of Urban Mobility</i>
TC	<i>Topology Control</i>
TCL	<i>Tool Command Language</i>
TCP	<i>Transmission Control Protocol</i>
TDMA	<i>Time Division Multiple Access</i>
TTL	<i>Time To Live</i>
UDP	<i>User Datagram Protocol</i>
UFLA	Universidade Federal de Lavras
UFMG	Universidade Federal de Minas Gerais
UMTS	<i>Universal Mobile Telecommunications System</i>
V2I	Veículo para Infraestrutura
V2V	Veículo para Veículo
V2X	Veículo para Veículo ou Infraestrutura
VANET	<i>Vehicular Ad Hoc Network</i>
WAVE	<i>Wireless Access in Vehicular Environments</i>

SUMÁRIO

1	Introdução	14
1.1	Definição do Problema	15
1.2	Motivação	17
1.3	Objetivo Geral.....	18
1.4	Objetivos Específicos	18
1.5	Contribuições do Trabalho	19
1.6	Estrutura do Trabalho.....	19
2	Referencial Teórico.....	21
2.1	Comunicações em Redes Veiculares.....	21
2.1.1	Padrão 802.11p	24
2.1.2	Arquitetura Wireless Access in Vehicular Networks – WAVE	26
2.2	Padrões de transmissão de dados de Redes Móveis Celulares	27
2.3	Aplicações em VANETs	28
2.3.1	Tecnologias de Segunda Geração (2G).....	29
2.3.2	Tecnologias de Terceira Geração (3G)	30
2.3.3	Tecnologias de Quarta Geração (4G)	30
2.4	Protocolos de Roteamento	30
2.4.1	<i>Ad hoc On-Demand Distance Vector (AODV)</i>	31
2.4.2	<i>Optimized Link State Routing Protocol (OSLR)</i>	32
2.4.3	<i>Better Approach To Mobile Ad-hoc Networking (BAT-</i> <i>MAN)</i>	34
3	Trabalhos Relacionados.....	39
3.0.4	Comparação de desempenho de protocolos de rote- amento.....	39
3.1	Simulações em Redes Veiculares	39
3.2	Dispositivos e experimentos práticos em VANETs....	40
3.3	Projetos Colaborativos ou de Grandes Empresas	42
4	Metodologia.....	45
4.1	Ambiente das avaliações	45
4.2	Métricas Avaliadas	46
4.3	Simulações	47
4.3.1	Ferramentas Utilizadas	48
4.3.2	Malha Viária.....	50
4.3.3	Mobilidade dos veículos	50
4.3.4	Simulação de Mobilidade dos Veículos.....	50

4.3.5	Simulação da Rede	50
4.4	Experimentos Práticos.....	51
5	Desenvolvimento do Dispositivo OBU/RSU	55
5.1	<i>Driver</i> IEEE 802.11p	55
5.2	Compilação do OpenWRT	56
5.3	Instalação do OpenWRT	57
5.3.1	Inicialização via rede.....	58
5.3.2	Instalação permanente.....	59
5.4	Configuração das VANETs.....	59
5.5	Custo estimado dos equipamentos	60
5.6	Algoritmo de Seleção do Link de comunicação – ASL	62
6	Resultados e Discussão	64
6.1	Simulações	64
6.1.1	Especificação dos cenários das latências	64
6.1.2	Latência medida no último nó	68
6.1.3	Latência medida na infraestrutura localizada no ponto <i>D</i>	69
6.1.4	Latência medida na infraestrutura localizada no ponto <i>E</i>	70
6.1.5	Vazão	72
6.2	Experimentos Práticos.....	73
6.2.1	Vazão máxima	74
6.2.2	Protocolos de Roteamento	77
6.2.3	IEEE 802.11p (Comunicações V2V)	80
6.2.4	IEEE 802.11p (Comunicações V2X)	82
6.2.5	IEEE 802.11p e rede 3G.....	88
7	Conclusões e Trabalhos Futuros	93
	REFERÊNCIAS.....	96
	ANEXOS	102

1 Introdução

Todo ano, cerca de 1,24 milhões de pessoas morrem e cerca de 50 milhões ficam feridas em acidentes de trânsito em todo o mundo (ORGANIZATION, 2013). Muito se tem feito para amenizar estas estatísticas, desenvolvendo dispositivos que aprimoram a segurança, como freios ABS e *Air Bags*. No entanto, praticamente não existem equipamentos capazes de prevenir acidentes baseando-se em informações trocadas entre veículos e outros dispositivos na estrada. Situações de engavetamento ou de colisões poderiam ser evitadas caso os veículos envolvidos possuíssem equipamentos capazes de transmitir informações de eventos ou situações do trânsito naquele determinado momento.

Redes Veiculares é o termo utilizado para se referir aos vários tipos de comunicação de dados *ad hoc*, envolvendo veículos. Essa comunicação pode ser exclusivamente entre veículos (V2V), comunicação exclusivamente de veículos para dispositivos de infraestrutura (V2I) ou comunicações híbridas (V2X). Os nós das redes V2X têm capacidade de se comunicar tanto com veículos quanto com dispositivos de infraestrutura (VEGNI; LITTLE, 2011). Essas redes, também denominadas de *Vehicular Ad Hoc Networks* (VANETs), é um tema bastante amplo e que empolga os pesquisadores, principalmente devido aos seus desafios e escalas de soluções (KARAGIANNIS et al., 2011). O principal objetivo da utilização de tecnologias de comunicação entre veículos é aprimorar a segurança do trânsito, reduzindo o número de fatalidades. Isso é possível por meio da transmissão dos estados e ações de um veículo para outros dispositivos onde a comunicação seja possível.

As VANETs possuem características peculiares, como: mobilidade dos veículos normalmente limitada às pavimentações (ruas, estradas e avenidas), mudanças de trajetória, velocidade dos veículos e curto tempo de contato entre os envolvidos na transmissão. Devido a tais características, estas redes possuem diversos desafios a serem explorados, como: manter confiabilidade da conexão, minimizar atrasos na entrega das informações, evitar perda de pacotes e manter uma largura de banda suficiente para atender às diferentes categorias de aplicações (CHENG; SHAN; ZHUANG, 2011; KARAGIANNIS et al., 2011).

Ao contrário das redes sem fio que utilizam a faixa de frequência *Industrial, Scientific and Medical* (ISM), a faixa de comunicação utilizada em redes veiculares é exclusiva para estas comunicações. Esta faixa é denominada *Dedicated Short-Range Communications* (DSRC). Já para prover regras e padrões para as VANETs, foram propostos os padrões IEEE 802.11p e a Arquitetura *Wireless Access in Vehicular Environments* (WAVE). O padrão IEEE 802.11p define principalmente as regras de controle de acesso físico e ao meio.

1.1 Definição do Problema

As aplicações de segurança de trânsito realizam a comunicação de acidentes e de outros eventos críticos aos motoristas. Realizar a avaliação destas redes é de fundamental importância para entender o comportamento, características e peculiaridades, a fim de otimizar aplicações desta categoria, maximizar o desempenho dessas comunicações, minimizando assim as fatalidades.

Atualmente, existem poucas soluções disponíveis no mercado capazes de suportar o padrão IEEE 802.11p. O custo destes equipamentos é proibitivo, na casa dos milhares de dólares. Se em países desenvolvidos este custo é bastante elevado, no Brasil se torna inviável. Desenvolver um equipamento acessível, capaz de habilitar comunicações de dados em veículos é uma tarefa promissora.

Um problema a ser considerado é que o padrão IEEE 802.11p ainda é pouco difundido, justificado atualmente pela falta de hardwares disponíveis no mercado e seu alto custo (VANDENBERGHE; MOERMAN; DEMEESTER, 2011). Para resolver este problema de eventual falta de conectividade no padrão IEEE 802.11p, deve-se pensar em utilizar uma outra estrutura de comunicação já amplamente disponível, a fim de garantir que quando não houver conectividade via padrão IEEE 802.11p, o nó consiga transferir dados usando o outro enlace redundante.

Este trabalho propõe a criação de um ambiente de simulação e experimentação de redes veiculares envolvendo comunicações híbridas (V2X). Para realizar os experimentos, foi desenvolvido um hardware de comunicação de baixo custo, customizável, capaz de ser instalado em veículos ou em infraestruturas, viabilizando as comunicações veiculares. Além disso, esse dispositivo oferece suporte a um enlace secundário utilizado para redundância, e um algoritmo de escolha do link principal. Esse algoritmo foi desenvolvido, baseado no monitoramento da qualidade do sinal e da conectividade do link.

1.2 Motivação

De acordo com Neves et al. (2011), os experimentos práticos em VANETs são escassos. Portanto, esforços em realizar experimentos práticos são necessários, e validar simulações é uma lacuna que precisa ser melhor explorada pelos pesquisadores desta área. Levando também em consideração que cenários reais de redes veiculares irão envolver arquiteturas de comunicações híbridas (V2X), faz-se necessário analisar o tráfego de dados nestes cenários, a fim de otimizá-lo.

De acordo com a literatura consultada, os trabalhos que abordam experimentos práticos em redes veiculares estão em menor número, se comparados aos trabalhos que abordam simulações. Além dos já citados, outros fatores limitantes na execução de experimentos práticos são o desenvolvimento de *driver* e software para tais equipamentos e a grande complexidade para viabilizar tais experimentos. A versão mais recente do padrão de redes veiculares IEEE 802.11p foi aprovada em junho de 2010 (IEEE STANDARD FOR INFORMATION TECHNOLOGY - IEEE, 2010). Visto que redes veiculares é tópico em constante pesquisa pela academia e indústria, futuras versões do padrão poderão ser aprovadas à medida que as pesquisas avançam.

Conforme citado anteriormente, a análise do tráfego de dados em redes veiculares híbridas é um tema com grande potencial a ser explorado. É de extrema importância analisar, validar e promover melhorias nas comunicações V2X, para que os dados, principalmente os relacionados à segurança de trânsito, alcancem os destinatários a tempo de evitar algum acidente. Tais análises poderão auxiliar e promover, em breve, a implanta-

ção e popularização das VANETs, tornando-as realidade no dia a dia das pessoas.

1.3 Objetivo Geral

O objetivo geral deste trabalho é desenvolver um hardware de comunicação customizável e de baixo custo, capaz de operar no padrão IEEE 802.11p, e avaliar seu desempenho em redes veiculares híbridas (V2X). Serão avaliados os seguintes fatores na comunicação de dados: latência, taxa de perda de pacotes e vazão da rede.

1.4 Objetivos Específicos

Nesta dissertação, objetivou-se especificamente:

- Criar e executar simulações de VANETs no padrão IEEE 802.11p;
- Avaliar o desempenho das simulações executadas;
- Desenvolver um dispositivo de comunicação customizável, de baixo custo, capaz de operar no padrão IEEE 802.11p;
- Avaliar, por meio de experimentos, protocolos de roteamento para redes *ad hoc*;
- Realizar experimentos práticos em cenários compatíveis com os simulados;
- Desenvolver e avaliar o desempenho de um algoritmo de escolha do link de saída (VANET ou 3G), para maximizar a taxa de entrega de dados em tempo real;

- Analisar e comparar os resultados das simulações e experimentos práticos.

1.5 Contribuições do Trabalho

A avaliação e experimentação do padrão IEEE 802.11p, por meio de simulações e experimentos práticos é uma das contribuições deste trabalho. Essa avaliação é importante para identificar os limites e o comportamento das VANETs, compatíveis com os cenários propostos neste trabalho. Outra importante contribuição é o desenvolvimento de um protótipo de comunicação customizável e de baixo custo, capaz de operar no padrão IEEE 802.11p. Este dispositivo proporciona um arcabouço para futuros experimentos práticos em redes veiculares. Outras contribuições são importantes, como o desenvolvimento de um algoritmo que ativa o link de redundância dinamicamente, baseado em características físicas da rede. O algoritmo aprimora a conectividade dos nós pois quando não há conexão no padrão IEEE 802.11p, os nós passam a utilizar o link 3G.

1.6 Estrutura do Trabalho

Este trabalho está organizado da seguinte forma: os conceitos sobre redes veiculares, características, comportamento e fatores que envolvem comunicações entre veículos são apresentados no Capítulo 2. O Capítulo 3 apresenta os trabalhos relacionados mais relevantes. A metodologia de desenvolvimento da pesquisa é apresentada no Capítulo 4. Os processos de desenvolvimento do dispositivo de comunicação e do algoritmo de escolha do link são apresentados no Capítulo 5. No capítulo 6 são apresentados

uma descrição dos testes e os resultados obtidos. Por fim, no Capítulo 7, são colocadas as considerações finais deste trabalho.

2 Referencial Teórico

O conceito de comunicação entre veículos tem fascinado os pesquisadores desde a década de 1980 (HARTENSTEIN; LABERTEAUX, 2008). Nos últimos anos, principalmente a partir da década de 2000, esta temática tem sido pesquisada mais frequentemente. Alguns fatores tornaram possível o desenvolvimento destas pesquisas, como por exemplo: a adoção maciça acompanhada da redução de custo das tecnologias de comunicação sem fio, o empenho dos fabricantes de automóveis em aumentar a segurança dos veículos e a necessidade de prover novos serviços aos motoristas. Um outro fator importante que viabilizou tais pesquisas foi o comprometimento dos governos (principalmente dos Estados Unidos e de países da Europa) em alocar faixas de frequência exclusivas para as comunicações veiculares.

2.1 Comunicações em Redes Veiculares

Cada dispositivo na rede, seja ele veículo ou um dispositivo de infraestrutura, é considerado como sendo um nó na rede. As comunicações entre os nós de redes veiculares podem ser classificadas em três principais categorias, descritas a seguir (SICHITIU; KIHIL, 2008):

- Comunicações entre veículos (V2V): Comunicações entre veículos, também denominadas de comunicações de veículos para veículos – V2V, são comunicações *ad hoc*, envolvendo exclusivamente dois ou mais veículos. Neste tipo de comunicação não há coordenador ou suporte externo para se realizar a comunicação. Cada veículo é equipado com um dispositivo chamado *On Board Unit* (OBU) ou *On Board Equipment* (OBE), responsável por realizar estas comunicações. Neste tipo

de comunicação podem-se envolver transmissões de um único salto ou de múltiplos saltos. Múltiplos saltos são necessários quando o destinatário não está no alcance do emissor, mas está no alcance de um veículo intermediário. As diferenças de tais comunicações são ilustradas na Figura 1 (SICHITIU; KIHL, 2008).

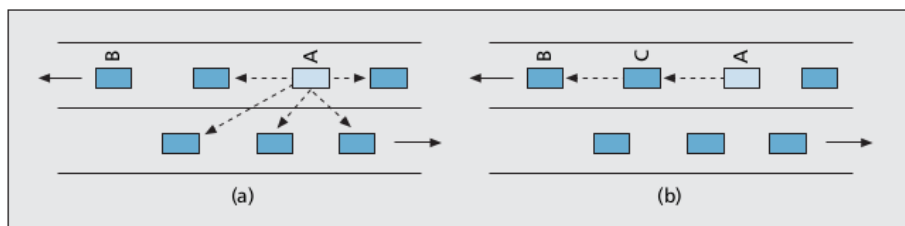


Figura 1 (a) Comunicação em um único salto. (b) Comunicação em múltiplos saltos.

- Comunicação entre veículos e dispositivos de infraestrutura (V2I): Neste tipo, as comunicações são realizadas exclusivamente entre um veículo e um dispositivo de infraestrutura – V2I. Este dispositivo pode ser denominado como *Road-Side Equipment (RSE)* ou *Road-Side Unit (RSU)*. É um dispositivo fixo e normalmente se localiza próximo à pavimentação da estrada. A área de cobertura da rede é limitada à área de cobertura dos dispositivos de infraestrutura. Estes dispositivos centralizam todo o tráfego da rede, atuando como nós intermediários. A vantagem do modo infraestruturado é a possibilidade da comunicação com outras redes, como por exemplo a Internet. A conectividade da rede, entretanto, só é garantida mediante um grande número de dispositivos de infraestrutura, o que pode elevar os custos de implantação.
- Comunicações híbridas (V2X): este tipo de comunicação envolve dois ou mais veículos e dispositivos de infraestrutura. Em redes V2X, uma

infraestrutura mínima é utilizada para estender a conectividade da rede e prover determinados serviços. Neste cenário, é possível que os veículos se comuniquem entre si ou com dispositivos de infraestrutura utilizando múltiplos saltos.

A Figura 2 ilustra os três cenários de comunicações veiculares descritos (ALVES et al., 2009).

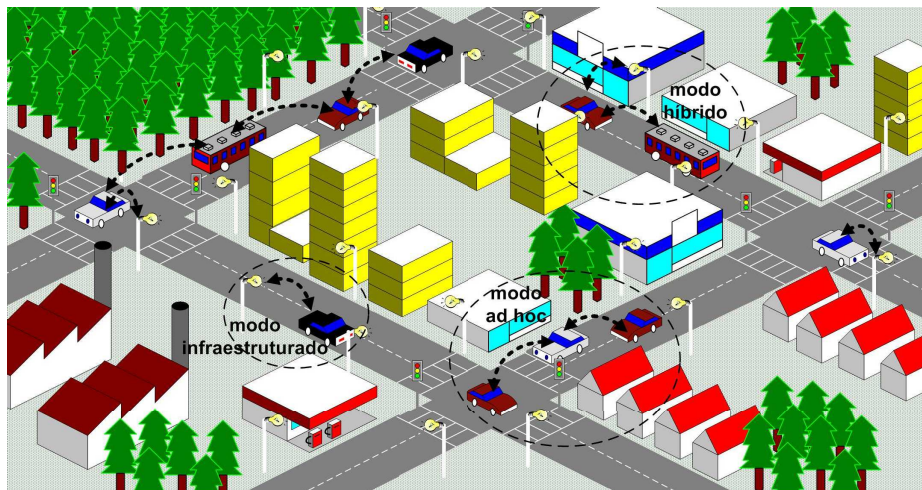


Figura 2 Ilustração de comunicações *ad hoc* entre veículos (V2V), veículos para infraestrutura (V2I) e comunicações híbridas (V2X).

De acordo com Alves et al. (2008), os primeiros esforços de padronização das redes veiculares surgiram em 1999 quando a Federal Communications Commission (FCC), nos Estados Unidos, alocou uma faixa de 75 MHz no espectro de frequência de 5,9 GHz (5,850 GHz a 5,925 GHz), exclusivamente para as comunicações veiculares. Esta faixa de frequência foi denominada de *Dedicated Short Range Communications* (DSRC), uma faixa licenciada porém livre. É restrita em termos das aplicações e tecnologias utilizadas, mas não é cobrada taxa pela sua utilização. De acordo com

European Telecommunications Standards Institute – ETSI (2013), a faixa reservada para as comunicações veiculares na Europa são: de 5,855 GHz a 5,875 GHz (para aplicações gerais), de 5,875 GHz a 5,905 GHz (exclusiva para aplicações de emergência e segurança de trânsito) e de 5,905 GHz a 5,925 GHz (faixa reservada para uso futuro).

Em 2004, o IEEE iniciou a padronização das comunicações em redes veiculares dentro do grupo de trabalho IEEE 802.11. O padrão, que está em constante desenvolvimento e tem sua última versão publicada em 2010, foi denominado de *IEEE 802.11p Wireless Access in Vehicular Environment* (WAVE). O WAVE é uma arquitetura regida pelos documentos elaborados pelos grupos IEEE 1609 (GROUP, 2013) e IEEE 802.11p (IEEE, 2010) e que padroniza as comunicações veiculares. O padrão IEEE 802.11p lida diretamente com a camada física e de enlace das comunicações veiculares. Já a família de padrões IEEE 1609 é composta por quatro documentos que definem um conjunto complementar de serviços padronizados e interfaces que coletivamente viabilizam as comunicações entre veículos.

2.1.1 Padrão 802.11p

Nos Estados Unidos, o padrão IEEE 802.11p opera na faixa entre 5,850 GHz e 5,925 GHz, ao contrário dos padrões IEEE 802.11b/g que usam a faixa não licenciada de 2.4 GHz. Nesta faixa de frequência, os nós conseguem se comunicar a uma distância máxima de 1000 metros, com taxas de transmissão de dados que variam de 1 a 27 Mbps. O IEEE 802.11p consegue garantir transmissão de dados em nós que se movem entre si com uma velocidade de até 200 km/h (ALVES et al., 2009).

A faixa de frequência é dividida em canais de 10 MHz cada. A Tabela 1 apresenta todos os parâmetros do IEEE 802.11p comparado ao padrão Wi-Fi (LI, 2012). O padrão IEEE 802.11p é baseado no padrão IEEE 802.11a, porém as principais diferenças entre eles são a faixa de frequência e a largura dos canais. No padrão IEEE 802.11p definiu-se que um canal será exclusivo para controle das comunicações (CCH) e os outros canais serão utilizados para diferentes categorias de serviços da rede (SCH). O CCH é reservado para transferência de mensagens curtas de alta prioridade ou dados de gerenciamento, enquanto outros tipos de dados são transmitidos nos SCHs. O canal de controle é o canal com prioridade e potência de transmissão se comparado aos canais de serviços.

Tabela 1 Especificações da camada física do padrão IEEE 802.11p.

Parâmetro	WAVE	Wi-Fi
Faixa de Frequência	5,9 GHz	2,4/5 GHz
Largura do Canal	10 MHz	20 MHz
Taxas de Transmissão (Mbps)	3, 4,5, 6, 9, 12, 18, 24 e 27	6, 9, 12, 18, 24, 36, 48 e 54
Modulação	BPSK, QPSK, 16QAM e 64QAM	BPSK, QPSK, 16QAM e 64QAM
Codificação de Canal	Taxa de codificação convolucional: 1/2, 2/3 e 3/4	Taxa de codificação convolucional: 1/2, 2/3 e 3/4

A camada controle de acesso ao meio (MAC) do protocolo IEEE 802.11p é baseado no padrão IEEE 802.11e (VANDENBERGHE; MOERMAN; DEMEESTER, 2011). O protocolo utiliza o método *Enhanced Distributed Channel Access* (EDCA) com extensão de Qualidade de Serviço (QoS). Este esquema é similar ao do padrão IEEE 802.11 CSMA/CA denominado *Distributed Coordination Function* (DCF). O EDCA pode diferenciar 4 tipos de categorias de aplicação: tráfego em segundo plano (*background traffic* – BK), tráfego de melhor esforço (*best effort traffic* – BE), tráfego de voz (VO) e tráfego de vídeo (VI). A Tabela 2 apresenta uma adequação das categorias

de aplicações do EDCA para serem utilizados em redes veiculares (RAWAT et al., 2009). Cada categoria de aplicação ou Classe de Acesso (*Access Class* – AC) possui uma janela de contenção variável e número arbitrário de espaço entre quadros - *Arbitration Inter-Frame Space Number* (AIFS), conforme mostrado na Tabela 3 (MIAO et al., 2011). Estas variáveis são responsáveis por permitir priorização de serviços e consequentemente prover qualidade de serviço na rede.

Tabela 2 Equivalência de priorização de mensagens em redes veiculares.

Prioridade (tráfego do EDCA)	Tipos de Mensagem para VANET
Prioridade 1 (Tráfego de Voz – (Classe de Acesso 3))	Notificação de acidentes, Mensagens de veículos de emergência (polícia, ambulâncias, bombeiros, etc).
Prioridade 2 (Tráfego de Vídeo – (Classe de Acesso 2))	Mensagens de indicação de acidente eminente
Prioridade 3 (Tráfego de Melhor Esforço (<i>best effort</i>) – (Classe de Acesso 1))	Mensagens de condições climáticas, condições das estradas e mensagens de alerta (ex: área escolar a frente, lombada a frente, etc.)
Prioridade 4 (Tráfego de segundo plano (<i>background</i>) – (Classe de Acesso 0))	Outras mensagens em geral

Tabela 3 Parâmetros Específicos de Priorização de Mensagens.

AC	Janela de Contenção mínima (CWmin)	Janela de Contenção máxima (CWmax)	AIFS
3	3	7	2
2	7	15	3
1	15	1023	6
0	15	1023	9

O padrão IEEE 802.11p não possui autenticação e associação nas camadas MAC e física, pois estes métodos do padrão IEEE 802.11 demoram um tempo grande, tornando inviável aplicá-los em redes veiculares (BOOYSEN; ZEADALLY; ROOYEN, 2011).

2.1.2 Arquitetura Wireless Access in Vehicular Networks – WAVE

O IEEE 1609 foi designado para disponibilizar uma fundação para uma variada gama de aplicações em ambientes veiculares incluindo segurança de trânsito, navegação aprimorada, controle de tráfego, entre outras. Cada um dos documentos do padrão IEEE 1609 trata de características específicas das redes veiculares. Estes documentos são:

- IEEE 1609.0 "Draft Standard for Wireless Access in Vehicular Environments (WAVE) – Architecture."
- IEEE 1609.1 "Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) – Resource Manager."
- IEEE 1609.2 "Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) – Security Services for Applications and Management Messages."
- IEEE 1609.3 "Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services."
- IEEE 1609.4 "Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operations."

A Figura 3 mostra visualmente a arquitetura do IEEE 1609 e suas respectivas áreas (GRÄFLING; MAHONEN; RIIHILJÄRVI, 2010). Uma breve descrição de cada um desses documentos pode ser encontrada no Anexo A.

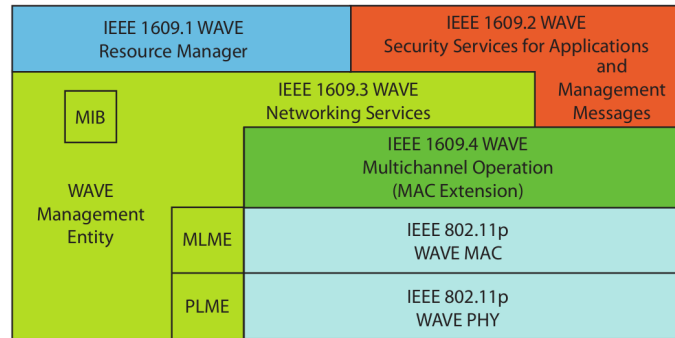


Figura 3 Os padrões IEEE 1609 da arquitetura WAVE e suas relações com o padrão IEEE 802.11p.

2.2 Padrões de transmissão de dados de Redes Móveis Celulares

As primeiras redes celulares surgiram no final da década de 1970, no Japão e início da década de 1980, nos EUA. Utilizavam sinais analógicos, com tecnologia baseada em *Frequency Division Multiple Access* (FDMA) (YAMAUCHI; CHEN; WEI, 2005). A utilização destas redes para tráfego de dados se popularizou a partir da segunda geração da tecnologia, a *Global System for Mobile Communications* (GSM), desenvolvida pela *3rd Generation Partnership Project* (3GPP). Todas as versões de transmissão de dados também são propostas por esta instituição.

2.3 Aplicações em VANETs

De acordo com Hartenstein e Laberteaux (2008), as aplicações que são executadas em redes veiculares podem ser divididas em três categorias gerais:

- Aplicações relacionadas à segurança de trânsito: englobam as aplicações que alertam os outros motoristas sobre um acidente à frente

ou outros eventos cruciais para a segurança do veículo. Mensagens oriundas destas aplicações possuem maior prioridade perante qualquer outra aplicação.

- Aplicações relacionadas à eficiência de transporte: englobam as aplicações que otimizam o deslocamento do veículo de acordo com informações atualizadas do trânsito. Mensagens transmitidas na rede provenientes destas aplicações têm prioridade intermediária.
- Aplicações de informação/entretenimento de modo geral: englobam as aplicações gerais, como acessar a Internet, redes sociais ou ler e-mails. Estas aplicações geram pacotes de dados de prioridade mínima circulando na rede.

Para avaliar as chances de sucesso de uma aplicação, é necessário analisar se ela satisfaz seu propósito, levando em consideração a quantidade e usuários que utilizarão o serviço e qual impacto a aplicação trará para a sociedade. O programador deve considerar atualmente o nível de penetração de redes veiculares no mundo real, que ainda é muito limitada. Adicionalmente, determinadas aplicações só são viáveis se existirem diversos nós (veículos equipados com dispositivos de rede sem fio) em operação na rede.

2.3.1 Tecnologias de Segunda Geração (2G)

As redes de celular de segunda geração utilizam tecnologia de transmissão digital baseada em múltiplos acessos por divisão de tempo – *Time Division Multiple Access* (TDMA) e foram projetadas para trafegar, principalmente, serviços de voz pois utilizam comutação por circuito. A partir

da adoção do *General Packet Radio Service* (GPRS), foi possível utilizar as redes para transmitir dados por meio de dispositivos móveis.

A tecnologia GPRS surgiu com o intuito de otimizar o uso do espectro para a transmissão de dados. Proporciona uma vazão máxima teórica de 50 kbps, sendo que na prática esta taxa pode chegar a 40 kbps. A banda disponível para transmissão de dados é compartilhada com a banda de transmissão de voz, que tem preferência. Quanto maior o número de usuários ativos conectados na estação base, menor é a banda disponível para transmissão de dados. Como um circuito de dados é alternado com o circuito de voz, quanto mais gente usar o serviço de voz, o circuito de dados terá menos tempo disponível.

De acordo com Furuskar et al. (1999), o *International Telecommunication Union* (ITU) elaborou as especificações do *International Mobile Telecommunications* no ano de 2000 (IMT-2000). As redes *Enhanced Data rates for GSM Evolution* (EDGE) são baseadas nestas especificações e proporcionam suporte à comutação por pacotes, que é mais eficiente do que a comutação por circuito. É considerada uma evolução do GPRS e pode ser referida na literatura como redes de 2,5 geração. Esta tecnologia proporciona uma vazão máxima teórica de 384 kbps, sendo que na prática esta taxa pode chegar a 150 kbps.

2.3.2 Tecnologias de Terceira Geração (3G)

O *Universal Mobile Telecommunications System* (UMTS) é a terceira geração de telefonia celular, baseada no padrão GSM e utiliza codificação *Wideband Code Division Multiple Access* (W-CDMA) com comutação totalmente baseada em pacotes, onde os dados (inclusive de voz) são trans-

mitidos em pacotes e remontados no destino. Lançado em 1999, a primeira versão pode proporcionar velocidades de 384 kbps em downloads e 64 kbps em uploads (YAMAUCHI; CHEN; WEI, 2005).

O *High Speed Packet Access* (HSPA) é considerada a tecnologia de 3,5 geração. Foi introduzida em 2002, a partir da quinta versão do padrão UMTS e permite atingir velocidades de até 14,4 Mbps em downloads e 5,76 Mbps em uploads (LI et al., 2008; SHAH, 2008). A partir da sétima versão, lançada em 2007, foi introduzido o HSPA+, que oferece velocidades de 28,8 Mbps em downloads e 11,5 Mbps em uploads (HOLMA et al., 2007).

2.3.3 Tecnologias de Quarta Geração (4G)

O *Long Term Evolution* (LTE) foi proposto no oitavo lançamento realizado pelo 3GPP, em 2008. Nas especificações, esta tecnologia pode proporcionar velocidades de até 100 Mbps em downloads e 50 Mbps em uploads (ELNASHAR; EL-S Aidny, 2013). Ainda é uma tecnologia cara e menos popular, se comparada com as tecnologias anteriormente citadas.

2.4 Protocolos de Roteamento

Nesta seção, será descrito o funcionamento de alguns protocolos de roteamento que podem ser aplicados em VANETs além de suas respectivas análises de desempenho encontrados na literatura. As VANETs, por serem redes *ad hoc*, suportam protocolos de roteamento. Alguns deles são descritos a seguir.

2.4.1 *Ad hoc On-Demand Distance Vector (AODV)*

O AODV é um protocolo reativo baseado no *Destination-Sequenced Distance Vector (DSDV)*. Protocolos reativos realizam a descoberta de nós destinos somente quando for necessário transmitir. Portanto, o AODV minimiza o tráfego de dados através da criação de rotas somente quando for necessário. Os nós da rede mantêm uma tabela de informação de rotas. Essas informações são trocadas entre os mesmos. Quando um nó fonte quer enviar dados para um nó destino, ele primeiro inicia um processo de descobrimento de rota. Neste processo, o nó fonte envia um pacote de requisição de rota, ou *Route Request (RREQ)* aos seus vizinhos via *broadcast*. Os nós que receberam os RREQs também encaminham estes pacotes aos seus vizinhos. O processo continua até que o RREQ alcançar o nó destino ou alcançar um nó que conheça uma rota até o destinatário.

Os nós envolvidos na troca de pacotes RREQ também atualizam suas tabelas com as informações dos vizinhos, por meio de um caminho reverso. Quando o nó que conhece o caminho até o destino ou o nó destino recebe o RREQ, a rota reversa é enviada como resposta ao nó de origem. Esta resposta é o *Route Reply (RREP)*. O pacote RREP é transmitido usando a rota reversa. Quando o nó fonte recebe o RREP, ele passa a conhecer a rota até o nó destino e atualiza esta informação em sua tabela de roteamento. Para manter a tabela de rotas atualizada, cada nó periodicamente envia pacotes HELLO aos nós destinos de suas tabelas de roteamento, com a finalidade de detectar rotas quebradas.

2.4.2 *Optimized Link State Routing Protocol (OSLR)*

O *Optimized Link-State Routing* (OSLR) é um protocolo de roteamento pró-ativo baseado no estado de enlace. Os protocolos pró-ativos realizam a atualização da tabela de roteamento constantemente, independente do envolvimento do nó nas comunicações. Dessa forma, ganha-se em desempenho pois a tabela de roteamento estará sempre atualizada. O ponto fraco é o aumento no *overhead*, pois as informações de roteamento estão constantemente circulando na rede.

De acordo com Almeida (2011) e Couto et al. (2009), para se obter uma cópia da topologia da rede em todos os nós, o protocolo envia periodicamente mensagens de controle, por meio de mensagens HELLO e de controle de topologia (*Topology Control* – TC). Mensagens HELLO são enviadas apenas aos nós vizinhos a um salto, fornecendo informações do estado de enlace desse nó com seus nós vizinhos. As mensagens de TC carregam os estados dos enlaces do OLSR e são enviadas a todos os nós da rede por meio de *flooding* para o endereço de *broadcast*, de modo que todos os nós dentro da área de cobertura do emissor recebam a mensagem por meio de uma única transmissão. Entretanto, como um nó pode receber a mesma mensagem várias vezes de nós diferentes (enviadas pelo nó fonte e por um nó retransmissor da mensagem), o OLSR utiliza um método de controle de inundação para diminuir o número de mensagens redundantes. É neste ponto que o OLSR se destaca. Isto é permitido por meio da utilização de uma técnica denominada múltiplos pontos de retransmissão, ou *Multipoint Relaying* (MPR). Nesta técnica, cada nó seleciona um grupo de nós para propagar as mensagens de controle.

Os MPR, que são criados com as informações obtidas nos pacotes TC, são compostos pelo menor conjunto de vizinhos de um salto capazes de alcançar todos os vizinhos de dois saltos. Apenas os nós do conjunto MPR retransmitem os estados dos enlaces do nó que os escolheu. Os demais nós apenas ouvem as mensagens. A Figura 4 (ALMEIDA, 2011) apresenta o processo de envio de mensagem por difusão de pacotes sem a técnica MPR. Em contrapartida, a Figura 5 (ALMEIDA, 2011) apresenta a difusão com a técnica MPR. Além do uso do MPR, o OLSR pode utilizar os parâmetros *TcRedundancy*, *MprCoverage* e *LinkQualityFishEye* para controlar a carga de tráfego. Esses parâmetros, citados por Couto et al. (2009), são descritos a seguir.

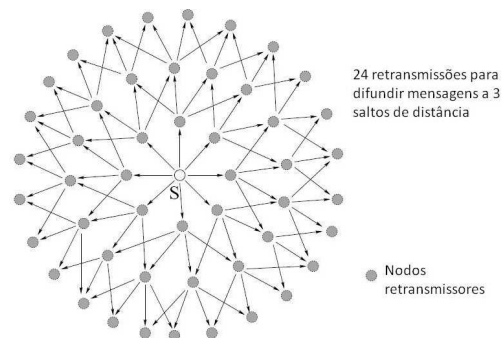


Figura 4 Difusão normal.

A quantidade de informações contida em cada mensagem de controle de topologia é ajustada pelo parâmetro *TcRedundancy*. Esse parâmetro define três possíveis níveis. O nível 0 representa o nível mínimo de informação necessária para que todos os nós possam calcular caminhos entre qualquer par origem-destino da rede. Nele, as mensagens de controle de topologia se limitam a informar apenas os estados dos enlaces entre o nó emissor da mensagem e os nós que o escolheram como MPR (*MPR selector set*). No

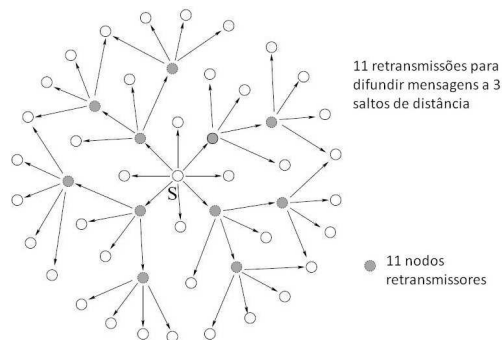


Figura 5 Difusão utilizando MPRs

nível 1, as mensagens contém, além dos estados dos enlaces contidos no nível 0, os estados dos enlaces entre o nó emissor e os seus vizinhos MPR (*MPR set*). No último nível, nível 2, os nós anunciam os estados dos enlaces entre eles e todos os seus vizinhos.

O parâmetro *MprCoverage*, que pode assumir qualquer valor inteiro maior que um, define o número de nós pertencentes ao conjunto MPR que devem ser utilizados para alcançar os vizinhos de dois saltos. Caso o seu valor seja igual a um, a carga de controle é mantida no mínimo. Se o *MprCoverage* for igual a m , sempre que possível, cada nó seleciona o seu conjunto MPR, de modo a garantir que cada vizinho de dois saltos seja alcançado por, pelo menos, m vizinhos do conjunto MPR. Quanto maior o valor do *MprCoverage*, menor será a redução do controle proporcionada pelo conjunto MPR.

Por fim, o parâmetro *LinkQualityFishEye* define se será utilizado ou não o método de controle de *flooding* denominado Fisheye. Este método foi proposto ao verificar que nós mais distantes não se comunicam com a mesma frequência que os mais próximos. Além disso, a precisão das mensagens de controle vão sendo reduzidas de acordo com a distância. Por isto, torna-se

mais eficiente concentrar as mensagens de controle de topologia entre os nós mais próximos do nó origem. Para regular o alcance das mensagens, o Fisheye ajusta o valor do campo *Time-To-Live* (TTL) do protocolo IP.

2.4.3 *Better Approach To Mobile Ad-hoc Networking* (BATMAN)

O OLSR não tem sofrido modificações suficientes para lidar com problemas de grandes redes Mesh sem fio (NEUMANN; AICHELE; LINDNER, 2007). Além disso, o cálculo de rotas com o OLSR em redes com mais de 100 nós é uma tarefa complexa para pequenos processadores. Superar os limites deste protocolo tornou-se um desafio. Em 2006, dois dos desenvolvedores do OLSR decidiram partir para o desenvolvimento de um novo protocolo. Com uma abordagem mais simples, evitando que cada nó tenha rotas completas para todos os outros nós da rede, o BATMAN vem sendo aprimorado desde então. A abordagem proposta pelo algoritmo BATMAN é dividir o conhecimento sobre os melhores caminhos fim-a-fim entre todos os nós participantes da rede. Cada nó mantém apenas a informação sobre seu melhor vizinho de um salto, dentre todos seus vizinhos. Além disso, um mecanismo de *flooding*, baseado em evento, previne a geração de informações contraditórias de topologia, evitando por exemplo *loops* de rotas. O algoritmo é projetado para lidar com redes que são baseadas em links não confiáveis.

De acordo com Neumann, Aichele e Lindner (2007), o protocolo BATMAN funciona da seguinte forma: cada nó transmite mensagens em *broadcast* denominadas *Originator Messages* (OGMs), para informar a vizinhança sobre a sua existência. Estes vizinhos irão retransmitir as OGMs de acordo com regras específicas para informar seus vizinhos sobre a exis-

tência do nó original que iniciou a transmissão. As OGMs são pequenas, tipicamente pacotes de tamanho de 52 bytes, incluindo o *overhead* dos protocolos IP e UDP. OGMs contêm pelo menos o endereço do nó de origem, o endereço do nó transmissor do pacote, um TTL e um número de sequência que guarda o percurso do pacote OGM desde sua origem. O percurso de um pacote OGM é ilustrado na Figura 6. Quando um nó recebe uma mensagem OGM, ele atualiza sua tabela de roteamento com essas informações. O receptor de uma OGM diminui o TTL e encaminha para um de seus vizinhos. Quando um mesmo OGM chega a um nó por caminhos diferentes, eles serão descartados, mantendo somente o que chegou mais rápido. Links bidirecionais são detectados, ouvindo o encaminhamento das OGMs pelos nós aos seus vizinhos.

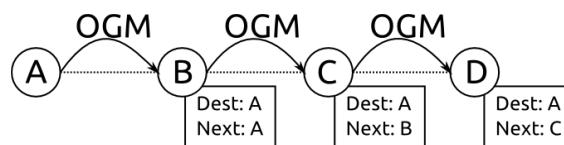


Figura 6 Percurso de um pacote OGM.

As OGMs que seguem um caminho onde a qualidade do link sem fio é saturada ou ruim irão sofrer perda de pacotes e atrasos em seu caminho pela rede. No entanto, as OGMs que são transmitidas em rotas boas irão propagar-se mais rápido e de forma mais confiável. Para informar que uma OGM foi recebida com sucesso uma ou mais vezes, ela contém um número de sequência, dado pelo nó de origem da OGM. Cada nó reenvia para o nó de origem as OGMs recebidas pelo vizinho que foi identificado como o melhor (o vizinho com melhor ranking). Dessa forma, as OGMs são enviadas por *flood* seletivo na rede e informam os nós receptores sobre a existência de outros nós.

Um nó X irá aprender sobre a existência de um nó Y pelo recebimento de suas OGMs, quando as OGMs do nó Y forem reenviadas pelos seus vizinhos próximos. Se o nó X tem mais de um vizinho, ele pode detectá-los ao receber mensagens de origem de seus vizinhos de um salto. O algoritmo elege o melhor vizinho de um salto aquele que enviou mais rapidamente a mensagem e respectivamente configura sua tabela de roteamento.

3 Trabalhos Relacionados

Esta seção apresenta alguns trabalhos relacionados, relevantes para a execução desta dissertação.

3.0.4 Comparação de desempenho de protocolos de roteamento

Em Spaho et al. (2013), o desempenho dos protocolos AODV e OLSR foram analisados em VANETs, em cruzamentos de vias. O OLSR apresentou melhor desempenho na entrega de pacotes, menor latência e melhor vazão. A avaliação foi realizada por meio de simulações no NS-3.

Em Dias (2012), testes em VANETs foram realizados para eleger o melhor protocolo de roteamento. Diversos protocolos foram avaliados, dentre eles o OLSR e o BATMAN. Entre os dois, o OLSR teve o pior desempenho para tais redes, principalmente no que se diz ao *overhead* na rede, pois um nó não precisa atualizar constantemente os estados de todos os outros. No BATMAN, cada nó precisa saber apenas do estado de seus vizinhos.

3.1 Simulações em Redes Veiculares

Diversos esforços vêm sendo realizados para aprimorar e avaliar o protocolo IEEE 802.11p WAVE em simuladores, principalmente no simulador NS-2. Uma modelagem do IEEE 802.11p foi realizada no simulador NS-2 baseada em um rascunho do protocolo (GUKHOOL; CHERKAOUI, 2008). A taxa de pacotes perdidos foi avaliada em comunicações V2I, comparando-se o protocolo 802.11p com o protocolo 802.11a. Resultados promissores

foram obtidos, já que houve menor perda de pacotes nas redes que usaram o protocolo padrão para redes veiculares.

Em outro trabalho, foi analisado o desempenho de comunicações V2V por meio de simulações no NS-2, levando em consideração a velocidade dos veículos (MURRAY; COJOCARI; FU, 2008). Nesta abordagem, foram avaliadas a latência, taxa de perda de pacotes e vazão entre veículos que se comunicavam por meio de uma versão do protocolo IEEE 802.11p implementada no simulador pelos autores.

Simulações no NS-2 que abordam tráfego de mensagens de segurança foram realizadas por Wei et al. (2011). Um aprimoramento na entrega de mensagens foi proposto por meio da técnica de controle de potência de transmissão. O objetivo desta técnica é evitar colisões de dados promovendo a transmissão com potências específicas, de acordo com a distância do destinatário.

Com o intuito de otimizar especificamente a entrega de mensagens de segurança de trânsito, foram testadas técnicas de transmissão destas mensagens (ABABNEH; LABIOD, 2010). As técnicas de *flooding* ou baseadas em trajetória foram analisadas em simulações implementadas no NS-2.

De acordo com Neves et al. (2011), a maioria dos trabalhos envolvendo simulações de redes veiculares não são validados por experimentos práticos. Existe a necessidade de realizar testes práticos para validar os modelos de simulação, a fim de aprimorá-los.

3.2 Dispositivos e experimentos práticos em VANETs

Alguns trabalhos na literatura mostram os esforços da comunidade acadêmica em viabilizar as comunicações veiculares. Testes foram realiza-

dos em dispositivos equipados com transmissores operando no padrão IEEE 802.11b, a fim de avaliar a viabilidade das VANETs (GONZÁLEZ et al., 2008). Pacotes de dados foram transmitidos entre veículos e obteve-se relativo sucesso na transmissão. No entanto, como o padrão utilizado não foi o proposto para redes veiculares, não é possível dizer que os resultados obtidos são compatíveis com o padrão IEEE 802.11p.

Como é difícil encontrar equipamentos capazes de operar nativamente no padrão IEEE 802.11p, adaptações foram realizadas em equipamentos que operam no padrão IEEE 802.11a, para que operem conforme o padrão IEEE 802.11p (VANDENBERGHE; MOERMAN; DEMEESTER, 2011).

Nos trabalhos de Kamal, Lou e Zhao (2012) é apresentado um equipamento de pequena escala capaz de operar nativamente na frequência DSRC, para ser utilizado em VANETs. O equipamento executa uma distribuição Linux sendo altamente configurável. Mensagens de *ping* foram transmitidas de um equipamento para outro, em arquiteturas de comunicação V2I ou V2V. Não foi analisado o comportamento do equipamento em arquiteturas híbridas.

Equipamentos operando na faixa DSRC também foram testados para comunicações V2V por Martelli, Renda e Santi (2011) e Neves et al. (2011). Em cenários onde os nós tinham ou não visada de sinal entre si, foi avaliado o desempenho da comunicação por meio de pacotes UDP de tamanho fixo, transmitidos a uma mesma periodicidade. Nestes experimentos, levou-se em consideração apenas as taxas de sinal e de transmissão. A latência não foi avaliada nestes trabalhos.

Em Teixeira et al. (2013), uma avaliação prática do padrão foi realizada utilizando-se dois notebooks equipados com uma placa IEEE 802.11p nativa. Latência, *jitter*, vazão, taxa de perda de pacotes e tempo de associação dos nós foram avaliados. Os resultados indicaram que o padrão IEEE 802.11p proporcionou adequadamente comunicações entre veículos.

3.3 Projetos Colaborativos ou de Grandes Empresas

Existem diversos projetos de grandes empresas ou outros consórcios que realizam pesquisas ativamente no campo de comunicações veiculares. Os primeiros projetos provenientes de consórcios, como o *Vehicle WAVE Safety Communications Consortium* (VSC) e o *Car-to-Car Communication Consortium* (C2C-CC), focaram no aprimoramento da segurança e na eficiência do deslocamentos dos veículos. Foram pioneiros e promoveram o início da padronização das comunicações entre veículos (HARTENSTEIN; LABERTEAUX, 2008; KARAGIANNIS et al., 2011). Apesar de existirem diversos projetos pioneiros, os próximos parágrafos abordam os mais recentes e relevantes.

O *Grand Cooperative Driving Challenge* (GCDC) foi um evento colaborativo realizado na Holanda, iniciado em 2009 e finalizado em 2011, com a finalidade de organizar equipes para o desenvolvimento de aplicações *Intelligent Transportation Systems* (ITS) (LIDSTRÖM et al., 2011). As aplicações ITS são patrocinadas principalmente por diversos governos e focam na otimização de tráfego e na transmissão de informações que promovem a segurança do trânsito. Dentre as diversas contribuições deixadas pelo GCDC, foram os desenvolvimentos dos protocolos CALM e IEEE 802.11p.

Um conjunto de três projetos alemães apoiados pelo Ministério da Educação e Pesquisa da Alemanha têm diversos objetivos, entre eles: promover segurança; diminuir a carga de trabalho do motorista por meio de assistência e otimização de rotas; otimização da capacidade de rodovias; preocupação com o meio ambiente; ser aceito pela sociedade e por seus usuários. Estes projetos, denominados *Adaptive und Kooperative Technologien für den Intelligenten Verkehr* (Aktiv) – Tecnologias Adaptativas e Cooperativas para o Tráfego Inteligente. Os projetos contam com um conjunto de 29 colaboradores, entre eles grandes empresas automobilísticas, operadoras de telefonia celular, desenvolvedores de software, fabricantes de hardware e de dispositivos de comunicação (VERKEHR, 2013).

Um destes projetos do grupo Aktiv é o Aktiv-AS (*Aktive Sicherheit* – Segurança Ativa). O projeto lida com o desenvolvimento de sistemas de assistência ao motorista, focando em aplicações que promovem segurança de trânsito. O custo estimado do projeto foi de 37,5 milhões de Euros e guiou desenvolvimentos de dispositivos de segurança que detectam acidentes, mudança de faixas, detecção de pedestres e ciclistas e alertas aos usuários.

O Aktiv-VM (*Verkehrsmanagement* – Gerenciamento de Tráfego) desenvolve tecnologias que otimizam a performance das rodovias, evitando congestionamentos e sobrecargas. Com o custo estimado de 18 milhões de Euros, este projeto trouxe avanços nas áreas de otimização de rede, sistema de navegação adaptativa, direção baseada em situações externas e plataforma de informações ao motorista.

O último projeto do grupo Aktiv é o *Cooperative Cars* (CoCar), que focam em comunicações V2V e V2I para promover aplicações colaborativas, usando rede de dados celulares. Para isto, um simulador foi elaborado,

além de uma plataforma de serviços para realizar experimentação prática em comunicações celulares. O custo do projeto foi de 4 milhões de Euros com duração de 2 anos e meio.

4 Metodologia

Baseando-se nos conceitos de Jung (2004), neste trabalho buscou-se realizar uma pesquisa de natureza aplicada, com objetivo de caráter exploratório e utilizando procedimentos experimentais práticos.

As redes veiculares requerem técnicas particulares para avaliar a performance por meio de simulações e experimentações. Essas técnicas se justificam devido ao constante desenvolvimento das pesquisas em VANETs, características peculiares destas redes e de seus protocolos (KARAGIANNIS et al., 2011).

A proposta deste trabalho é avaliar, por meio de simulações e experimentações, o comportamento do padrão IEEE 802.11p em comunicações veiculares. Diante do levantamento de diversos artigos e trabalhos científicos que abordaram redes veiculares, não foi identificado um padrão metodológico geral para avaliação de VANETs. Normalmente, cada autor realiza a metodologia de acordo com os itens que se pretende avaliar e com o cenário testado. Assim, será proposto a seguir o detalhamento das atividades e procedimentos que foram executados durante o projeto.

4.1 Ambiente das avaliações

O campus da Universidade Federal de Lavras (UFLA) foi o ambiente utilizado para a execução das simulações e dos experimentos práticos. Especificamente, utilizaram-se as intermediações do Departamento de Ciência da Computação (DCC) desta universidade, devido à possibilidade de instalar equipamentos de testes neste departamento. As avenidas centrais, por serem mais extensas, foram utilizadas nas simulações. A Avenida Sul foi utilizada nos experimentos práticos. Um dos fatores que influenciaram na

escolha deste ambiente foi o fato que o trânsito nesta região só é intenso em determinados períodos do dia. Assim foi possível ter um melhor controle sobre os experimentos práticos.

Para as simulações e experimentos, foi disposto um nó físico localizado no DCC (RSU), e os outros nós móveis que circularam pelas avenidas do campus. A Figura 7, obtida no Google Mapas, apresenta uma foto de satélite do ambiente real utilizado em simulações e experimentos.



Figura 7 Foto de satélite do ambiente real utilizado nas simulações e experimentos.

A avenida sul possui duas pistas (exceto nos retornos) com extensão total de 850 metros (medidas entre os pontos 3 e 4).

4.2 Métricas Avaliadas

Assim como nos trabalhos de Murray, Cojocari e Fu (2008), foram considerados, nas simulações e experimentos práticos, os seguintes tópicos:

- Latência nas transmissões de pacotes: será medido o instante em que o pacote foi transmitido até o instante em que chegou ao receptor;
- Taxa de perda de pacotes: será analisado o número de pacotes perdidos, baseando-se na diferença entre pacotes transmitidos e recebidos.
- Vazão: será analisada a quantidade de pacotes transmitidos em um intervalo de tempo. Desta forma, será possível saber qual a taxa de transmissão ideal para minimizar a perda de informações.

Estes tópicos foram eleitos para análise já que são cruciais para avaliar o desempenho e comportamento de transmissão de dados em redes veiculares.

4.3 Simulações

As simulações foram realizadas no ambiente descrito na Seção 4.1. De maneira geral, para realizar simulações em VANETs, as seguintes etapas foram executadas, na seguinte ordem: implementar/importar o mapa do ambiente e o modelo de mobilidade dos veículos; simular o deslocamento dos veículos no simulador de mobilidade; utilizar a saída do simulador de mobilidade para implementar a simulação da rede; executar a simulação da rede e analisar os dados.

4.3.1 Ferramentas Utilizadas

Para realizar simulações em redes veiculares, as ferramentas apresentadas na Tabela 4 foram utilizadas:

Dentre todos os simuladores de rede analisados no início das pesquisas, a escolha foi feita levando-se em consideração que o NS-2 era o único

Tabela 4 Software utilizado na elaboração e execução de simulações em VANETs.

	Simulador de Mobilidade	Simulador de Rede	Ferramenta de Integração
Nome	Simulation of Urban Mobility - SUMO	Network Simulator 2 - NS-2	MObility model generator for VEhicular networks - MOVE
Versão	0.12.3	2.35	2.91
Plataforma	Linux	Linux	Linux
Descrição	Pacote de simulação de tráfego rodoviário de código aberto e altamente portátil. É projetado para lidar inclusive com grandes redes de estradas e intenso tráfego de veículos.	NS-2 é um simulador de rede de código aberto, orientado a eventos. Utiliza a linguagem oTCL e C++ para montagem e execução de simulações. Provê suporte substancial para TCP, roteamento e protocolos multicast sobre redes cabeadas e sem fios.	Ferramenta que facilita e agiliza o desenvolvimento de simulações de redes veiculares através da geração dos modelos de mobilidade que serão utilizados pelo simulador SUMO e integrando-os com o simulador de rede NS-2.
Site	http://sumo.sourceforge.net	http://nsnam.isi.edu/nsnam/index.php/Main_Page	http://lens.csie.ncku.edu.tw/Joomla_version/index.php/research-projects/past/18-rapid-vanet

simulador de rede amplamente utilizado, de código aberto, gratuito e que suporta o padrão IEEE 802.11p. O NS-2 oferece suporte ao padrão utilizado em redes veiculares desde a versão 2.34. Neste simulador, é possível definir diversos detalhes da rede a serem simulados, fator crucial para a customização das simulações.

O simulador de mobilidade SUMO foi escolhido porque é de código aberto e capaz de simular deslocamentos reais de veículos. Este simulador de mobilidade também é amplamente utilizado em outros trabalhos que abordam redes veiculares.

Para a correta realização dos trabalhos, o refinamento e finalização do código-fonte das simulações foi realizado, manipulando diretamente os arquivos fonte nas linguagens *object TCL* (oTCL) e C++ do NS-2. As ferramentas descritas foram utilizadas em conjunto para a elaboração das simulações. A Figura 8 representa o fluxo de utilização das ferramentas

neste processo, e a descrição destes procedimentos é realizada nas subseções a seguir.

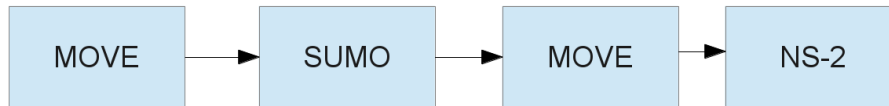


Figura 8 Sequência de utilização das ferramentas para elaboração das simulações de VANETs.

4.3.2 Malha Viária

Para a realização das simulações, a implementação das avenidas do ambiente descrito foi realizada utilizando a ferramenta MOVE. Nesta ferramenta, foi possível realizar a importação e adequação de mapas disponibilizados em plataformas gratuitas na Internet (ex. Google Maps e OpenStreetMap).

4.3.3 Mobilidade dos veículos

Para simular o movimento dos veículos nos mapas, foram utilizados os geradores de movimento de veículos da ferramenta MOVE. Os veículos seguiram trajetórias definidas pelas avenidas dos cenários, com velocidade compatível com o ambiente.

4.3.4 Simulação de Mobilidade dos Veículos

Após a configuração dos deslocamentos realizados pelos veículos, a simulação de mobilidade foi realizada utilizando o simulador de tráfego de veículos SUMO. A saída deste simulador foi utilizada novamente pela ferra-

menta MOVE como entrada para a criação da simulação de redes veiculares no simulador de rede NS-2.

4.3.5 Simulação da Rede

No simulador de rede NS-2, o deslocamento dos nós da rede será representado pela saída da simulação de mobilidade gerada pelo simulador SUMO. A partir de então, as simulações de rede foram implementadas definindo os eventos que irão ocorrer na rede, em momentos pré-definidos. Dados foram transmitidos entre os veículos e o dispositivo de infraestrutura de acordo com os cenários definidos.

Após a implementação dos arquivos de simulações de rede, as simulações foram executadas no simulador de rede NS-2 e os resultados gerados foram analisados por ferramentas do próprio simulador de rede.

4.4 Experimentos Práticos

Os experimentos práticos foram realizados a fim de validar as simulações. Para isto, cenários compatíveis com os simulados foram replicados nos experimentos. Para realizar experimentos práticos em VANETs foram desenvolvidos equipamentos capazes de se comunicar no padrão IEEE 802.11p, na frequência de 5,9 GHz. Este processo de elaboração do hardware de comunicação veicular visou atender a alguns requisitos: custo acessível, capacidade de customização, capacidade de operar tanto como OBU quanto RSU, robustez para operação em cenários extremos, tamanho compatível para instalação em veículos e execução de um sistema operacional e programas de código aberto.

Para atender a estes requisitos, foi adotada uma placa RouterBoard. RouterBoard é o nome dado a uma série de equipamentos de rádio ou roteadores da fabricante letonesa MikroTik (MIKROTIK, 2014). São projetadas primariamente para provedores de Internet oferecendo acesso banda larga via rede sem fios, suportando alta capacidade de tráfego. No total, foram utilizadas quatro unidades do modelo RB433AH e uma unidade do modelo RB411U. A justificativa para a escolha destes modelos e suas respectivas quantidades foi a disponibilidade dos equipamentos. A maioria deles foram cedidos gentilmente pelo Diretoria de Gestão de Tecnologia da Informação da UFLA (DGTI/UFLA).

O modelo RB433AH (Figura 9) possui três portas Ethernet, três *slots* para cartões miniPCI, um *slot* microSD para cartões de memória e uma interface serial RS232. O modelo RB411U (Figura 10) possui entrada *slot* para um *simcard* (chip de celular GSM), um *slot* miniPCI-e para modem 3G, um *slot* para cartão miniPCI, uma porta USB, uma porta Ethernet e uma porta serial RS232.

Uma das RouterBoards do modelo 433AH foi configurada para atuar como RSU e foi instalada em um ponto fixo no DCC. Os equipamentos restantes foram instalados em veículos (OBUs). Dos que atuaram como OBUs, um possui conectividade de dados celulares 3G, para ser utilizado como um link redundante de Internet. Nas RouterBoards restantes, foram instaladas dois cartões miniPCI: um para prover uma rede local, interna ao veículo, no padrão IEEE 802.11g e outro para comunicar com os veículos e dispositivos de infraestrutura no padrão IEEE 802.11p. A arquitetura geral do hardware proposto é apresentada na Figura 11.

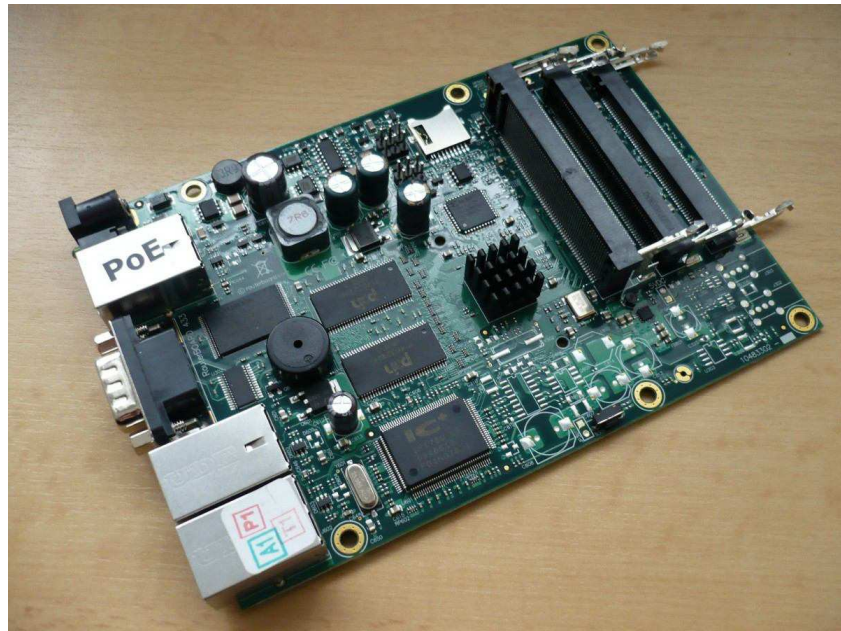


Figura 9 Routerboard modelo RB433AH.

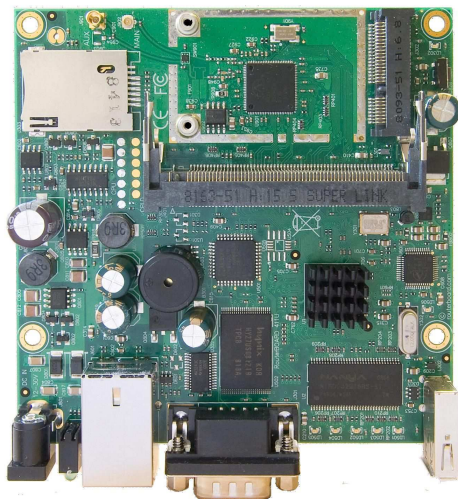


Figura 10 Routerboard modelo RB411U.

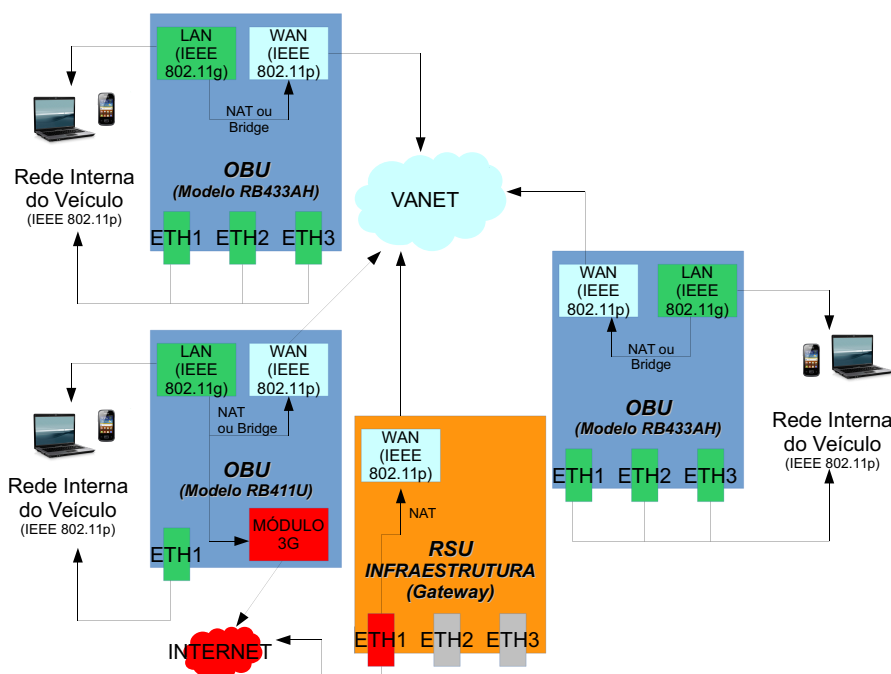


Figura 11 Arquitetura geral dos dispositivos.

Para operar na faixa de frequência de 5,9GHz com canais de 10 MHz, uma versão do *driver* de código aberto Ath5k (que atua em dispositivos com chipset Atheros AR5xxx) foi adaptado para que o cartão pudesse operar no padrão IEEE 802.11p.

Por padrão, a RouterBoard roda o sistema operacional proprietário da Mikrotik, o RouterOS. No entanto, este sistema operacional foi substituído por uma distribuição Linux voltada para roteadores, o OpenWRT (OPENWRT, 2013).

Conforme descrito na Seção 3.0.4, o protocolo de roteamento padrão utilizado nos dispositivos de comunicação foi o BATMAN. Segundo Dias (2012), o BATMAN proporciona menor latência e menor perda de pacotes,

quando comparado ao OLSR. O problema encontrado no funcionamento do OLSR é a latência elevada para detectar entradas e saídas de nós da rede, o que não ocorre com o BATMAN, já que ele é um protocolo distribuído.

5 Desenvolvimento do Dispositivo OBU/RSU

Após a montagem do hardware especificado na Seção 4.4, o sistema operacional e os *drivers* precisaram ser compilados para a arquitetura do dispositivo antes de serem instalados. Como ambos os modelos de Router-Boards possuem processadores de mesma arquitetura, uma única compilação do sistema foi necessária. O processo de adaptação e compilação dos *drivers* e sistema são descritos nas seções a seguir.

5.1 *Driver* IEEE 802.11p

Como os cartões miniPCI utilizados operam de fábrica nos padrões IEEE 802.11a/b/g, foi necessário utilizar um *driver* modificado para que pudessem operar na frequência DSRC. Isto foi possível pois as especificações dos cartões utilizados indicam possibilidade de operações em frequências de até 6,1GHz. Uma versão modificada do *driver* Ath5k foi utilizada, pois os cartões são equipados com o *chipset* Atheros AR5414. A Figura 12 mostra o modelo de cartão utilizado nos experimentos.



Figura 12 Cartão miniPCI IEEE 802.11a/b/g da Mikrotik, modelo R52.

Utilizou-se o código-fonte do *driver* disponibilizado pelo evento GCDC para dispositivos Atheros. Porém, diversas modificações e correções no

código-fonte tiveram que ser realizadas para que esse pudesse ser compilado e executado corretamente no OpenWRT, em arquitetura MIPS.

A adaptação do *driver* de dispositivo permitiu que o cartão operasse na faixa DSRC em canais de 10 MHz, sem a transmissão de *beacons* periódicos. A remoção destes *beacons* é crucial para aprimorar o desempenho da rede, tendo em vista a dinamicidade da rede e o curto período de contato entre os nós. As modificações foram realizadas nos seguintes módulos do *driver*: *ath5k*, *ath*, *mac80211*, *iw* e *config80211*.

No padrão IEEE 802.11a, o *driver* permite que o cartão opere até a frequência máxima de 5,835 GHz nos EUA, devido à regulamentação de domínio imposta pelo FCC. Para desbloquear esta limitação, o domínio regulatório do *driver* foi ajustado para que o cartão operasse de acordo com as especificações do hardware, e não baseado nas especificações de países. Para se sobrepor a esta limitação, o *driver* só pode ser executado em dispositivos com *kernel* versão 2.6.32 ou inferior, pois a partir desta versão, os *kernels* possuem um sistema de trava de domínio que não pode ser transpassada. A versão do OpenWRT Backfire 10.03 foi escolhida para ser utilizada nas RouterBoards, por ser compatível com o hardware e com o *driver* IEEE 802.11p. Esta versão utiliza *kernel* com versão 2.6.32.

5.2 Compilação do OpenWRT

Um computador foi utilizado como apoio para a compilação do sistema OpenWRT. Os códigos-fonte da versão 10.03 Backfire do sistema foram obtidos dos repositórios oficiais. Os *patches* fornecidos pelo GCDC foram incluídos à imagem principal, ajustados antes de serem compilados. A seleção dos pacotes foi realizada por meio do comando *make menuconfig*

(Figura 13) para que, tanto o sistema e o *kernel* pudessem suportar funcionalidades como IPv6, protocolos de roteamento (OLSR e BATMAN), GPS e sistemas de arquivos *ext* e *fat*. Para o modelo RB411U, por conter uma porta USB, foi habilitado adicionalmente o suporte à USB, modems 3G, Bluetooth, dispositivos de armazenamento removíveis, suporte a áudio e a câmeras. O suporte a essas diversas funcionalidades foi adicionado aos dispositivos a fim de proporcionar funcionalidades adicionais a serem utilizadas em experimentos futuros.

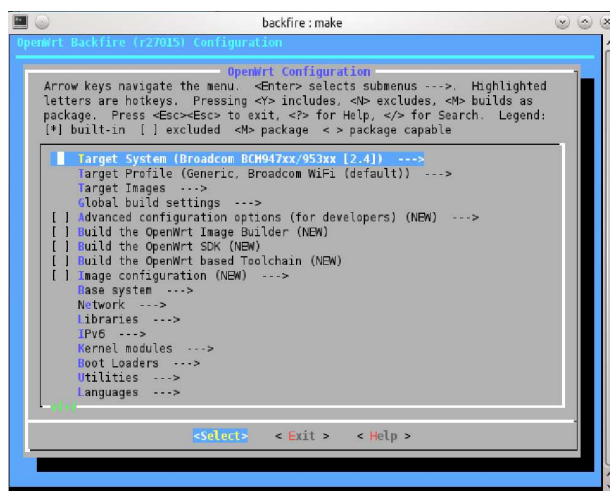


Figura 13 Interface de geração do arquivo de configuração do sistema a ser compilado.

Além de selecionar os pacotes, foi necessário escolher o tipo de arquitetura (*ar71xx*) e quais os tipos das imagens a serem geradas. Dois tipos de imagens foram geradas, *ramdisk* (para a inicialização da RouterBoard via rede) e *tgz* (para instalação na memória *flash* do equipamento). A imagem final de instalação possui em média 20 MB.

5.3 Instalação do OpenWRT

O computador utilizado na compilação também serviu como um servidor para a instalação do OpenWRT. As interfaces serial e de Ethernet da RouterBoard foram conectadas ao servidor. A interface de comandos era disponibilizada por meio de um terminal conectado remotamente via interface serial. Arquivos de inicialização e de instalação foram transferidos via interface Ethernet. De modo resumido, para que fosse possível substituir o sistema RouterOS pelo OpenWRT nas Routerboards, foram necessárias três etapas:

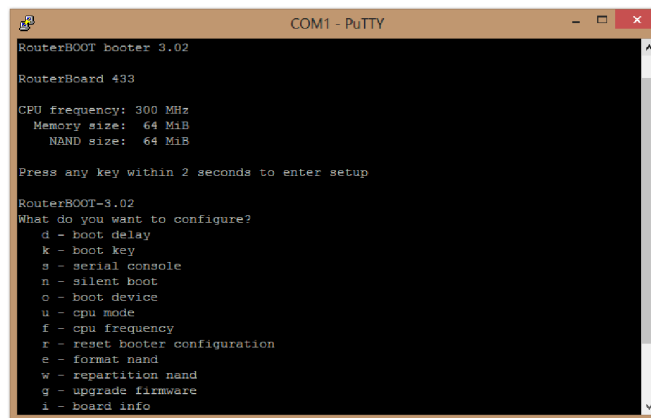
- Inicializar a RouterBoard via rede, com uma imagem do OpenWRT pré-compilada para este fim e disponibilizada por um servidor. Este servidor deverá estar executando os serviços de DHCP e TFTP.
- A partir da imagem inicializada, realizar a instalação do OpenWRT na memória *flash* interna do dispositivo por meio da ferramenta *wget2nand*. Serviços de HTTP ou FTP são necessários para transferência da imagem entre o servidor e a RouterBoard.
- Reinicializar a máquina a partir da memória flash interna e realizar as configurações necessárias no OpenWRT instalado.

5.3.1 Inicialização via rede

Para que a RouterBoard possa carregar o sistema OpenWRT via rede, o servidor precisa possuir os serviços de DHCP e TFTP. O pacote *dnsmasq* fornece ambos os serviços e foi instalado no servidor. O *dnsmasq* foi configurado para fornecer um IP fixo (vinculado ao endereço MAC da

RouterBoard). O protocolo TFTP foi habilitado, permitindo o carregamento do sistema via rede.

Durante os primeiros segundos de inicialização da RouterBoard (antes da inicialização do sistema), é possível realizar configurações de inicialização. Por meio desta ferramenta (RouterBOOT), configurou-se a RouterBoard para inicializar via rede, no protocolo *bootp*. A Figura 14 ilustra esta ferramenta.



```
COM1 - PuTTY
RouterBOOT booter 3.02
RouterBoard 433
CPU frequency: 300 MHz
Memory size: 64 MaB
NAND size: 64 MaB
Press any key within 2 seconds to enter setup
RouterBOOT-3.02
What do you want to configure?
d - boot delay
k - boot key
s - serial console
n - silent boot
o - boot device
u - cpu mode
f - cpu frequency
r - reset booter configuration
e - format nand
w - repartition nand
g - upgrade firmware
i - board info
```

Figura 14 Ferramenta RouterBOOT que configura a inicialização das RouterBoards.

5.3.2 Instalação permanente

O servidor web *apache* foi instalado no servidor para disponibilizar os arquivos de instalação via HTTP. Antes da instalação permanente do OpenWRT nas RouterBoards, a licença do sistema RouterOS original foi exportada, caso seja necessário restaurá-lo posteriormente. Para isto, a ferramenta WinBOX da Mikrotik foi utilizada. Em seguida, a memória *flash* foi formatada usando a ferramenta RouterBOOT.

Após a inicialização via rede, o endereço da interface de rede foi configurado para a mesma faixa de IP do servidor. Em seguida, o comando *wget2nand* foi utilizado para gravar a imagem compilada diretamente na memória flash da RouterBoard, por meio do seguinte comando:

```
wget2nand http://192.168.0.1/ar71xx
```

Após a instalação, a RouterBoard deve ser novamente configurada via RouterBOOT para inicializar via memória interna.

5.4 Configuração das VANETs

Um *script* de inicialização foi adicionado a todas as OBU/RSUs. Este *script* se conecta a uma rede *ad hoc* pré-configurada, define o endereço de IP e ativa o protocolo de roteamento.

Utilizou-se o sistema RouterOS para escanear redes *ad hoc* e checar se os dispositivos estavam operando na frequência de 5,890 GHz, em uma faixa de canal de 10 MHz. Esta é a frequência utilizada para transmissão de dados críticos e de controle em VANETs. Este escaneamento validou a presença da VANET criada na frequência selecionada, como mostra a Figura 15.

Os dispositivos e a distribuição utilizada oferecem suporte ao IPv6 e sua utilização foi cogitada, principalmente no dispositivo equipado com modem 3G. O IPv6 proporciona a utilização de um único IP em diferentes redes. Porém, infelizmente nenhuma operadora nacional de celular móvel disponibilizava suporte a este padrão. Por esta razão, utilizou-se IPv4 nos nós e cada um recebeu um endereço IP fixo, a fim de obter um melhor controle do tráfego da rede.

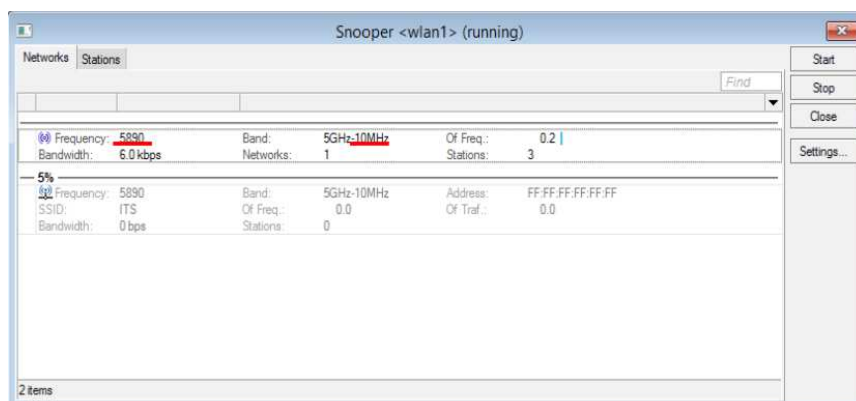


Figura 15 Validação da VANET por meio do RouterOS.

5.5 Custo estimado dos equipamentos

O hardware proposto é composto no mínimo por uma RouterBoard, um módulo de GPS e duas placas de rede sem fio (para modelos que atuam como OBU): uma placa para operar no padrão IEEE 802.11p e outra para fornecer rede interna ao veículo, no padrão IEEE 802.11g. A Tabela 5 mostra um levantamento realizado em Janeiro/2014, referente ao custos (sem impostos), para cada modelo de dispositivo.

Tabela 5 Custo médio estimado para cada modelo de equipamento.

Modelo	Custo Médio Estimado (sem impostos)	DISPOSITIVO DE COMUNICAÇÃO	
		Modelo sem 3G	Modelo com 3G
Routerboard RB433AH	US\$ 149,00	1 unidade	-
Routerboard RB411U	US\$ 79,00	-	1 unidade
Modem 3G Huawei EM770	US\$ 40,00	-	1 unidade
Módulo de GPS Serial	US\$ 20,00	1 unidade	1 unidade
Cartão Mini PCI R52	US\$ 59,00	2 unidades	1 unidade
Placa IEEE 802.11g USB	US\$ 20,00	-	1 unidade
CUSTO TOTAL ESTIMADO:		US\$ 287,00	US\$ 218,00

A RouterBoard que atua como RSU tem o custo inferior, visto que só é necessário um único cartão que opera no padrão IEEE 802.11p. Soluções disponíveis no mercado podem atingir valores de até U\$ 3.000,00, como é o caso do modelo OBE-101¹ da fabricante Unex (cotação realizada em Julho/2013).

O custo superior do modelo sem 3G se justifica pela superioridade do hardware da RouterBoard, que tem mais memória, processador mais robusto e maior quantidade de interfaces de rede.

5.6 Algoritmo de Seleção do Link de comunicação – ASL

Com a finalidade de manter sempre a conectividade da OBU, um algoritmo de seleção de link (ASL) foi desenvolvido e utilizado no modelo RB411U, equipado com modem 3G. O link 3G só é ativado quando não há conectividade da VANET no padrão IEEE 802.11p.

O estado do link da VANET é monitorado por meio do indicativo de força do sinal recebido (*Received Signal Strength Indication* – RSSI). Este valor é obtido diretamente da camada física por meio do comando *iw* executado diretamente na OBU.

Em redes ad hoc, o comando *iw* pode retornar informações de todos os nós vizinhos em seu raio de alcance. O objetivo do ASL é identificar se a VANET proporciona conectividade ao dispositivo de infraestrutura fixo e se o nó possui um nó vizinho com RSSI maior que -85 dBm. O valor de -85 dBm foi obtido considerando os trabalhos de Monks, Bharghavan e Hwu 2001 associados a testes iniciais de campo, realizados nos dispositivos desenvolvidos. Foi identificado que, se o melhor vizinho apresentar valores

¹<http://unex.com.tw/product/obe-101>

de RSSI inferiores a -85 dBm, muito provavelmente este link irá se romper em breve. Valores menores que este índice tornam a transmissão de dados intermitente. O pseudocódigo do ASL é mostrado no Algoritmo 1.

Foi necessário limitar o tempo de escaneamento de RSSI dos vizinhos em 100 milissegundos para que o processo não demore muito tempo, nos casos em que houver muitos veículos ao redor. Nos testes realizados com 4 nós vizinhos, o processo de escaneamento não demorou mais do que 4 ms. A funcionalidade do algoritmo foi avaliada e os resultados obtidos são apresentados na Seção 6.

```

1 Procedimento ASL();
2 início;
3 se Interface 3G está desativada então
4   | Ativa o 3G;
5 se Interface VANET está desativada então
6   | Ativa a VANET;
7 LinkPrincipal ← VANET;
8 ErrosAcumuladosVANET ← 0;
9 ErrosAcumulados3G ← 0;
10 while verdadeiro do
11   | Pesquise o RSSI dos vizinhos por no máximo 100 ms;
12   | se RSSI de algum vizinho > -85 e ping IP infra via VANET
13   | então
14   |   | se LinkPrincipal == 3G então
15   |   |   | LinkPrincipal ← VANET;
16   |   |   | ErrosAcumuladosVANET ← 0;
17   |   | senão
18   |   |   | ErrosAcumuladosVANET ++;
19   |   |   | se ErrosAcumuladosVANET > 2 e Conectividade3G ==
20   |   |   | verdadeiro então
21   |   |   |   | LinkPrincipal ← 3G;
22   |   | se ping IP da infra via 3G então
23   |   |   | se Conectividade3G == falso então
24   |   |   |   | Conectividade3G ← verdadeiro;
25   |   |   |   | ErrosAcumulados3G ← 0;
26   |   | senão
27   |   |   | ErrosAcumulados3G ++;
28   |   |   | se ErrosAcumulados3G > 2 e Conectividade3G ==
29   |   |   | verdadeiro então
30   |   |   |   | Conectividade3G ← falso;
31   | fim;

```

Algoritmo 1: Mecanismo de seleção do link de comunicação.

6 Resultados e Discussão

Os resultados apresentados nesta seção estão divididos em 2 partes: uma relacionada às simulações realizadas e outra referente aos experimentos práticos. Para ambos estudos, foram avaliados a latência, taxa de perda de pacotes e vazão de dados nas intermediações do DCC/UFLA, descrito na Seção 4.1.

6.1 Simulações

Diversas simulações foram realizadas no simulador NS-2 por meio de ferramentas de apoio, conforme descrito na seção 4.3.1. As simulações foram realizadas para avaliar o comportamento do padrão IEEE 802.11p em redes veiculares. O cenário híbrido foi adotado pois é mais próximo ao real, tendo em vista que implementações de VANET não constarão de comunicações exclusivamente V2I (devido ao alto custo de implementar infraestruturas em curtas distâncias para viabilizar as comunicações), nem de comunicações exclusivamente V2V (visto que são restritivas por não proporcionarem troca de dados com redes externas). Para viabilizar as comunicações veiculares, a camada física foi configurada no NS-2, de acordo com as especificações do padrão IEEE 802.11p. O raio de alcance de cada nó foi limitado a 300 metros.

6.1.1 Especificação dos cenários das latências

Diversos nós foram espalhados na Avenida Central da UFLA, cenário utilizado para a avaliação das latências. As localizações do dispositivo de infraestrutura e os pontos de partida dos nós foram instalados conforme

ambiente ilustrado na Figura 16. Os nós se deslocaram com probabilidade de 50% de entrar em um dos retornos da malha viária.

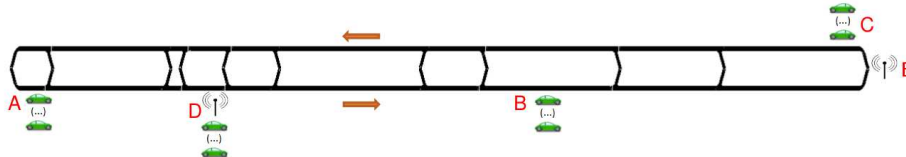


Figura 16 Cenário utilizado nas simulações de avaliação das latências.

Os pontos *A*, *B*, *C* e *D* são pontos de partida dos nós. Uma única infraestrutura fixa (RSU) foi utilizada, ora posicionada no ponto *D*, ora no ponto *E*. Desta forma, foi possível avaliar o impacto de uma infraestrutura posicionada em posição mais central ou em um dos extremos da via. Quanto ao tamanho dos pacotes, foram avaliados os tamanhos de 100 bytes (tamanho mínimo para comunicados de eventos de emergência (SUWANNASA; PUANGPRONPITAG; PHONGSIRI, 2013)) e 1024 bytes (tamanho médio utilizado por aplicações gerais). Duas quantidades de nós foram avaliadas: 51 e 151 nós. As diferentes quantidades de nós está relacionada respectivamente a densidades média e alta de veículos. Um nó era sempre fixo (RSU) e os restantes (OBUs) podiam se mover a uma velocidade máxima de 40 km/h.

O dispositivo de infraestrutura difere dos nós móveis pelo fato de ser fixo e eventualmente proporcionar aos veículos uma comunicação com outras redes. Além disso, esses dispositivos poderão se conectar a centrais de monitoramento de tráfego de veículos.

Em todos os cenários simulados, os nós enviam periodicamente pequenas mensagens em *broadcast* aos seus vizinhos imediatos, informando suas localizações e *status*. Essas mensagens simulam o ambiente real, onde

o nó comunica sua existência a seus vizinhos imediatos. A fim de evitar colisões, cada nó realiza a transmissão dessas mensagens após um período de tempo aleatório de até 100 ms. É importante frisar que, nos resultados das simulações apresentados a seguir, essas mensagens de *status* não foram contabilizadas.

Para todos os cenários, o tempo total de duração das simulações foi de 60 segundos. A fim de medir a latência, dez pacotes foram disparados em *broadcast*, onde mediu-se o momento em que a informação chega ao dispositivo fixo e o momento em que a informação alcança o maior número possível de nós da rede. O primeiro evento foi disparado no instante 3 e os restantes a cada seis segundos. Na Tabela 6, apresenta-se um resumo das especificações das simulações realizadas em quatro cenários base utilizados.

Tabela 6 Especificação resumida do ambiente simulado.

DADOS GERAIS DA SIMULAÇÃO				
	Cenário 1	Cenário 2	Cenário 3	Cenário 4
Duração total	60 segundos	60 segundos	60 segundos	60 segundos
Número total de nós	51 (1 fixo e 50 móveis)	51 (1 fixo e 50 móveis)	151 (1 fixo e 150 móveis)	151 (1 fixo e 150 móveis)
Número de repetições realizadas	5 (variando a trajetória dos nós)	5 (variando a trajetória dos nós)	5 (variando a trajetória dos nós)	5 (variando a trajetória dos nós)
Velocidade máxima dos nós móveis	40 km/h	40 km/h	40 km/h	40 km/h
MENSAGENS DE EVENTOS DE EMERGÊNCIA				
	Cenário 1	Cenário 2	Cenário 3	Cenário 4
Quantidade	10 eventos	10 eventos	10 eventos	10 eventos
Instante (em segundos) de disparo de cada evento	3, 9, 15, 21, 27, 33, 39, 45, 51 e 57	3, 9, 15, 21, 27, 33, 39, 45, 51 e 57	3, 9, 15, 21, 27, 33, 39, 45, 51 e 57	3, 9, 15, 21, 27, 33, 39, 45, 51 e 57
Tamanho	100 bytes	1024 bytes	100 bytes	1024 bytes
Tipo de transmissão	<i>Broadcast (flooding)</i>	<i>Broadcast (flooding)</i>	<i>Broadcast (flooding)</i>	<i>Broadcast (flooding)</i>
MENSAGENS DE STATUS				
	Cenário 1	Cenário 2	Cenário 3	Cenário 4
Periodicidade de envio	A cada 100 ms	A cada 100 ms	A cada 100 ms	A cada 100 ms
Tamanho	100 bytes	100 bytes	100 bytes	100 bytes
Tipo de transmissão	<i>Broadcast (1 hop)</i>	<i>Broadcast (1 hop)</i>	<i>Broadcast (1 hop)</i>	<i>Broadcast (1 hop)</i>

Para cada cenário base, variou-se a posição do dispositivo fixo (pontos *D* e *E*), conforme dito anteriormente. Desta forma, um total de oito cenários foram avaliados. Foram medidos a latência, perda de pacotes e vazão de dados através da realização de quinze repetições para cada um dos oito cenários.

6.1.2 Latência medida no último nó

Pelas Figuras 17 e 18, mostra-se o tempo máximo necessário para que a comunicação de um determinado evento chegue ao maior número possível de nós da rede. Na Figura 17, mostra-se, especificamente, os resultados das simulações realizadas com 51 nós e a Figura 18 apresenta os resultados das simulações realizadas com 151 nós. Em cada figura são apresentados os resultados de simulações variando o tamanho dos pacotes (100 e 1024 bytes).

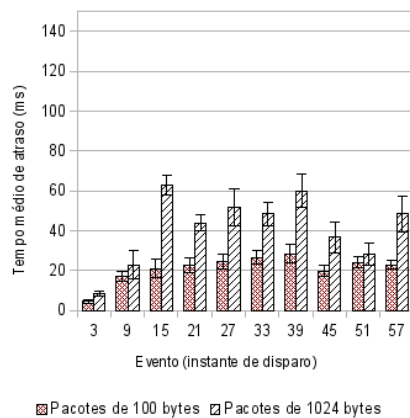


Figura 17 Latência média no último nó a receber a informação (51 nós).

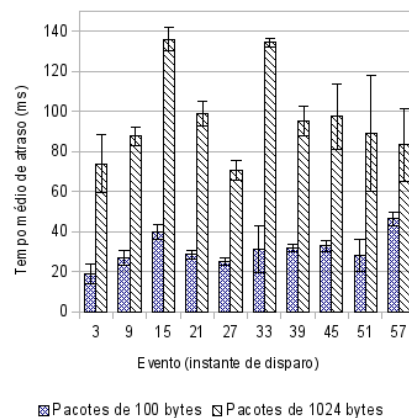


Figura 18 Latência média no último nó a receber a informação (151 nós).

Era esperado que os valores de latência obtidos no cenário com pacotes de 100 bytes fossem inferiores aos obtidos nos cenários com pacotes de 1024 bytes. Independente da quantidade de nós, as latências para os cenários que utilizaram pacotes de 100 bytes permaneceram abaixo de 100 ms. No cenário com 151 nós e mensagens de 1024 bytes, em uma determinada repetição foram detectadas latências de até 158 ms medido o último nó que recebeu o comunicado do evento. A média para os eventos 15 e 33 foi de aproximadamente 140 ms (Figura 18).

O aumento do número de nós causou um incremento no tempo de entrega das mensagens. O impacto causado pela variação do tamanho das mensagens foi maior do que o impacto causado pelo aumento do número de nós da rede. Contudo, uma rede com muitos nós e que transmite mensagens de tamanho maior pode ter latências superiores a 100 ms como consequência. Portanto, detectou-se que quanto maior o tamanho da mensagem e o número de nós, maior será o tempo necessário para que as mensagens se espalhem para todos os nós da rede.

6.1.3 Latência medida na infraestrutura localizada no ponto *D*

Nas Figuras 19 e 20, consta o tempo máximo necessário para que a comunicação de um determinado evento chegue ao dispositivo de infraestrutura localizado no ponto *D*. A Figura 19 mostra especificamente os resultados das simulações realizadas com 51 nós e a Figura 20 apresenta os resultados das simulações realizadas com 151 nós. Nessas figuras estão os dados das simulações variando o tamanho da mensagem (100 e 1024 bytes).

Quando o dispositivo de infraestrutura foi fixado no ponto *D*, os comunicados dos eventos chegaram ao dispositivo em um tempo inferior a 100

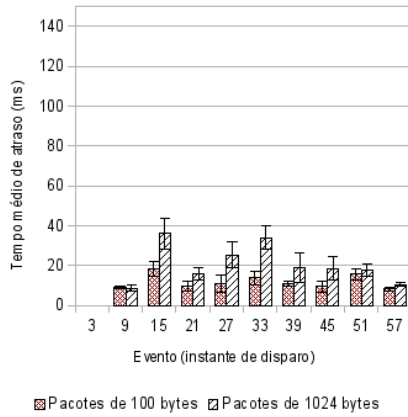


Figura 19 Latência média da infraestrutura localizada no ponto D (51 nós).

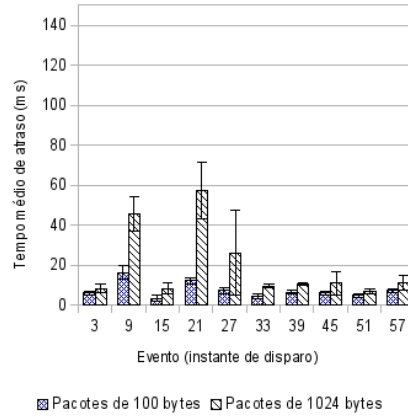


Figura 20 Latência média da infraestrutura localizada no ponto D (151 nós).

ms em todos os cenários simulados. No cenário com 51 nós, o evento do instante 3 não é recebido pelo dispositivo pois o emissor está muito distante e os nós intermediários não estão suficientemente espalhados nas vias. A latência do comunicado do evento no dispositivo fixo é proporcional à distância da posição do emissor. Em alguns eventos, os valores obtidos nos cenários com 151 nós foram menores que os obtidos com 51 nós, pois em cada cenário o deslocamento dos veículos foi diferente. Os emissores destes eventos estavam coincidentemente mais próximos do dispositivo infraestruturado, o que justifica algumas latências inferiores às obtidas em cenários com 51 nós.

6.1.4 Latência medida na infraestrutura localizada no ponto E

As Figuras 21 e 22 mostram o tempo máximo necessário para que a comunicação de um determinado evento chegue ao dispositivo de infraestrutura localizado em um dos extremos da via, neste caso no ponto E .

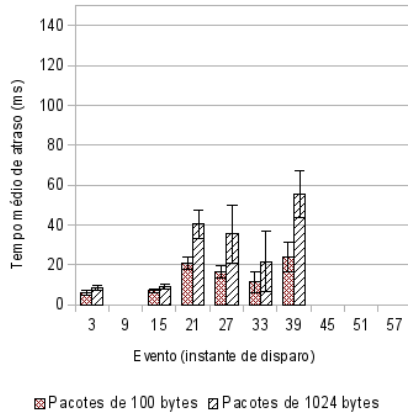


Figura 21 Latência média da infraestrutura localizada no ponto *E* (51 nós).

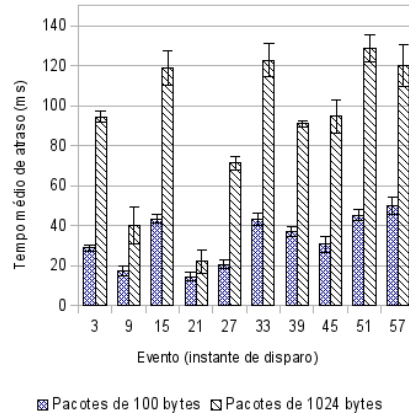


Figura 22 Latência média da infraestrutura localizada no ponto *E* (151 nós).

Quando o dispositivo foi disposto em um dos extremos, foi possível verificar que os comunicados disparados nos instantes 9, 45, 51 e 57 não foram recebidos pela infraestrutura quando foi utilizado um menor número de nós. Isto se justifica pois não há nós intermediários para viabilizar a comunicação dos eventos. No final da simulação, a maioria dos veículos se concentrava no outro extremo da malha viária. Quando se utiliza uma maior quantidade de veículos, todos os eventos chegam até o dispositivo fixo. O dispositivo, por estar localizado em um dos extremos, recebeu os comunicados dos eventos nos cenários com 151 nós, seguindo um padrão compatível com o obtido na Figura 18.

Os pontos *D* e *E* estão cerca de 500 m distantes entre si. Nos cenários avaliados a disposição de dispositivos respeitando esta distância média poderá fazer com que os comunicados dos eventos cheguem no menor tempo possível até as centrais de monitoramento. No dispositivo do ponto *E*, apesar de alguns comunicados terem latências superiores a 100 ms, os mesmos

eventos foram detectados com latências inferiores quando o dispositivo se localizava no ponto central *D*.

De maneira geral, o número de nós e o tamanho das mensagens causam impacto na latência das comunicações no dispositivo de infraestrutura, seguindo o mesmo padrão para os comunicados até o último nó da rede. No entanto, a variação do tamanho da mensagem causa um impacto maior na latência se comparado à variação da quantidade de nós da rede. Na próxima seção serão abordadas outras variáveis a serem testadas para avaliar do comportamento das redes veiculares híbridas.

Dentre todas as avaliações de latência realizadas, foram obtidos valores abaixo de 100 ms em todos os cenários com pacotes de tamanho de 100 bytes. Nos cenários onde foram transmitidos pacotes de 1024 bytes, latências inferiores a 100 ms foram obtidas apenas no cenário no qual mediu-se a latência do comunicado no dispositivo de infraestrutura, localizado no ponto *D*. A justificativa para este comportamento é que o dispositivo fixo está em uma posição relativamente central no cenário em específico, recebendo os comunicados diretamente dos emissores ou por meio de poucas retransmissões. Nos cenários restantes foram obtidas latências superiores a 100 ms, em pelo menos um dos eventos transmitidos. No entanto, mesmo com latências superiores a 100 ms, os nós que estão a uma distância significativa do evento terão um maior tempo para reagir e evitar o evento.

A posição dos emissores e dos receptores variou aleatoriamente nas diferentes repetições. Com isso, as latências das transmissões das mensagens podem variar de forma significativa entre uma repetição e outra. Esta característica reflete a dinamicidade das redes veiculares.

6.1.5 Vazão

A fim de medir a vazão de transmissão de dados, um fluxo de dados UDP contínuo foi estabelecido. O fluxo estabelecido entre o veículo 1 (OBU) e o dispositivo de infraestrutura (RSU) posicionado sempre no ponto *D*. Este ponto foi escolhido pois a infraestrutura posicionada em um ponto central apresentou melhores resultados nos testes de latência. Foi adotado o protocolo OLSR e comunicações V2X, permitindo que o pacote passe por nós intermediários (*multihops*) durante a transmissão do emissor até o destinatário. Os nós intermediários podem ser outros veículos ou o dispositivo de infraestrutura. Para cada fluxo, duas variações de tamanho de pacotes foram utilizadas: 100 bytes e 1024 bytes, a uma taxa de 2048 kbps. As Figuras 23 e 24 mostram as taxas obtidas para os experimentos com 51 e 151 nós, respectivamente. Foi considerado um intervalo de confiança de 95%.

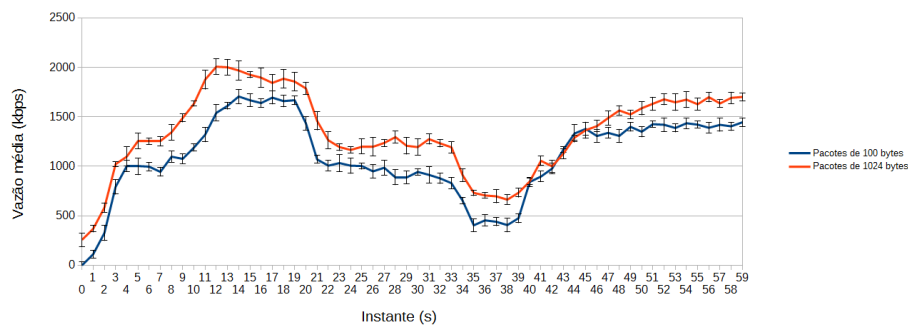


Figura 23 Vazão média (51 nós).

Os valores obtidos das simulações indicam que, quanto maior o número de nós, mais chances de haver nós intermediários capazes de manter a transferência de dados ativa. Pacotes com tamanhos maiores proporcionaram uma maior variação da vazão. Pacotes de 100 bytes tornaram a

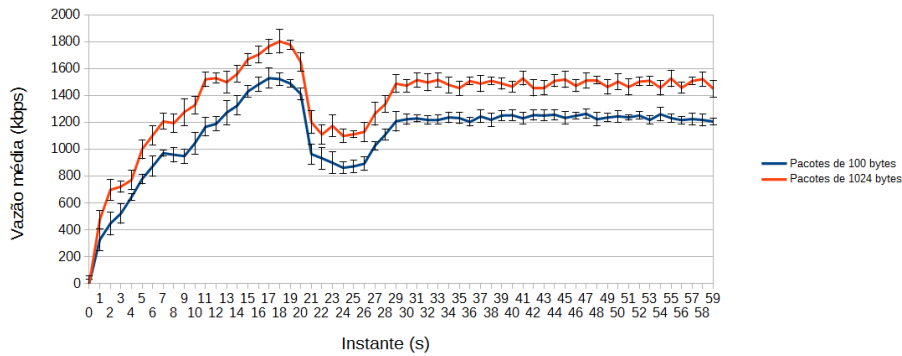


Figura 24 Vazão média (151 nós).

vazão mais estável. De acordo com Suwannasa, Puangpronpitag e Phongsir (2013), mesmo os pacotes menores estão sujeitos a *overheads* de segurança. Por isso, pacotes com tamanho de 512 bytes foram adotados na realização dos experimentos práticos.

6.2 Experimentos Práticos

Dispositivos propostos na seção 5 foram utilizados na realização dos experimentos práticos. Testes em laboratório avaliaram inicialmente a vazão e o desempenho dos protocolos de roteamento. Em seguida, testes de campo foram realizados em VANET criada entre os dispositivos, onde avaliou-se a latência, vazão e perda de pacotes.

6.2.1 Vazão máxima

Transferência de dados entre dois nós estáticos foi realizada em laboratório, a fim de identificar a máxima vazão disponibilizada pelo protocolo IEEE 802.11p na prática. Um fluxo de dados UDP foi estabelecido entre

os dois nós, com pacotes de 512 bytes. Os nós permaneceram a uma distância de 2 metros entre si, sem obstáculos. Os resultados, mostrados pela Figura 25, foram obtidos por meio de 10 repetições. O tráfego de dados teve duração total de 60 segundos.

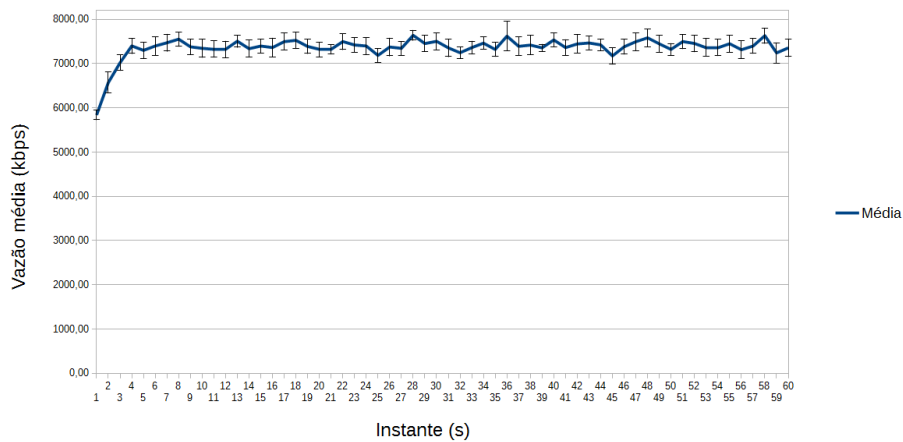


Figura 25 Taxas máximas de transferência obtida proporcionada pelo protocolo IEEE 802.11p.

Nos experimentos práticos foi possível obter taxas máximas de transmissão em torno de 7,5 Mbps (em média). Taxas menores foram obtidas no início da transmissão, estabilizando cerca de 3 segundos depois. De acordo com Consortium (2011), limitar a comunicação dos nós em, no máximo, 6 Mbps é recomendado para se obter uma melhor performance da rede. Esta melhora se justifica pois taxas maiores de transferência de dados estão mais sujeitas a oscilações proporcionadas pelo deslocamento dos nós e são mais sensíveis a fatores externos. Uma taxa de 2048 kbps foi fixada para a realização da avaliação do protocolo IEEE 802.11p pois, conforme já citado anteriormente, o foco principal das VANETs é promover a segurança no

trânsito e o tamanho dos pacotes de mensagens de emergência são pequenos, não exigindo grande quantidade de banda para serem transmitidos.

6.2.2 Protocolos de Roteamento

A fim de definir o melhor protocolo de roteamento para ser utilizado nos experimentos, testes foram realizados utilizando uma VANET com 4 nós parados. Os nós foram dispostos de uma forma em que os das extremidades só conseguiam se comunicar entre si utilizando um dos dois nós intermediários, ambos localizados em um mesmo ponto, conforme Figura 26.

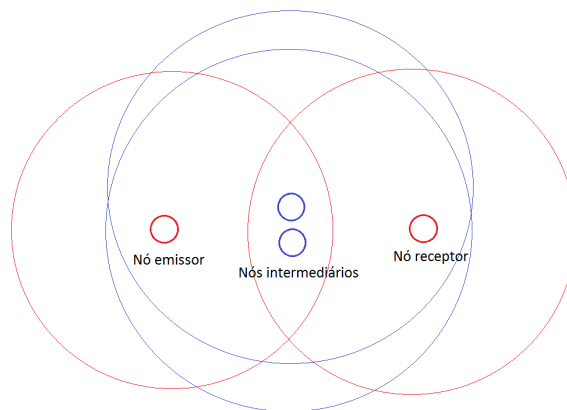


Figura 26 Posição dos nós utilizados nos testes dos protocolos de roteamento.

Para que o protocolo pudesse fazer o descobrimento de rotas, os nós intermediários alternavam seu funcionamento de forma que somente um poderia estar ativo por vez, nunca ambos. Assim o tráfego era encaminhado ora por um nó, ora por outro. O protocolo de roteamento que tivesse o

melhor desempenho em termos de latência e taxa de perda de pacotes seria o protocolo adotado nos experimentos de campo.

Um fluxo de dados UDP foi gerado entre os nós das extremidades, a uma taxa de 2048 kbps com tamanho de pacote de 512 bytes. O fluxo durou 60 segundos e, após seu início, os nós intermediários alternavam seu funcionamento a cada 10 segundos. Dois protocolos de roteamento foram testados em cada experimento: o OLSR e o BATMAN. Dez repetições deste experimento foram realizadas. Na Figura 27 mostra-se a latência média proporcionada pelos protocolos OLSR e BATMAN, considerando um intervalo de confiança de 95%.

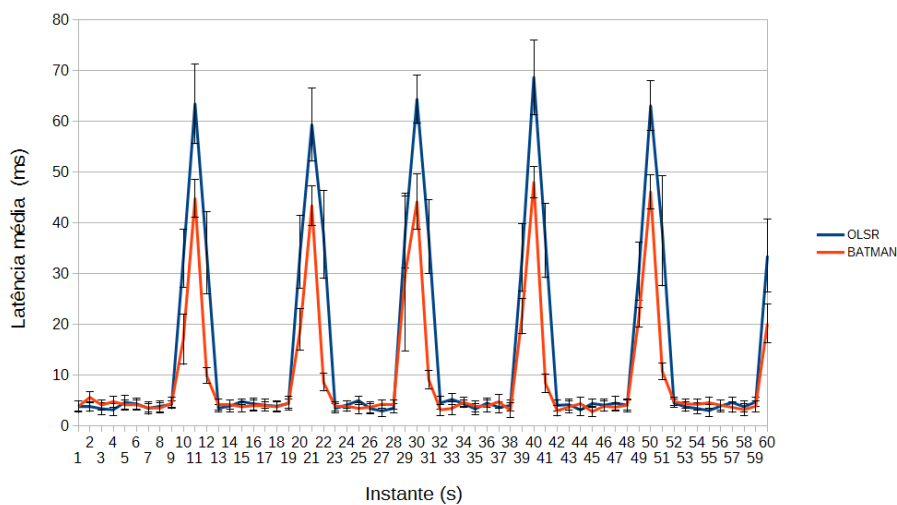


Figura 27 Latência média dos protocolos de roteamento OLSR e BATMAN.

Resultados demonstram que o OLSR tem um desempenho inferior ao BATMAN em todas as repetições. Ao alternar entre um nó e outro, o

BATMAN realizou a tarefa de descobrimento da rota em menor tempo do que o OLSR.

A Figura 28 apresenta a taxa média de perda de pacotes proporcionada pelos protocolos de roteamento OLSR e BATMAN, considerando um intervalo de confiança de 95%. Verificou-se que a taxa de perda proporcionada pelo protocolo BATMAN é menor do que a taxa do proporcionada pelo OLSR. Isto se deve ao menor tempo gasto pelo protocolo BATMAN para redirecionar o fluxo de um nó intermediário para o outro.

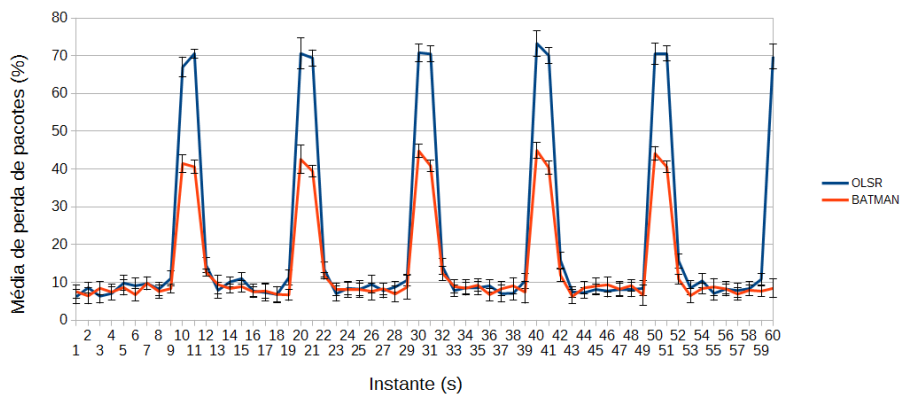


Figura 28 Média de perda de pacotes utilizando os protocolos de roteamento OLSR e BATMAN.

Pelos testes realizados, o protocolo BATMAN detecta mais rapidamente nós que entram e saem da rede, ao contrário do OLSR, que gasta mais tempo para identificar a quebra do link de um nó ou a entrada de um novo nó na rede. Os testes realizados reforçam os trabalhos de Dias (2012), que considerou o BATMAN o melhor protocolo de roteamento, superando o OLSR.

Tendo vista os resultados obtidos, optou-se por realizar os experimentos de análise desempenho do padrão IEEE 802.11p utilizando o protocolo de roteamento BATMAN, nos dispositivos de comunicação proposto.

6.2.3 IEEE 802.11p (Comunicações V2V)

Nesta seção são abordados testes realizados com apenas dois veículos móveis trocando dados no padrão IEEE 802.11p. A tecnologia 3G e o protocolo de seleção de link não foram utilizados durante a realização destes experimentos. Os veículos foram equipados com uma OBU e cada um foi posicionado inicialmente em um dos extremos da avenida (pontos 3 e 4 da Figura 7).

Em cada experimento, os nós iniciaram seus deslocamentos em um mesmo instante, e mantiveram velocidades constantes. Três velocidades foram avaliadas: 20 km/h, 40 km/h e 60 km/h. Para cada variação de velocidade, três repetições foram realizadas. Um fluxo de dados UDP, a uma taxa de 2048 kbps, foi criado entre os dois nós. A latência média obtida entre as comunicações dos nós é mostrada na Figura 29. Foram considerados somente os pacotes efetivamente recebidos pelo receptor. Os gráficos desta seção não apresentam os intervalos de confiança para facilitar a visualização.

É possível verificar que, apesar de visível, a latência média não variou de forma significativa em relação à distância. Em todas as repetições realizadas, nenhum valor médio de latência foi superior a 100ms. Foi verificado que, ao aumentar a velocidade, a latência nas comunicações também sofre incremento. Nas comunicações entre veículos, na velocidade mais alta,

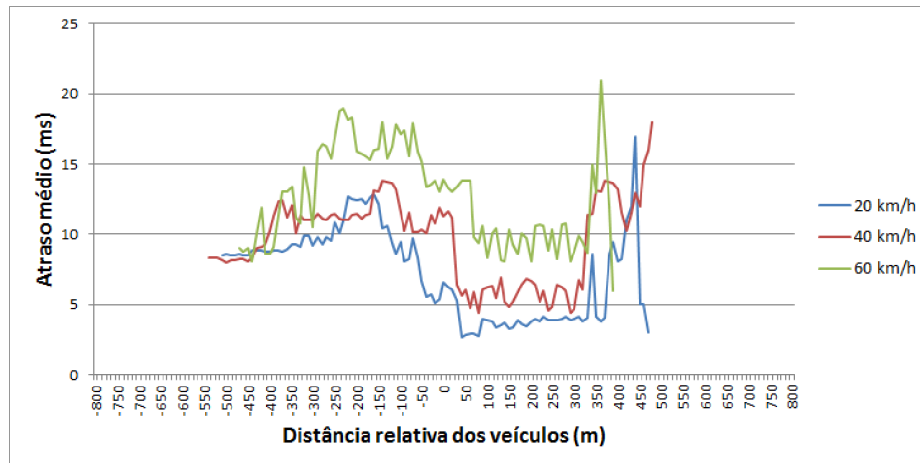


Figura 29 Latência média das comunicações V2V, usando exclusivamente o padrão IEEE 802.11p.

a velocidade relativa entre os nós foi de 120km/h. Neste cenário, os índices de latência foram os maiores.

A Figura 30 mostra a média de perda de pacotes. Os dados obtidos das três avaliações em diferentes velocidades de deslocamento mostram que a rede se comporta de maneira mais robusta enquanto os nós se movem em velocidades menores. Quanto mais próximo o veículo está do nó receptor, menor é a perda de pacotes. Quando os nós estão a uma distância relativa de até 200 metros, a perda de pacotes ficou abaixo de 10% para as comunicações V2V. A velocidade influencia na perda de pacotes. Em maiores velocidades, maiores são as perdas de pacotes.

Sobre a vazão média, a mesma é exibida na Figura 31. Os dados obtidos das três avaliações em diferentes velocidades mostram que a vazão permaneceu relativamente constante, independente da distância relativa dos nós. A taxa de transferência oscilou no início, ao se estabelecer a comunicação, mas depois se estabilizou.

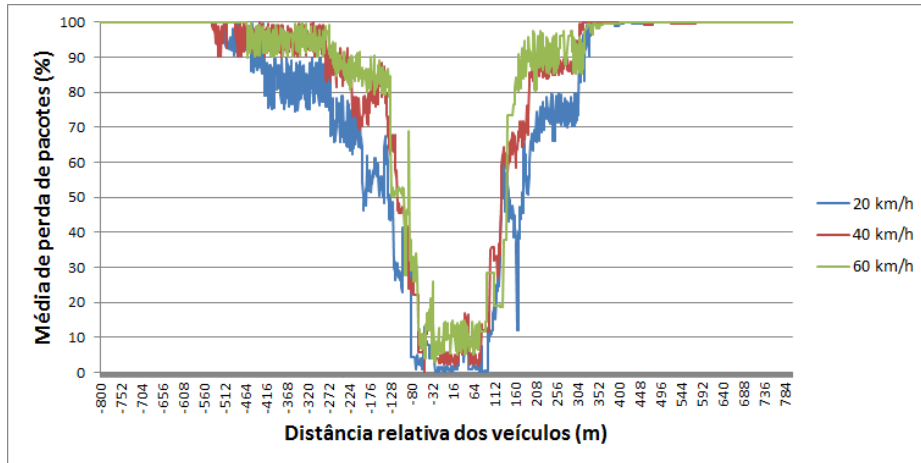


Figura 30 Média da taxa de perda de pacotes em comunicações V2V, utilizando exclusivamente o padrão IEEE 802.11p.

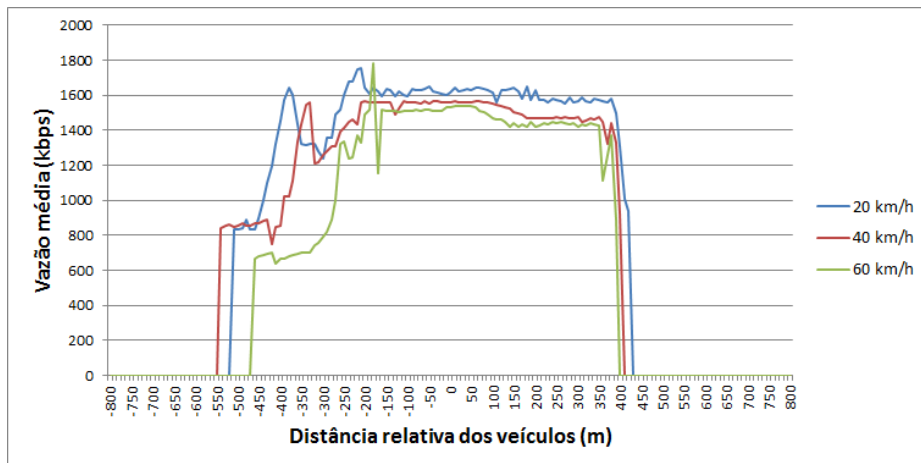


Figura 31 Vazão média em comunicações V2V, usando exclusivamente o padrão IEEE 802.11p.

Para o alcance das comunicações durante os testes foi possível verificar que o raio de cobertura do rádio de cada nó foi superior a 400 metros.

6.2.4 IEEE 802.11p (Comunicações V2X)

Nesta seção, são abordadas comunicações híbridas (V2X) no padrão IEEE 802.11p, que envolvem ao mesmo tempo comunicações entre OBU e RSU. De acordo com a Figura 7, são abordados os testes realizados com uma infraestrutura fixa (RSU) localizada no ponto 1, um veículo (OBU) estacionado no ponto 2 da avenida, e um veículo móvel (OBU) que se desloca entre os pontos 4 e 3. Três velocidades foram avaliadas: 20 km/h, 40 km/h e 60 km/h. Um fluxo de dados UDP, com velocidade de 2048 kbps foi estabelecido entre o veículo móvel e a RSU localizada no ponto 1. Três repetições foram realizadas para cada variação de velocidade. Os gráficos desta seção não apresentam os intervalos de confiança para facilitar a visualização.

A latência média obtida é mostrada na Figura 32. As distâncias nos gráficos diz respeito à distância entre o nó móvel e o veículo estacionado. Distâncias negativas indicam aproximação ao veículo estacionado. Distâncias positivas indicam o veículo se afastando deste ponto.

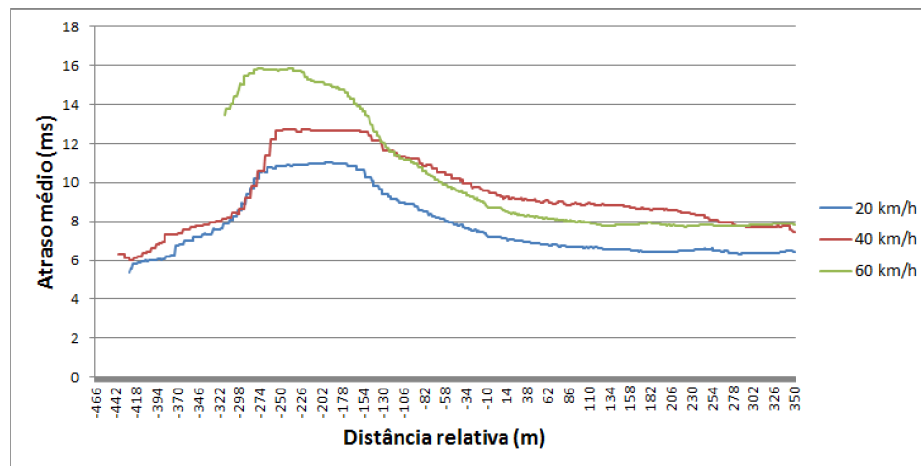


Figura 32 Latência média das comunicações V2X, usando exclusivamente o padrão IEEE 802.11p.

Os resultados obtidos indicam que a uma velocidade menor o nó móvel conseguiu iniciar a transmissão em um tempo inferior, se comparado a velocidades maiores. A 60 km/h, o nó começou a transmissão de dados a uma distância mais próxima do veículo estacionado, tendo em vista o protocolo de roteamento que detecta a presença do nó vizinho após um determinado momento. O pico de latência inicial é comum em todas as velocidades, e está relacionado à estabilização dos links de origem e destino. Apesar de discreta, foi possível verificar que em maiores velocidades e distâncias, maior é a latência nas comunicações.

Na Figura 33 está a média de perda de pacotes obtida entre as comunicações.

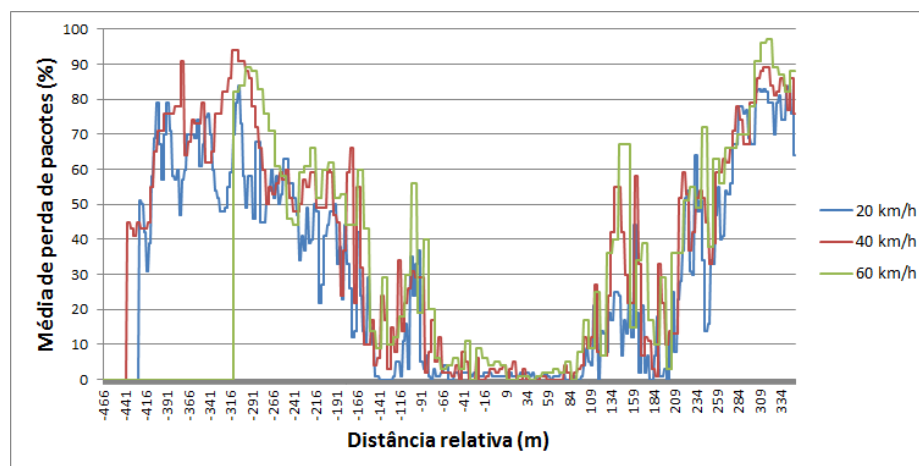


Figura 33 Taxa média de perda de pacotes, utilizando exclusivamente o padrão IEEE 802.11p em comunicações V2X.

Fica claro identificar que, em menores distâncias, o link se comporta de forma mais robusta e a perda de pacotes é menor. Quando o nó estava em distâncias inferiores a 200 metros, a perda de pacotes foi menor. Após

este limite, a qualidade da conexão fica prejudicada, fazendo com que a taxa de perdas aumente de forma mais considerável.

Para a vazão, os valores obtidos são exibidos na Figura 34.

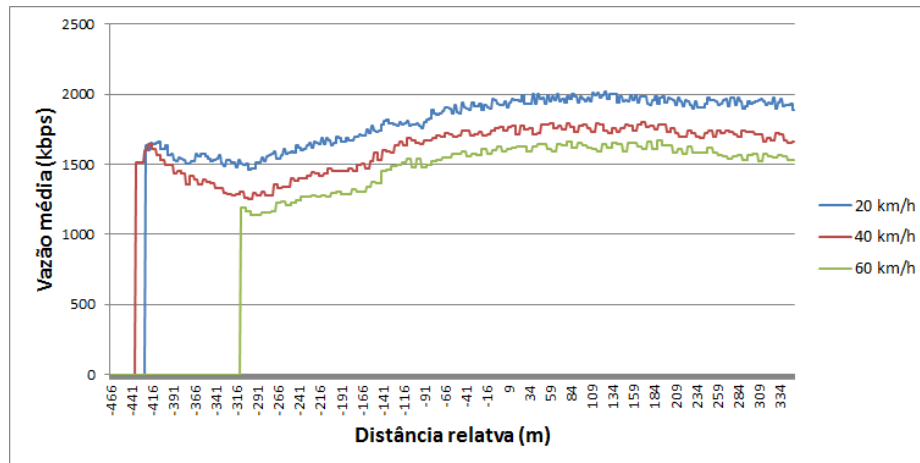


Figura 34 Vazão média utilizando exclusivamente o padrão IEEE 802.11p em comunicações V2X.

É importante dizer que o fluxo de dados foi mantido contínuo a uma velocidade de 2048 kbps. Velocidades de deslocamento mais baixas permitiram taxas de transmissão de dados maiores, se comparadas a velocidades de deslocamento maiores.

De modo geral, o comportamento do padrão IEEE 802.11p foi satisfatório ao realizar a transmissão de dados no raio de cobertura dos nós. A latência manteve-se abaixo dos 100 ms, indicando que aplicações de emergência podem fazer o uso deste padrão para transferir dados críticos (CONSORTIUM, 2004; ILBANEZ et al., 2011).

6.2.5 IEEE 802.11p e rede 3G

Nesta seção são abordados os experimentos utilizando-se o padrão IEEE 802.11p como link principal para transferência de dados e um link 3G usado como backup. As mesmas especificações utilizadas nos experimentos da seção 6.2.4 foram replicadas nestes experimentos. O ASL, mostrado na Seção 5.6 foi utilizado nestes experimentos. Os gráficos desta seção não apresentam os intervalos de confiança para facilitar a visualização.

Um fluxo de dados UDP com pacotes de 512 bytes a uma taxa de 512 kbps foi utilizado nestes experimentos. Nestes experimentos foi também adotada uma taxa de transmissão menor, pois o link 3G fornecido pela operadora móvel oscila constantemente no quesito vazão, permitindo entregar velocidades de, no máximo, 1024 kbps. Realizar os testes com taxas de transmissão maiores geraria perdas de pacotes desnecessárias.

A latência média obtida é mostrada na Figura 35. Na figura, o eixo das ordenadas está em escala logarítmica visto que os atrasos proporcionados pelo link 3G são bem maiores do que os do padrão IEEE 802.11p.

As latências proporcionadas pelo link 3G variaram entre 62 ms e 658 ms. A comunicação não foi interrompida em nenhum momento durante os testes, visto que o link 3G era utilizado quando não havia comunicação do link IEEE 802.11p. O ASL identificou valores de RSSI inferiores a -85 dBm somente em distâncias superiores a 310 m. No raio de 150 m, os nós se comunicaram somente utilizando o padrão IEEE 802.11p. Entre as distâncias de 150 m e 310 m, o ASL escolheu o melhor link possível, proporcionando a alternância sempre que necessário. Em distâncias maiores que 310 m, o link 3G era sempre utilizado. Por proporcionar latências

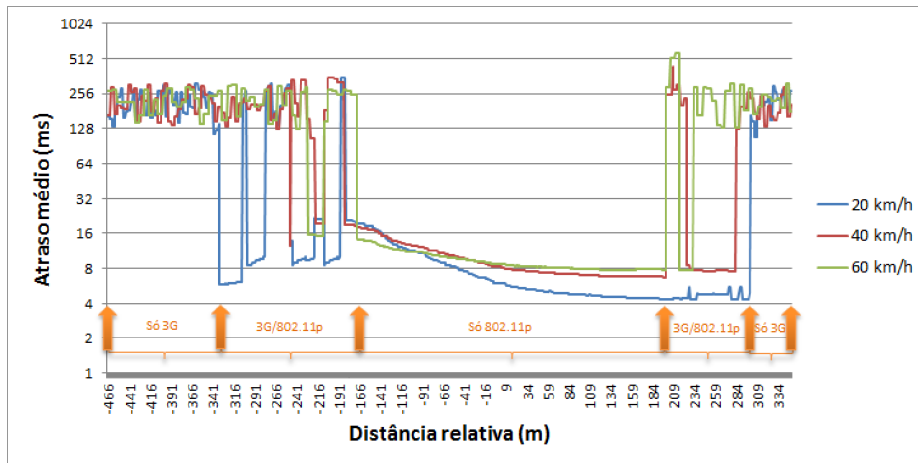


Figura 35 Latência média das comunicações, utilizando o 3G como link redundante.

superiores a 100 ms, o link 3G deve ser evitado por aplicações sensíveis a latência.

Em relação à taxa média de perda de pacotes, a Figura 36 apresenta os resultados obtidos.

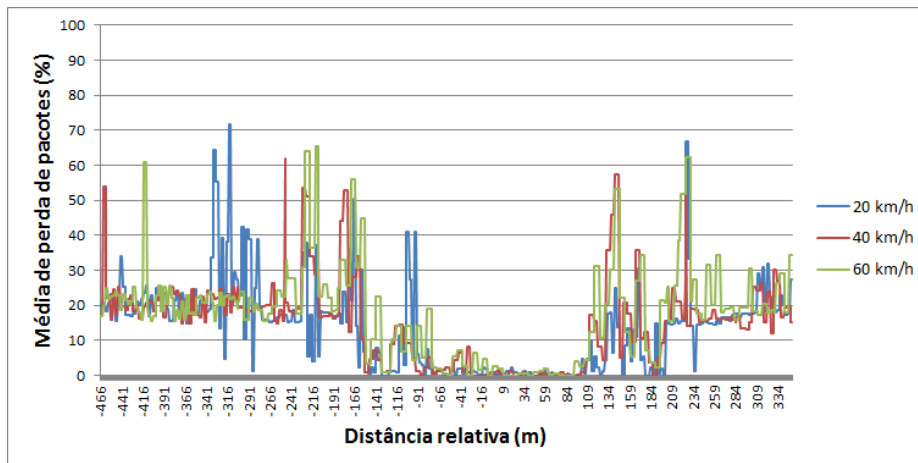


Figura 36 Média da taxa de perda de pacotes, utilizando o 3G como link redundante.

O link 3G proporcionou mais perda de pacotes que o padrão IEEE 802.11p. Tal perda proporcionada pelo 3G também variou mais intensamente. Mas em ambos os padrões, a diferença de velocidade não influenciou significativamente na taxa de perdas. O comportamento da rede foi similar mesmo com velocidades diferentes.

A vazão média é exibida na Figura 37. Foi possível verificar que no link 3G, a taxa de transmissão de dados oscilou mais intensamente do que no link IEEE 802.11p. Em relação às velocidades de deslocamento do nó, quanto maior a velocidade, menor a vazão proporcionada pelo link IEEE 802.11p. Já em relação ao link 3G, a variação da velocidade não apresentou diferença significativa na vazão.

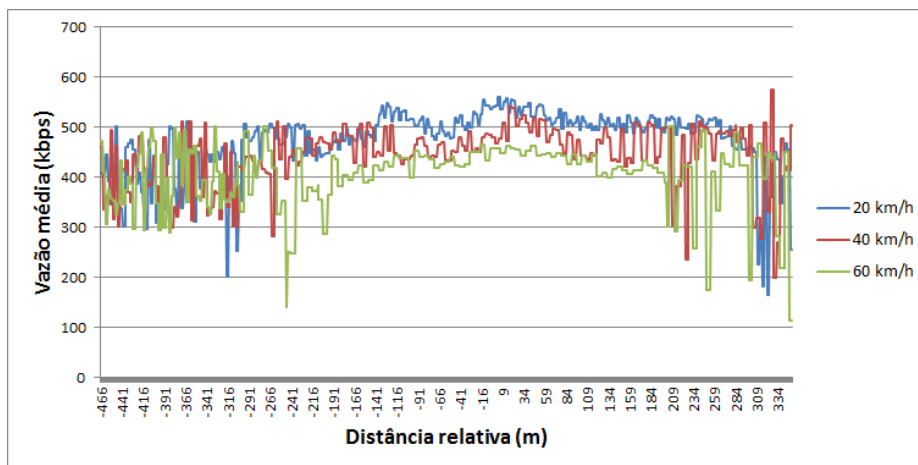


Figura 37 Vazão média utilizando o 3G como link redundante.

O dispositivo OBU equipado com o link 3G redundante apresenta mais aplicabilidade do que o modelo que possui apenas conectividade pelo padrão IEEE 802.11p. Infelizmente, redes neste padrão ainda não são populares. No entanto, disponibilidade de cobertura sinal de celular, princi-

palmente da tecnologia 3G, já é uma realidade em diversas cidades. Desta forma, o usuário já poderia usufruir de alguma aplicação celular que exige conectividade de dados utilizando este dispositivo. Mas é importante reforçar que a latência proporcionada pelo link 3G torna inviável o uso desta tecnologia por aplicações de emergência que exigem baixas latências. Os trabalhos de Consortium (2004) e Ilbanez et al. (2011) indicam que esta categoria de aplicações tolera latências de até 100 ms.

De modo geral, o uso combinado dos dois links pode ser o caminho para a popularização e adoção de dispositivos OBU em carros.

7 Conclusões e Trabalhos Futuros

Redes Veiculares é um tópico bastante amplo e com grande potencial na realização de pesquisas. O padrão IEEE 802.11p está em constante desenvolvimento, a medida que as pesquisas avançam. É de fundamental importância analisar e compreender o tráfego de dados relacionados a aplicações de segurança no trânsito, pois tais aplicações são o objetivo principal das comunicações veiculares. Outro fator importante a ser considerado é que, quando forem implantadas, as VANETs serão compostas por comunicações V2V e V2I em mesmo ambiente. Os estudos que abordam estas comunicações híbridas ainda não foram totalmente explorados e podem ser aprimorados.

Este trabalho deixa como contribuições o desenvolvimento de um hardware customizável de custo relativamente baixo, capaz de se comunicar no padrão IEEE 802.11p. Este hardware fornece uma estrutura básica para que veículos possam se comunicar, permitindo futuras pesquisas e experimentos na área.

As simulações do NS-2 foram cruciais para definir parâmetros como tamanho de pacotes e localização de dispositivos fixos nos cenários avaliados. Primordialmente, as simulações permitiram uma compreensão do tráfego de dados nas VANETs avaliadas.

O algoritmo ASL apresentou um papel importante ao garantir a conectividade nas áreas de sombra, que eventualmente ocorrem nas VANETs, durante o deslocamento dos veículos. Nos nossos testes, o ASL proporcionou conectividade ao veículo 100% do tempo. Em contrapartida, o link redundante 3G não apresentou grande capacidade de vazão de dados, e

proporcionou latências médias em torno de 200ms. Compete à operadora melhorar este comportamento do link 3G.

Os experimentos realizados para o padrão IEEE 802.11p nos cenários avaliados mostraram que, quanto maior o tamanho do pacote transferido, maior a taxa de transferência possível entre os nós e maior será a latência nas comunicações. A velocidade dos nós tem impacto negativo na latência, taxa de transmissão e perda de pacotes. Os resultados dos experimentos realizados indicam que, quanto maior a velocidade de um nó, pior é o desempenho da rede.

Como trabalhos futuros, pretendemos estender as funcionalidades do dispositivo de comunicação, implementando os protocolos da família IEEE 1609 a fim de tornar o dispositivo compatível com a Arquitetura WAVE. Também pretende-se agregar novos dispositivos de hardware (como câmera, microfone), a fim de transformar o dispositivo em uma espécie de caixa preta para veículos. Assim será possível registrar as informações do condutor e veículo localmente ou remotamente, transmitindo-as em tempo real para um servidor externo.

Acredita-se que as pesquisas utilizando o padrão IEEE 802.11p têm grande potencial para proporcionar tecnologias comerciais e acessíveis à população em geral. No nosso país é necessário que o governo regulamente uma faixa de frequência específica para as VANETs. Assim, além de garantir troca de dados entre veículos, os governos ganhariam em uma melhor gestão do trânsito, menores índices de acidentes e consequente redução com despesas hospitalares das possíveis vítimas.

REFERÊNCIAS

ABABNEH, N.; LABIOD, H. Safety message dissemination in vanets: flooding or trajectory-based? IFIP ANNUAL MEDITERRANEAN, 9., 2010, Juan-Les-Pins. **Proceedings...** Juan-Les-Pins: IEEE, 2010. p. 1-8.

ALMEIDA, V. D. D. **Análise de desempenho de protocolos de roteamento Ad Hoc e DTN em redes de emergência**. 2011. 70 p. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Minas Gerais, Belo Horizonte, 2011.

ALVES, R. D. S. et al. Uma análise experimental da capacidade de redes adhoc veiculares. SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES, 26., 2008, Rio de Janeiro. **Anais...** Rio de Janeiro: SBRT, 2008. 1 CD-ROM.

ALVES, R. D. S. et al. Redes veiculares: princípios, aplicações e desafios. SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 9., 2009, Recife. **Anais...** Recife: SBRC, 2009. p. 56.

BOOYSEN, M.; ZEADALLY, S.; ROOYEN, G. J. van. Survey of media access control protocols for vehicular ad hoc networks. **Communications IET**, Ottawa, v. 5, n. 11, p. 1619-1631, 2011.

CHENG, H. T.; SHAN, H.; ZHUANG, W. Infotainment and road safety service support in vehicular networking: from a communication perspective. **Mechanical Systems and Signal Processing**, London, v. 25, n. 6, p. 2020-2038, 2011. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S0888327010004127>>. Acesso em: 10 jan. 2014.

CONSORTIUM, C. A. M. P. V. S. C. **Vehicle safety communications project: task 3 final report: identify intelligent vehicle safety applications enabled by DSRC**. Washington: National Highway Traffic Safety Administration, 2004. Disponível em: <<http://books.google.com.br/books?id=BwmMNwAACAAJ>>. Acesso em: 10 dez. 2013.

CONSORTIUM, T. C. V. S. C. **Vehicle safety communications applications (VSC-A): final report**. Washington: Department of Transportation, 2011. 102 p. Disponível em: <<http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2011/811492A.pdf>>. Acesso em: 10 dez. 2013.

COUTO, R. D. S. et al. **Uma avaliação experimental do roteamento das redes em malha sem-fio em ambientes fechados**. Blumenau: SBRC, 2009. 6 p.

DIAS, J. F. **Mobilidade em comunicações veiculares**. 2012. 142 p. Dissertação (Mestrado em Engenharia Eletrônica e Telecomunicações) - Universidade de Aveiro, Aveiro, 2012.

ELNASHAR, A.; EL-SAIDNY, M. Looking at lte in practice: a performance analysis of the lte system based on field test results. **IEEE Vehicular Technology Magazine**, New York, v. 8, n. 3, p. 81-92, Sept. 2013.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **En draft 302 571 v 1.2.0, intelligent transport systems (its):** radiocommunications equipment operating in the 5855 mhz to 5925 mhz frequency band: harmonized en covering the essential requirements of article 3.2 of the rtte directive. Paris: Intelligent Transport Systems, 2013. 47 p.

FURUSKAR, A. et al. Edge: enhanced data rates for gsm and tdma/136 evolution. **IEEE Personal Communications**, New York, v. 6, n. 3, p. 56-66, June 1999.

GONZALEZ, V. et al. Experimental demonstration of the viability of Ieee 802.11b based inter-vehicle communications. INTERNATIONAL CONFERENCE ON TESTBEDS AND RESEARCH INFRASTRUCTURES FOR THE DEVELOPMENT OF NETWORKS & COMMUNITIES, 4., 2008, Brussels. **Proceedings...** Brussels: ICST, 2008. p. 1:1-1:7. Disponível em: <<http://dl.acm.org/citation.cfm?id=1390576.1390578>>. Acesso em: 12 dez. 2013.

GRÄFLING, S.; MAHONEN, P.; RIIHIJÄRVI, J. Performance evaluation of ieee 1609 wave and ieee 802.11p for vehicular communications. UBIQUITOUS AND FUTURE NETWORKS INTERNATIONAL CONFERENCE, 2., 2010, Jeju Island. **Proceedings...** Jeju Island: ICUFN, 2010. p. 344-348.

GROUP, I. W. **IEEE 1609 working group public site**. Disponível em: <http://vii.path.berkeley.edu/1609_wave/>. Acesso em: 12 dez. 2013.

GUKHOOL, B.; CHERKAOUI, S. Ieee 802.11p modeling in ns-2. IEEE CONFERENCE, 33., 2008, Montreal. **Proceedings...** Montreal: LCN, 2008. p. 622-626.

HARTENSTEIN, H.; LABERTEAUX, K. A tutorial survey on vehicular adhoc networks. **IEEE Communications Magazine**, New York, v. 46, n. 6, p. 164-171, June 2008.

HOLMA, H. et al. Highspeed packet access evolution in 3gpp release 7: topics in radio communications. **IEEE Communications Magazine**, New York, v. 45, n. 12, p. 29-35, Dec. 2007.

IEEE STANDARD FOR INFORMATION TECHNOLOGY. **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**. New York, 2010. 51 p.

ILBANEZ, A. G. et al. A performance study of the 802.11p standard for vehicular applications. INTELLIGENT ENVIRONMENTS, INTERNATIONAL CONFERENCE ON IEEE COMPUTER SOCIETY, 1., 2011, Nottingham. **Proceedings...** Nottingham: IEEE, 2011. p. 165-170.

JUNG, C. F. **Metodologia para pesquisa e desenvolvimento: aplicada a novas tecnologias, produtos e processos**. Rio de Janeiro: Axcel Books, 2004. 328 p.

KAMAL, F.; LOU, E.; ZHAO, V. Design and validation of a small-scale 5.9 ghz dsrc system for vehicular communication. IEEE CANADIAN CONFERENCE, 25., 2012, Montreal. **Proceedings...** Montreal: CCECE, 2012. p. 1-4.

KARAGIANNIS, G. et al. Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions. **IEEE Communications Surveys Tutorials**, New York, v. 13, n. 4, p. 584-616, 2011.

LI, X. et al. Hsupa backhaul bandwidth dimensioning. IEEE INTERNATIONAL SYMPOSIUM, 19., 2008, Cannes. **Proceedings...** Cannes: PIMRC, 2008. p. 1-6.

LI, Y. J. An overview of the dsrc/wave technology. **Quality, reliability, security and robustness in heterogeneous networks**. New York: Springer, 2012. p. 544-558.

LIDSTRÖM, K. et al. **Halmstad university grand cooperative driving challenge 2011 technical paper**. Halmstad: Halmstad University, 2011. 14 p.

MARTELLI, F.; RENDA, M.; SANTI, P. Measuring Ieee 802.11p performance for active safety applications in cooperative vehicular systems. VEHICULAR

TECHNOLOGY CONFERENCE, 73., 2011, Budapest. **Proceedings...**
Budapest: VTC Spring, 2011. p. 1-5.

MIAO, L. et al. Evaluation and enhancement of Ieee 802.11 p standard: a survey. **Mobile computing**. Riley: ASERican V-King Scientific, 2011. p. 1-7.

MIKROTIK. **Routerboard website**. Disponível em:
<<http://www.routerboard.com>>. Acesso em: 10 jan. 2014.

MONKS, J.; BHARGHAVAN, V.; HWU, W. M. A power controlled multiple access protocol for wireless packet networks. ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER AND COMMUNICATIONS SOCIETIES, 20., 2001, Anchorage. **Proceedings...** Anchorage: IEEE, 2001. v. 1, p. 219-228.

MURRAY, T.; COJOCARI, M.; FU, H. Measuring the performance of IEEE 802.11p using ns-2 simulator for vehicular networks. IEEE INTERNATIONAL CONFERENCE, 2008, Ames. **Proceedings...** Ames: EIT, 2008. p. 498-503.

NEUMANN, A.; AICHELE, C. E.; LINDNER, M. B. A. T. M. A. N. **Status report**. München: GUNet, 2007. 13 p.

NEVES, F. et al. Real-world evaluation of IEEE 802.11p for vehicular networks. ACM INTERNATIONAL WORKSHOP ON VEHICULAR INTER-NETWORKING, 8., 2011, New York. **Proceedings...** New York: ACM, 2011. p. 89-90.

OPENWRT, D. T. **OpenWRT website**. Disponível em: <<https://openwrt.org>>. Acesso em: 12 dez. 2013.

ORGANIZATION, W. H. **Global status report on road safety 2013: supporting a decade of action**. Geneva: World Health Organization, 2013. Disponível em: <<http://books.google.com.br/books?id=qzK2nQEACAAJ>>. Acesso em: 20 dez. 2013.

RAWAT, D. et al. Dynamic adaptation of joint transmission power and contention window in VANET. IEEE CONFERENCE, 70., 2009, Anchorage. **Proceedings...** Anchorage: VTC, 2009. p. 1-5.

SHAH, S. Umts: high speed packet access (HSPA) technology. NETWORKING AND COMMUNICATIONS CONFERENCE, 2008, Lahore. **Proceedings...** Lahore: IEEE International, 2008. p. 2.

SICHITIU, M.; KIHIL, M. Inter-vehicle communication systems: a survey. **IEEE Communications Surveys Tutorials**, New York, v. 10, n. 2, p. 88-105, 2008.

SPAHO, E. et al. Performance evaluation of olsr and aodv protocols in a vanet crossroad scenario. **INTERNATIONAL CONFERENCE, 27.**, 2013, Barcelona. **Proceedings...** Barcelona: AINA, 2013. p. 577-582.

SUWANNASA, A.; PUANGPRONPITAG, S.; PHONGSIRI, W. A novel authentication scheme for v2i communication based on wave unicast services. **International Journal of Distributed Sensor Networks**, Cairo, v. 1, p. 10, 2013.

TEIXEIRA, F. A.; SILVA, V. F.; LEONI, J. L.; SANTOS, G. C.; SOUZA, A.; MACEDO, D. F.; NOGUEIRA, J. M. S. Análise experimental de redes veiculares utilizando o padrão iee 802.11p. Em: Anais do V Simpósio Brasileiro de Computação Ubíqua e Pervasiva (SBCUP). Maceió. **Anais...** Maceió: SBCUP, 2013. p. 10.

UZCATEGUI, R.; ACOSTA-MARUM, G. Wave: a tutorial. **IEEE Communications Magazine**, New York, v. 47, n. 5, p. 126-133, May 2009.

VANDENBERGHE, W.; MOERMAN, I.; DEMEESTER, P. Approximation of the Ieee 802.11p standard using commercial off-the-shelf iee 802.11a hardware. **INTERNATIONAL CONFERENCE, 11.**, 2011, Saint Pittsburg. **Proceedings...** Saint Pittsburg: ITST, 2011. p. 21-26.

VEGNI, A. M.; LITTLE, T. D. Hybrid vehicular communications based on v2v-v2i protocol switching. **International Journal of Vehicle Information and Communication Systems, Inderscience**, Michigan, v. 2, n. 3, p. 213-231, 2011.

VERKEHR, A. **Kooperative technologien für den I. Aktiv**. Disponível em: <<http://aktiv-online.org>>. Acesso em: 10 nov. 2013.

WEI, L. et al. Power-control-based broadcast scheme for emergency messages in vanets. **INTERNATIONAL SYMPOSIUM, 11.**, 2011. Hangzhou. **Proceedings...** Hangzhou: ISCIT, 2011. p. 274-279.

YAMAUCHI, K.; CHEN, W.; WEI, D. 3g mobile phone applications in telemedicine: a survey. **INTERNATIONAL CONFERENCE ON COMPUTER AND INFORMATION TECHNOLOGY, 5.**, 2005, Xangai. **Proceedings...** Xangai: CIT, 2005. p. 956-960.

ANEXOS

ANEXO A - Padrões IEEE 1609

A Padrões IEEE 1609

A Arquitetura WAVE é composta por quatro documentos do padrão IEEE 1609. Uma breve descrição destes documentos é realizada a seguir, baseada nos trabalhos de Li (2012) e Uzcategui e Acosta-Marum (2009).

A.1 IEEE P1609.1 – Gerenciamento de Recursos

O padrão IEEE 1609.1 define a aplicação WAVE denominada gerenciamento de recursos, que tem o objetivo de fornecer determinados acessos aos recursos de comunicação do sistema. Este padrão recebe requisições de aplicações denominadas de aplicações de gerenciamento de recursos, que são executadas remotamente em outros hosts. O objetivo destas aplicações é usar os recursos de uma ou mais OBUs. O gerenciamento de recursos atua como um corretor que retransmite comandos e respostas entre o as aplicações de gerenciamento de recursos e as OBUs. Uma entidade de software chamada de processador de comandos de recurso, localizado na OBU, executa os comandos enviados pelo gerenciador de recurso em nome das aplicações que realizam as solicitações.

Quando uma solicitação de recurso é realizada pela aplicação de gerenciamento de recursos remota, a camada de gerenciamento de recursos registra a solicitação no plano de gerenciamento de recursos local. Esta solicitação, quando realizada, é atendida pelo processador de comandos de recursos que verifica a disponibilidade e reserva para a aplicação caso estejam disponíveis. Para que o recurso possa ser utilizado, uma notificação é realizada ao host solicitante, para que se junte ao *WAVE Basic Service Set* (WBSS). O WBSS equivalem a pequenas redes, formadas pelos nós que estão utilizando determinado serviço. O solicitante então utiliza os re-

recursos solicitados até que a aplicação de gerenciamento de recursos deseje terminar a sessão, solicitação que também é processada por esta camada de gerenciamento de recursos e pelo processador de comandos de recursos.

Alguns exemplos dos recursos que as aplicações de gerenciamento de recursos podem controlar são: acesso à memória (leitura e escrita), interfaces de usuário que estão incluídas como parte da OBU, barramentos especializados e outros equipamentos de segurança opcionais que podem estar acoplados à OBU (como sensores, entre outros).

Este conceito de manipulação de recursos foi necessário para reduzir custos, pois a aplicação não precisa ser executada inteiramente na OBU, não havendo necessidade de hardware robusto. Apenas os recursos necessários locais necessitados por aplicações remotas são fornecidos.

A.2 IEEE 1609.2 – Serviços de Segurança

Devido à ampla possibilidade de utilização das VANETs por diversas aplicações, estas redes enfrentam problemas específicos de segurança. Um exemplo são as aplicações de emergência, que necessitam de baixas latências, para isto a banda e o processamento devem ser mínimos. Além disto, os mecanismos de autenticação das mensagens deve ser o mais escalável e flexível possível. Garantir um mecanismo flexível, com baixo *overhead* para atender às demandas das aplicações é uma tarefa desafiadora. Afinal, as mensagens devem ser protegidas de captura, alterações e retransmissões por usuários mal-intencionados. E outros pontos, como a privacidade do usuário, vazamento de informações pessoais e uso de informação privada sem autorização devem ser tratados.

O padrão IEEE 1609.2 trata destes desafios. Nele, encontra-se serviços de segurança para a arquitetura WAVE e para aplicações que rodam nestas redes. São abordados mecanismos de criptografia e autenticação de mensagens de gerenciamento WAVE e de outras mensagens que não requerem anonimidade. Desta forma, é possível garantir que a informação crítica na rede é real, autêntica e, em determinados casos, anônima. Para atingir esses objetivos são utilizadas chaves secretas para codificação e decodificação da informação, algoritmos assimétricos, como usos de chaves de criptografia públicas e privadas, e funções *hash* para codificar as informações. Quanto maior a quantidade de ferramentas utilizadas, maior será o tempo para decodificação da informação, e mais segura será a transmissão da informação.

A.3 IEEE 1609.3 – Serviços de Rede

O padrão IEEE 1609.3 especifica funções associadas às camadas *Open Systems Interconnection* (OSI) de enlace, rede e transporte da arquitetura WAVE. De forma geral, este padrão pode ser dividido em Plano de Serviços de Dados e Plano de Gerenciamento de Serviços.

No Plano de Dados são especificados o suporte ao tradicional protocolo IP e ao específico *Wave Short Message Protocol* (WSMP). Desta forma, é possível transferir dados sensíveis ao tempo e de alta prioridade por meio do WSMP e outros pacotes tradicionais por meio do UDP/TCP/IP. Os dispositivos que suportam WSMP devem estar habilitados para tratar e/ou encaminhar pacotes *Wave Short Message* (WSM) para os respectivos nós.

No Plano de Gerenciamento de Serviços, também conhecido como *WAVE Management Entity* (WME), são tratados dos seguintes temas:

- Registro de aplicações: Cada aplicação que deseja utilizar a arquitetura WAVE deve ser registrada primeiramente por meio do WME. Cada aplicação é registrada com um identificador único e por meio de três campos. O primeiro contém a informação das aplicações que disponibilizam um determinado serviço. O segundo campo registra os serviços que são de interesse da aplicação em residir localmente na unidade, e o terceiro campo contém o endereço IP, portas e outros campos utilizados por aplicações externas para notificações.
- Gerenciamento do WBSS: O WME deve iniciar uma WBSS relacionada com uma determinada aplicação que disponibiliza um serviço. Para isto deve ser estabelecido um link, inclusão/remoção de credenciais de segurança, manutenção do WBSS baseado no estado da aplicação, e por último, encerramento do WBSS.
- Monitoramento de utilização de canais: Apesar deste padrão não definir como o monitoramento de canais deve ser feito, o WME deve monitorar o uso dos SCH e CCH a fim de escolher e alocar os canais menos utilizados às WBSS.
- Configuração do IPv6: Gerencia o endereço IPv6 da unidade, para que as aplicações possam ser executadas corretamente.
- Monitoramento do indicador de potência do canal recebido: Qualquer aplicação poderá solicitar a um dispositivo remoto sobre a força do sinal recebido. Isto é útil para uma melhor utilização dos serviços, e se necessário o WME poderá tomar alguma providência para trocar de canal.

- Manutenção do gerenciamento da base de informação: O WME mantém o gerenciamento da base de informação que se refere a informações relacionadas ao sistema e de rede, como endereço do roteador, *gateway*, DNS, MAC, tamanho da WSM, porta de registro, taxa e potência de transmissão, entre outros.

A.4 IEEE 1609.4 – Operação Multicanal

A arquitetura WAVE suporta aplicações gerais, que devem ser executadas em canais de serviços, e aplicações críticas, que devem sempre ser transmitidas no canal de controle. Coordenar e otimizar a alternância constante de canais é fundamental para o correto funcionamento da rede. Esta coordenação é baseada no controle de acesso ao meio do padrão IEEE 802.11 e interage com as seguintes camadas: de enlace do padrão IEEE 802.2 e física do padrão IEEE 802.11.

A contenção do MAC é realizada pelo EDCA de acordo com a prioridade do serviço do usuário. A coordenação dos canais é realizada de acordo com as operações de sincronização de canais da camada MAC. Desta forma, os pacotes de cada serviço são transferidos nos canais corretos. O padrão dá prioridade para o WSMP, baseado no tipo do serviço e no cabeçalho do pacote.

São dois os tipos de informação que são transmitidos na arquitetura WAVE: os frames de dados e os frames de gerenciamento. Os frames de anúncio são transmitidos somente no CCH. As WSM podem ser transmitidas, tanto em um SCH, quanto no CCH. A coordenação de canal baseia-se no Tempo Universal Coordenado (UTC), garantindo que todos os dispositivos da rede estarão escutando o CCH no mesmo instante de tempo.

O mecanismo garante também que, os nós inscritos em uma determinada WBSS irão acessar seu respectivo canal no mesmo instante.