THIAGO CARVALHO AMARANTE

DETECÇÃO AUTOMÁTICA E ALERTA DE ACIDENTES DE TRÂNSITO EM REDES VEICULARES REAIS

LAVRAS - MG

2015

THIAGO CARVALHO AMARANTE

DETECÇÃO AUTOMÁTICA E ALERTA DE ACIDENTES DE TRÂNSITO EM REDES VEICULARES REAIS

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

2015

Ficha catalográfica elaborada pelo Sistema de Geração de Ficha Catalográfica da Biblioteca Universitária da UFLA, com dados informados pelo(a) próprio(a) autor(a).

Amarante, Thiago Carvalho.
Detecção automática e alerta de acidentes de trânsito em redes veiculares reais / Thiago Carvalho Amarante. – Lavras : UFLA, 2015.
90 p. : il.

Dissertação (mestrado acadêmico)–Universidade Federal de Lavras, 2015.
Orientador(a): Luiz Henrique Andrade Correia.
Bibliografia.

1. Redes Veiculares. 2. VANET. 3. Detecção de acidentes. 4. Disseminação de alertas. I. Universidade Federal de Lavras. II. Título.

THIAGO CARVALHO AMARANTE

DETECÇÃO AUTOMÁTICA E ALERTA DE ACIDENTES DE TRÂNSITO EM REDES VEICULARES REAIS

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 24 de abril de 2015.

Dr. Daniel Fernandes Macedo UFMG

Dr. Arthur de Miranda Neto UFLA

Dr. Luiz Henrique Andrade Correia

Orientador

LAVRAS - MG

2015

Dedico esta dissertação aos meus pais, Guilherme e Lenice, a minha avó, Lucy, e a minha madrinha, Maria Célia, que sempre lutaram pela minha educação e tonaram possível que eu chegasse até aqui.

AGRADECIMENTOS

Agradeço ao meu orientador professor Luiz Henrique pelas dicas, conselhos e por estar sempre pronto para ajudar.

Agradeço ao professor Vladimir que, enquanto colega de pós-graduação, deixou o trabalho que serviu de base para o meu e, após terminar seu mestrado, continuou me auxiliando em tudo que pôde.

Agradeço aos amigos Carlos e Luciano que também contribuíram diretamente para a realização deste trabalho.

Agradeço aos amigos Ariel, Dyego, Gilson, João Paulo, João Renato, Lucas e Paulo que dedicaram algumas horas para me ajudar com os experimentos e/ou me ajudaram compartilhando conhecimento.

Agradeço à Mitah por proporcionar tempo para a realização das tarefas do mestrado permitindo que eu as conciliasse com o trabalho.

Agradeço aos meus pais, minhas irmãs, à Taiza, e todos familiares por me apoiarem sempre.

Agradeço a todos os meus colegas do PPGCC da UFLA pela ajuda durante as disciplinas do mestrado.

Agradeço a todos os professores do PPGCC da UFLA pelas instruções e conhecimentos passados.

Agradeço à secretaria do PPGCC da UFLA pela pronta disponibilidade.

RESUMO

Milhões de pessoas morrem anualmente vítimas de acidentes de trânsito no mundo. Para proporcionar maior segurança no trânsito, foram desenvolvidas redes de comunicação que podem prover troca de informações entre veículos, as VANETs (*Veicular Ad Hoc Networks*). Este trabalho apresenta como solução de segurança no trânsito, uma aplicação de detecção e alerta automáticos de acidente utilizando VANETs. A transmissão de alertas de acidente é feita de forma epidêmica e oportunista, se espalhando por todos os dispositivos da VANET que se encontram dentro do raio de interesse da informação do acidente. Foram considerados requisitos de qualidade de serviço para aplicações de segurança de trânsito e desenvolvidos algoritmos de detecção de acidentes e disseminação de alertas na VANET. A aplicação foi avaliada em um dispositivo real de comunicação. Os resultados mostram que é possível transmitir alertas entre veículos e entre veículos e infraestrutura. Os alertas foram transmitidos com valores de latência abaixo de 100 milissegundos e com alcances superiores a 150 metros nos cenários avaliados.

Palavras-chaves: Redes veiculares. VANET. Detecção de acidentes. Disseminação de alertas.

ABSTRACT

Millions of people die annually around the world, victims of traffic accidents. In order to provide greater traffic safety, communication networks that can provide the exchange of information between vehicles was developed, the VANETs (Vehicular Ad Hoc Networks). This work presents as solution for traffic safety an application of automatic detection and warning for traffic accidents using VANETs. The transmission of accident warnings is done in an epidemic and opportunistic manner, spreading throughout all VANET devices found within the radius of interest to the accident information. We considered service quality requisites for the application of traffic safety and developed accident detection and warning dissemination algorithms in VANET. The application was evaluated in a real communication device. The results showed that it is possible to transmit warnings between vehicles and between vehicles and infrastructures. The warnings were transmitted with latency values below 100 milliseconds and with ranges superior to 150 meters in the evaluated sceneries.

Keywords: Veihcular networks. VANET. Accident detection. Warning dissemination.

LISTA DE FIGURAS

Figura 1 Comunicações V2V, V2I E V2X 21
Figura 2 A pilha de protocolos da arquitetura WAVE..... 26
Figura 3 Alocação de espectro para aplicações DSRC. 27
Figura 4 Componentes tratados pelo padrão IEEE (2006). 28
Figura 5 Escopo do padrão IEEE 1609.3 (IEEE, 2010b). 31
Figura 6 O padrão IEEE 1609.4..... 34
Figura 7 O conector para *scanners* do OBD 2. 38
Figura 8 Formato do quadro do OBD 2 para os padrões SAE J1850, ISO 9141-2 e ISO 14230-4. 38
Figura 9 Formato do quadro do OBD 2 para o padrão ISO 15765-4. 39
Figura 10 Estrutura utilizada no AGPS..... 43
Figura 11 Características da aceleração e velocidade em batida a 48 Km/h..... 44
Figura 12 Características da aceleração e velocidade em batidas..... 45
Figura 13 O protocolo de roteamento Epidêmico. 47
Figura 14 Estrutura do sistema..... 52
Figura 15 Primeiro ambiente: o veículo. 53
Figura 16 Segundo ambiente: as vias de trânsito 54
Figura 17 Terceiro ambiente: internet. 56
Figura 18 Informações recebidas em notação JSON pela OBU por meio do dispositivo móvel..... 58
Figura 19 Alerta de acidente salvo em banco de dados pela aplicação em notação JSON. 62
Figura 20 Avenida central da UFLA, cenário utilizado nos experimentos. 65
Figura 21 Cenário utilizado para o primeiro experimento. 66
Figura 22 Cenário utilizado para o segundo experimento..... 67
Figura 23 Cenário utilizado no terceiro experimento. 68
Figura 24 Pontos de coleta de informações do veículo 2 no primeiro experimento. 70
Figura 25 Comunicação entre os Veículos 1 e 2 no primeiro experimento. 71
Figura 26 Comunicação entre o veículo 2 e a RSU no primeiro experimento. 72
Figura 27 Coletas de dados dos veículos no segundo experimento..... 74
Figura 28 Comunicação entre os veículos no segundo experimento..... 75

Figura 29 Pontos do trajeto em que foram coletados dados dos veículos..... 77
Figura 30 Página *web* disponibilizada para centrais de socorro..... 78

LISTA DE TABELAS

Tabela 1 Requisitos de qualidade de serviço para aplicações de segurança de trânsito. 23
Tabela 2 Lista de protocolos que fazem parte da arquitetura WAVE. 25
Tabela 3 Descrição dos pinos do conector para *scanners* OBD 2..... 39
Tabela 4 Exemplos de comandos do OBD 2. 40
Tabela 5 Comparação entre os trabalhos relacionados e a solução proposta neste trabalho. 50
Tabela 6 Modelo de arquitetura de comunicação. 51
Tabela 7 Configurações e equipamentos utilizados nos experimentos. 66

LISTA DE SIGLAS

3G	Tecnologia Celular de Terceira Geração
4G	Tecnologia Celular de Quarta Geração
AGPS	*Assisted Global Positioning System*
APDU	*Application Protocol Data Unit*
API	*Application Programming Interface*
ASDU	*Application Service Data Units*
ASN.1	*Abstract Syntax Notation One*
BATMAN	*Better Approach To Mobile Ad-hoc Networking*
CAN	*Controller Area Network*
CCH	Canal de Controle
DCC	Departamento de Ciência da Computação
DNIT	Departamento Nacional de Infraestrutura de Transporte
DSRC	*Dedicated Short-Range Communications*
DTN	*Delay Tolerant Network*
EDCA	*Enhanced Distributed Channel Access*
EPS	*Electronic Payment Service*
FCC	*Federal Comunications Commission of United States*
GND	*Ground*, terra
GPS	*Global Positioning System*
IEEE	*Institute of Electrical and Electronics Engineers*
IP	Protocolo de Internet
IPv6	Protocolo de Internet Versão 6
ISO	*International Organization for Standardization*
ITS	*Intelligent Transportation System*
IVHS	*Intelligent Vehicle Highway Systems*
JSON	*JavaScript Object Notation*
LLC	*Logical Link Control*
MAC	Camada de controle de acesso
MIB	*Management Information Base*
MIC	*Message Integrity Check*
MSDU	*MAC Service Data Unit*
OBD 2	*Onboard Diagnostic 2*
OBU	*Onboard Unit*
OFDM	*Orthogonal Frequency-division Multiplexing*
OGM	*OriGinator Message*
OSI	*Open Systems Interconnection*

PDU	*Protocol Data Units*
PHY	Camada física
PSID	*Provider Service Identifier*
RCP	*Resource Command Processor*
RM	*Resource Manager*
RMA	*Resource Manager Applications*
RSU	*Roadside Unit*
SAE	*Society of Automotive Engineers*
SCH	Canal de Serviços
SDU	*Service Data Units*
SHA-1	*Secure Hash Algorithm*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
UFLA	Universidade Federal de Lavras
USB	*Universal Serial Bus*
UTC	*Coordinated Universal Time*
V2I	*Vehicle to Infrastructure*
V2V	*Vehicle to Vehicle*
V2X	*Vehicle to X*, comunicações híbridas
VANET	*Vehicular Ad Hoc Network*
WAVE	*Wireless Access in Vehicular Enviroment*
WME	*WAVE Management Entity*
WSA	Anúncios de Serviços WAVE
WSM	*WAVE Short Message*
WSMP	*WAVE Short Message Protocol*

SUMÁRIO

1 INTRODUÇÃO 15
1.1 Motivação e definição do problema 18
1.2 Objetivo 18
1.2.1 Objetivos específicos 19
1.3 Estrutura do trabalho 19
2 REFERENCIAL TEÓRICO 20
2.1 Redes *ad hoc* 20
2.2 Redes Veiculares Ad Hoc (VANET) 20
2.3 Arquitetura WAVE 24
2.3.1 Padrão IEEE 802.11p: Camadas Física e de Controle de Acesso ao Meio 26
2.3.2 Padrão IEEE 1609.0: Arquitetura WAVE 27
2.3.3 Padrão IEEE 1609.1: Gerenciador de Recursos 27
2.3.4 Padrão IEEE 1609.2: Serviços de Segurança para Aplicações e Gerenciamento de Mensagens 29
2.3.5 Padrão IEEE 1609.3: Serviços de Rede 31
2.3.6 Padrão IEEE 1609.4: Operação em Múltiplos Canais 33
2.3.7 Padrão IEEE 1609.11: Transferência de Dados de Pagamento 35
2.3.8 Padrão IEEE 1609.12: Alocação de Identificadores ... 36
2.4 O protocolo de roteamento BATMAN 36
2.5 On-Board Diagnostic 2 (OBD 2) 37
2.6 Dispositivos móveis e suas ferramentas 40
2.7 Modelos de localização geográfica 41
2.7.1 Global Positioning System (GPS) 41
2.7.2 Assisted GPS (AGPS) 42
2.8 Detecção de acidentes de trânsito 42
2.9 Disseminação de alertas na VANET 45
3 TRABALHOS RELACIONADOS 48
4 SISTEMA DE DETECÇÃO E ALERTA DE ACIDENTES 51
4.1 Primeiro ambiente: o veículo 53
4.2 Segundo ambiente: as vias de trânsito 54
4.3 Terceiro ambiente: internet 55
4.4 A aplicação de detecção automática e alerta de acidentes 56
4.4.1 A detecção de acidentes 57

4.5 A disseminação de informações 63
4.6 Experimentos 65
4.6.1 Primeiro experimento: retransmissão do alerta para uma RSU 66
4.6.2 Segundo experimento: retransmissão do alerta para um veículo em movimento 67
4.6.3 Terceiro experimento: validação da disseminação de alertas 68
4.7 Métricas avaliadas 69
5 RESULTADOS E DISCUSSÕES 70
5.1 Primeiro experimento: retransmissão para RSU 70
5.2 Segundo experimento: retransmissão entre veículos .. 73
5.3 Terceiro experimento: validação da disseminação de alertas 76
6 CONCLUSÕES E TRABALHOS FUTUROS 80
REFERÊNCIAS 82

1 INTRODUÇÃO

Em 2010, cerca de 1,24 milhão de pessoas morreram vítimas de acidentes de trânsito no mundo (WORLD HEALTH ORGANIZATION - WHO, 2013). No Brasil, só nas rodovias federais, aconteceram mais de 180 mil acidentes no ano de 2010, segundo o Departamento Nacional de Infraestrutura de Transporte - DNIT (2010). Para ajudar a reduzir esse número de acidentes foram desenvolvidas as redes veiculares *ad hoc* (VANETs). Os principais objetivos das VANETs são segurança no trânsito e transporte eficiente (HARTENSTEIN; LABERTEAUX, 2008). Utilizando essas redes é possível coletar e disseminar informações para detecção automática e alerta de acidentes de trânsito, que podem reduzir o número de fatalidades.

As VANETs são caracterizadas por serem redes de comunicação entre veículos ou entre veículos e dispositivos de infraestrutura instalados nas vias de trânsito. Nessas redes, são trocadas mensagens sobre as condições do tráfego de veículos, segurança do trânsito, comunicação de acidentes e/ou mensagens de propósito geral (HARTENSTEIN; LABERTEAUX, 2008). Por transmitirem informações consideradas críticas e terem características próprias (diferentes trajetórias dos veículos e alta velocidade por exemplo), um padrão de comunicação foi elaborado para as VANETs, o IEEE 802.11p.

O desenvolvimento do padrão IEEE 802.11p *Wireless Access in Vehicular Enviroment* (WAVE) foi iniciado pelo *Institute of Electrical and Electronics Engineers* (IEEE) em 2004. Em 2012 este padrão foi incorporado ao padrão IEEE 802.11. Além deste padrão de comunicação, outros padrões foram criados para as VANETs. O padrão IEEE 1609 é dividido em seis documentos que tratam da segurança na transferência de informações, dos serviços de rede, do roteamento de canais de comunicação, da organização

dos padrões ISO e do gerenciamento de identificadores das VANETs. Os padrões IEEE 802.11 e IEEE 1609 formam a Arquitetura WAVE, que é definida de acordo com documentos criados pelo grupo de trabalho IEEE 1609 (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS - IEEE, 2015).

O padrão IEEE 802.11p exige *hardwares* específicos devido às adaptações necessárias para as VANETs. Esses *hardwares* ainda não se popularizaram devido ao seu alto custo (VANDENBERGHE; MOERMAN; DEMEESTER, 2011). Uma alternativa pode ser a utilização de dispositivos de arquitetura aberta, próprios para comunicação sem fio como as *Routerboards* (MIKROTIK, 2015). Elas possuem várias interfaces que permitem a utilização de várias tecnologias e a variação de padrões de comunicação sem fio. São exemplos de tecnologias de comunicação: 3G/4G, Wi-Fi, Ethernet, USB (*Universal Serial Bus*), Serial e as variações dos padrões IEEE 802.11 a/b/g. *Routerboards* com o padrão IEEE 802.11a podem ser modificadas de forma a ter um comportamento semelhante ao padrão de redes veiculares (BARCELOS et al., 2014a, 2014b). As *Routerboards* podem se comunicar com os dispositivos móveis, transmitindo as informações pela rede veicular utilizando o padrão IEEE 802.11p.

Para detectar acidentes automaticamente e emitir alertas, são necessárias informações sobre o estado do *airbag* e a velocidade do veículo, além das coordenadas geográficas para indicar a posição do veículo acidentado. Os dispositivos móveis possuem capacidade de comunicação utilizando *wireless* e *bluetooth*, alto poder de processamento e ferramentas como GPS (*Global Positioning System*) e acelerômetro que podem ser utilizadas como fonte de informação para as VANETs (ZHAO, 2000). Para conseguir infor-

mações como a velocidade do veículo e o estado de seu *airbag* é utilizado o sistema OBD 2 (*On-Board Diagnostic 2*).

O OBD 2 é um sistema que pode ser encontrado em carros fabricados a partir do ano de 1994 e consiste em um conjunto de sensores que trazem várias informações sobre o veículo. O dispositivo móvel pode ler essas informações de um **scanner** OBD 2 por meio de conectividade *Bluetooth*, Wi-Fi ou USB.

As informações extraídas dos veículos podem trafegar pelas VANETs até unidades com acesso à internet. Assim essas informações podem ser tratadas por servidores *web* e disponibilizadas para autoridades, familiares do motorista e seguradoras de veículos.

Devido ao caráter de emergência, as aplicações de segurança de trânsito exigem baixa latência nas comunicações e um alcance mínimo para que apresentem efetividade (IBANEZ et al., 2011). Em aplicações de detecção automática de acidentes, um alerta deve ser emitido o mais rápido possível, considerando um raio de alcance que permita que motoristas próximos do acidente sejam avisados a tempo de tomar medidas de precaução. Além disso, Ibanez et al. (2011) apresentam como valores ideais para este caso uma latência de 100 ms a um raio de 150 metros do acidente.

Existem vários estudos voltados para detecção e alertas de acidentes de trânsito. Fire et al. (2012), Thompson et al. (2010) e Zaldivar et al. (2011) criaram aplicativos para dispositivos móveis que detectam acidentes e emitem alertas utilizando mensagens de celular ou a rede 3G/4G. Na indústria são encontradas tecnologias semelhantes, como o dispositivo Sync (FORD, 2015) desenvolvido pela Ford. Entretanto, nenhum destes trabalhos utiliza VANET como meio de transmissão para emitir alertas de acidente.

Nesta dissertação foi desenvolvida uma aplicação que detecta acidentes de trânsito automaticamente e transmite alertas por uma VANET em tempo real. Os alertas são enviados para veículos próximos ao acidente e para dispositivos instalados nas vias de trânsito que podem retransmiti-los a servidores *web*.

1.1 Motivação e definição do problema

Não foi encontrada na literatura atual uma solução que faça a detecção automática de acidentes e emita alertas para veículos e/ou para uma central de monitoramento usando VANET no padrão IEEE 802.11p.

Uma aplicação com estas características permite que motoristas de veículos que trafegam próximos ao acidente tenham, antecipadamente, a informação do acidente e, consequentemente, tenham mais tempo para reagir a ele que teriam se não recebessem o alerta. Além disso, equipes de socorro podem receber a informação do acidente automaticamente, o que pode diminuir o tempo de socorro e aumentar as chances de uma vítima sobreviver.

O problema abordado é a melhoria da eficiência do socorro e da sinalização de acidentes de trânsito por meio da automatização do processo de detecção e alerta desses acidentes.

1.2 Objetivo

Este trabalho teve como objetivo criar uma aplicação de detecção e alerta automáticos de acidente, considerando os requisitos de qualidade de serviço para aplicações de segurança de trânsito. São desenvolvidos algoritmos de detecção de acidentes e de disseminação de alertas na VANET.

1.2.1 Objetivos específicos

Para o desenvolvimento da aplicação de detecção e alerta de acidentes de trânsito foram estabelecidos os seguintes objetivos específicos:

- avaliar quais informações são importantes para detectar acidentes de trânsito e emitir alertas;
- analisar e criar algoritmos que permitam a detecção de acidentes de trânsito;
- analisar e criar algoritmos que permitam a disseminação de alertas de acidentes em uma VANET;
- desenvolver e avaliar uma aplicação que detecte automaticamente um acidente e emita alertas pela VANET considerando os requisitos de qualidade de serviço para aplicações de segurança de trânsito em redes veiculares;
- realizar experimentos práticos, verificando se o sistema atende aos requisitos de qualidade de serviço, identificando características que possam ser melhoradas.

1.3 Estrutura do trabalho

Na seção 2 são mostrados os conceitos fundamentais para o entendimento do trabalho. Na seção 3 são apresentados trabalhos relacionados a esta pesquisa. A metodologia de desenvolvimento e os materiais necessários para a pesquisa são descritos na seção 4. Na seção 5 são mostrados os resultados. Por fim, na seção 6, são apresentadas as conclusões e os trabalhos futuros.

2 REFERENCIAL TEÓRICO

Nesta seção são apresentados os principais conceitos e padrões relacionados com aplicações de segurança de trânsito, além das ferramentas utilizadas no desenvolvimento da aplicação de detecção automática e alerta de acidentes.

2.1 Redes *ad hoc*

Uma rede *ad hoc* é uma rede de dispositivos que utiliza tecnologia sem fio criando uma rede sem administração (ZAFOUNE; KANAWATI; MOKHTARI, 2007). É uma rede onde todos os dispositivos podem se comunicar diretamente sem precisar de uma infraestrutura que gerencie a comunicação entre eles, como um roteador por exemplo.

Essas redes trazem características de mobilidade já que não precisam estar perto de uma infraestrutura para funcionar. As informações podem passar por vários dispositivos intermediários antes de chegarem ao seu destino, permitindo a comunicação de dispositivos distantes se existir uma rota entre eles.

2.2 Redes Veiculares Ad Hoc (VANET)

VANET é a tecnologia *wireless* que permite construir redes *ad hoc* entre veículos ou entre veículos e infraestruturas (HARTENSTEIN; LABERTEAUX, 2010). O padrão IEEE 1609.1 (IEEE, 2006) define dois tipos de dispositivos que fazem acesso a redes sem fio em redes veiculares: a RSU (*roadside unit*) ou dispositivo de infraestrutura e a OBU (*onboard unit*) ou dispositivo do veículo. O primeiro é fixo e é instalado ao longo das vias e o

segundo é móvel e é instalado dentro dos veículos.

As comunicações em VANETs são separadas em três categorias dependendo dos tipos de dispositivos envolvidos: comunicações entre veículos (*vehicle to vehicle* - V2V), comunicações entre veículos e infraestrutura (*vehicle to infrastructure* - V2I) e comunicações híbridas (V2X), que utilizam as outras duas categorias de comunicação. A Figura 1 ilustra essas categorias.

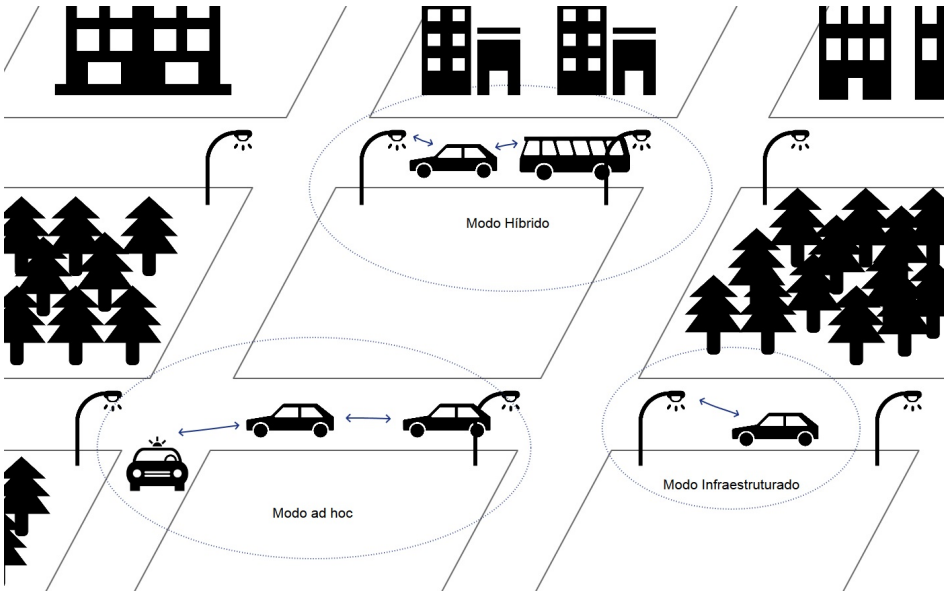


Figura 1 Comunicações V2V, V2I E V2X.

As aplicações de redes veiculares são classificadas em três categorias dependendo de seu propósito (HARTENSTEIN; LABERTEAUX, 2008):

- **Segurança de trânsito**: são aplicações que alertam motoristas sobre acidentes ou outros eventos cruciais para a segurança do veículo. Mensagens de aplicações deste tipo têm prioridade sobre mensagens dos demais tipos.

- **Eficiência de transporte**: são aplicações que otimizam o deslocamento do veículo utilizando informações sobre engarrafamentos ou outras informações do trânsito.

- **Informação/entretenimento**: são aplicações gerais, como acesso à internet e aplicações oportunistas.

Hartenstein e Laberteaux (2008) apresentam os principais desafios das VANETs, separando-os em desafios sócio-econômicos e técnicos.

Como desafio sócio-econômico, é apresentado o efeito de rede: o valor agregado pela VANET para um consumidor depende do número total de consumidores que possuem os equipamentos de redes veiculares instalados em seus veículos. O desafio nesse caso é como fazer com que os primeiros consumidores comprem os equipamentos de VANETs. Há sugestões como criar leis que obriguem que os veículos tenham estes equipamentos ou instalar as infraestruturas nas estradas, de forma a atrair a instalação dos equipamentos nos veículos.

Entre os desafios técnicos estão: coordenar a comunicação entre os dispositivos; tratar a topologia dinâmica baseada na mobilidade dos veículos e seu impacto na propagação de sinal; trabalhar em uma ampla gama de condições, como tráfego de veículos denso ou esparso; e a forte necessidade de potência de transmissão e controle de taxas adaptativas para alcançar um grau razoável de confiabilidade e baixa latência de comunicação (HARTENSTEIN; LABERTEAUX, 2008).

A Tabela 1 apresenta a latência para prover qualidade de serviço para diferentes aplicações em VANETs (IBANEZ et al., 2011).

Para especificar uma forma de atacar estes desafios e permitir que empresas pudessem produzir equipamentos compatíveis para redes veicula-

Tabela 1 Requisitos de qualidade de serviço para aplicações de segurança de trânsito.

Aplicações	Latência Máxima	Alcance
Violação de semáforo	100 ms	250 m
Aviso de excesso de velocidade antes de realizar uma curva	1000 ms	200 m
Luzes de freio de emergência	100 ms	200 m
Colisão à frente	100 ms	150 m
Aviso de mudança de faixa	100 ms	150 m

res, foi iniciada uma padronização das VANETs. Em 1996 o Departamento de Transportes dos Estados Unidos, a Sociedade Americana de Transporte Inteligente e outras partes interessadas desenvolveram o serviço *Intelligent Vehicle Highway Systems* (IVHS), um *framework* processual que foi o plano mestre para a iniciativa ITS (*Intelligent Transportation System*) (UZCATEGUI; ACOSTA-MARUM, 2009).

A iniciativa ITS implementou alguns serviços na faixa de frequência de 902 Mhz a 928 MHz. Esta faixa foi considerada pequena e muito poluída para os serviços de redes veiculares (UZCATEGUI; ACOSTA-MARUM, 2009). Em 1999 a *Federal Comunications Commission* (FCC), nos Estados Unidos, alocou uma faixa de 75 MHz no espectro de frequência de 5,85 a 5,925 GHz exclusivamente para comunicações veiculares (ALVES et al., 2009). Esta faixa foi denominada *Dedicated Short-Range Communications* (DSRC).

Em 2002 foi recomendada a adoção de um padrão único para as camadas física (PHY) e de controle de acesso ao meio (MAC) para as redes veiculares. Em 2004 um grupo de trabalho da IEEE começou a desenvolver uma emenda ao padrão IEEE 802.11, o IEEE 802.11p. Paralelamente, um outro grupo de trabalho da IEEE desenvolveu padrões para as outras

camadas de rede, o IEEE 1609. Inicialmente, o IEEE 1609 foi dividido em quatro documentos, IEEE 1609.1, IEEE 1609.2, IEEE 1609.3 e IEEE 1609.4 (UZCATEGUI; ACOSTA-MARUM, 2009). Posteriormente, o padrão IEEE 802.11p foi incorporado ao IEEE 802.11, o padrão IEEE 1609.1 foi considerado desnecessário tornando-se um padrão rascunho e foram adicionados mais documentos: IEEE 1609.0, IEEE 1609.5, IEEE 1609.6, IEEE 1609.11 e IEEE1609.12 (IEEE, 2014). Os padrões IEEE 802.11p e IEEE 1609.x são conhecidos como arquitetura WAVE (*Wireless Access in Vehicular Environments*).

2.3 Arquitetura WAVE

A arquitetura WAVE é composta por dez documentos que têm o objetivo de facilitar o acesso a *wireless* em aplicações veiculares. A arquitetura WAVE não define as camadas de sessão, apresentação e aplicação que são definidas no modelo de referência OSI (*Open Systems Interconnection*) utilizado em redes tradicionais. Porém, são definidos o gerenciador de recursos (IEEE 1609.1) e os blocos de serviços seguros (IEEE 1609.2) (UZCATEGUI; ACOSTA-MARUM, 2009). A Figura 2 apresenta a pilha de protocolos da arquitetura WAVE. A Tabela 2 resume os padrões e seus propósitos.

Os padrões IEEE 1609.5 e IEEE 1609.6, até o momento, ainda não foram publicados. A seguir são apresentados os detalhes dos outros documentos da Arquitetura WAVE. Este trabalho se baseou principalmente nos padrões IEEE 802.11p e IEEE 1609.1.

Tabela 2 Lista de padrões que fazem parte da arquitetura WAVE (AHMED et al., 2013; IEEE, 2014; UZCATEGUI; ACOSTA-MARUM, 2009).

Protocolo	Documento do Padrão	Propósito do padrão	Número da Camada no Modelo OSI
PHY e MAC da WAVE	IEEE 802.11p	Especifica as funções requeridas para as camadas PHY e MAC para um dispositivo IEEE 802.11 trabalhar com a rápida variação de aplicações veiculares	1 e 2
Arquitetura	IEEE 1609.0	Apresenta uma visão geral da arquitetura , WAVE seus componentes e sua operação	Nenhum
Gerenciamento de recursos	IEEE 1601.1	Descreve uma aplicação que permite uma interação com o OBU	Nenhum
Serviços de segurança	IEEE 1609.2	Formato de mensagens seguras e seu processamento	Nenhum
Serviços de rede	IEEE 1609.3	Serviços de endereçamento e roteamento em sistemas WAVE	2, 3 e 4
Operação Multicanal	IEEE 1601.4	Provê melhorias na camada MAC do IEEE 802.11p para que ele suporte operações multicanal	2
Gerenciamento de comunicação	IEEE 1609.5	Define os serviços de gerenciamento de comunicação para conexão *wireless* entre OBUs e entre OBUs e RSUs	Nenhum
Serviços de gerenciamento de dados	IEEE 1609.6	Em desenvolvimento, inclui um gerenciamento de transmissão *wirelless* e recursos de álias	
Troca de dados de pagamento via IEEE 802.11	IEEE 1609.11	Define um nível básico de interoperabilidade técnica para um equipamento de pagamento eletrônico via WAVE	Nenhum
Atribuição de identificadores	IEEE 1609.12	Especifica a atribuição de identificadores WAVE	Nenhum

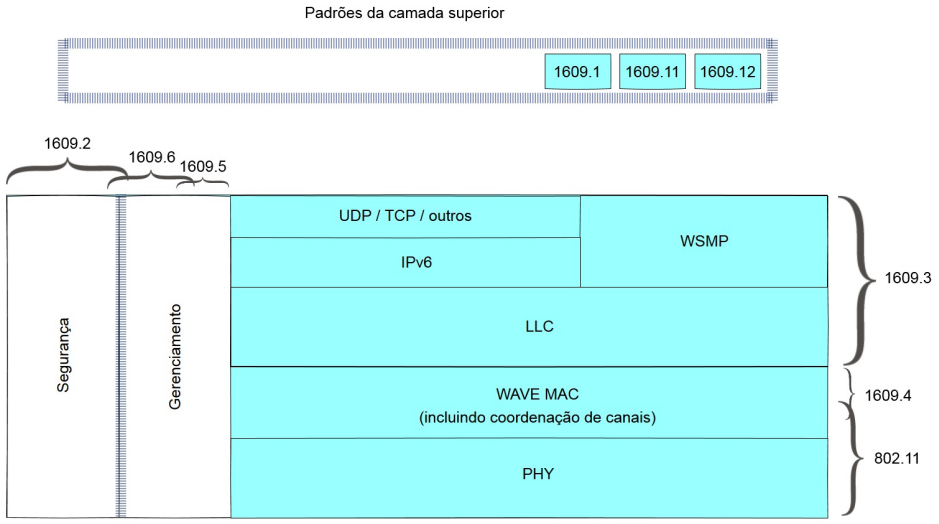


Figura 2 A pilha de protocolos da arquitetura WAVE.

2.3.1 Padrão IEEE 802.11p: Camadas Física e de Controle de Acesso ao Meio

O padrão IEEE 802.11p (IEEE, 2010a) foi criado para ser utilizado em aplicações com um tempo de comunicação muito curto e com grande mobilidade. Esse padrão pode ser considerado uma extensão da família de protocolos IEEE 802.11, baseando-se principalmente no padrão IEEE 802.11a, porém opera na faixa DSRC de 5.9 GHz (ALVES et al., 2009).

O padrão define uma camada física com multiplexação por divisão de frequência ortogonal (*orthogonal frequency-division multiplexing* - OFDM), usa sete canais de 10 MHz, sendo um canal de controle e o restante de serviços. As taxas de dados variam de 3 a 27 MB/s para cada canal, onde as taxas mais baixas são muitas vezes preferidas, a fim de obter uma comunicação robusta (HARTENSTEIN; LABERTEAUX, 2008). A Figura 3 apresenta a alocação de espectro para aplicações DSRC. A camada de con-

trole de acesso ao meio (*medium access control* - MAC) é baseada no padrão IEEE 802.11e.

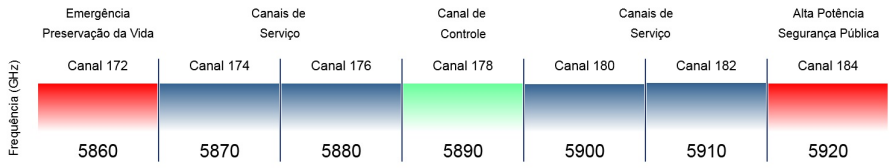


Figura 3 Alocação de espectro para aplicações DSRC.

2.3.2 Padrão IEEE 1609.0: Arquitetura WAVE

O Padrão IEEE 1609.0 (IEEE, 2014) é um documento introdutório que apresenta uma visão geral sobre a Arquitetura WAVE, seus componentes e sua operação. Nele é apresentado um pequeno histórico do desenvolvimento dos padrões WAVE, citando as principais entidades envolvidas e introduzindo os outros padrões da arquitetura, que são descritos individualmente neste documento.

2.3.3 Padrão IEEE 1609.1: Gerenciador de Recursos

O padrão IEEE 1609.1 especifica o acesso à internet sem fio em aplicações em ambientes veiculares. Este padrão foi concebido para permitir que aplicações remotas, como por exemplo aplicações que executam em servidores, chamadas de RMA (*Resource Manager Applications*), se comuniquem com aplicações que executam em OBUs que estão montados em veículos, as aplicações RCP (*Resource Command Processor*). Essas aplicações se comunicam por meio de uma aplicação WAVE a ser instalada no RSU que

realiza a multiplexação das requisições das RMAs, provendo o acesso às OBUs. Essa aplicação WAVE que executa no RSU é chamada de *resource manager* (RM) (IEEE, 2006).

A Figura 4 apresenta um diagrama com os elementos que compõem uma rede veicular. Os elementos tratados pelo padrão IEEE 1609.1 são: a comunicação entre um RMA e um RM; o tratamento feito pelo RM à requisição; a comunicação entre o RM e o RCP; e o tratamento da requisição feito pelo RCP. Estes elementos são apresentados em negrito na Figura.

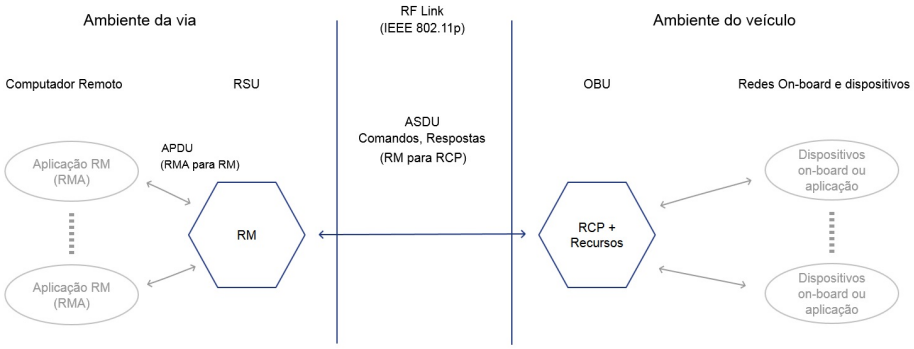


Figura 4 Componentes tratados pelo padrão IEEE (2006).

O propósito deste padrão é permitir a interoperabilidade de aplicações WAVE de forma que os sistemas integrados nos veículos sejam mais simples, promovendo redução de custos e uma melhora de performance (IEEE, 2006). Este padrão especifica:

- os serviços prestados pelas RMs para as RMAs;
- como os serviços prestados pelo padrão IEEE 1609.3 são usados para anunciar a presença do RM e das RMAs para a OBU;
- como o RCP reconhece e responde à presença do RM e cada uma das

suas RMAs associados para completar um processo ou uma transação de aplicação;

- o gerenciamento de recursos de memória dos OBUs e como essas memórias são usadas para armazenar e recuperar informações e controlar as interfaces das OBUs com usuários e outros equipamentos;
- o conjunto de comandos disponíveis para as RMAs gerenciarem esses recursos, como esses comandos e suas respostas são trocados entre RMAs, RMs e RCPs por uma frequência de rádio WAVE segura;
- o uso de recursos especializados de leitura e escrita de memória que permitem a transferência de dados para outros aparelhos com interface para a OBU e controlados pelo RCP.

2.3.4 Padrão IEEE 1609.2: Serviços de Segurança para Aplicações e Gerenciamento de Mensagens

Este padrão foi criado para desenvolver as técnicas de segurança que serão utilizadas para proteger os serviços que utilizam redes veiculares. Muitas aplicações em redes veiculares, especialmente as aplicações de segurança, são críticas em relação a tempo. Por isso, o processamento e a sobrecarga na largura de banda gastos com segurança devem ser os menores possíveis. O número de dispositivos pode variar muito, dependendo da densidade de veículos, por isso o mecanismo utilizado para autenticar mensagens deve ser o mais flexível e escalável possível (IEEE, 2013).

Este padrão especifica mecanismos que permitem gerenciar a autenticação de mensagens WAVE, autenticar mensagens que não requerem anonimato e criptografar mensagens para um destino conhecido (IEEE, 2013).

Segundo Uzcategui e Acosta-Marum (2009), para promover confidencialidade, autenticidade e integridade às redes veiculares, este padrão pode utilizar os seguintes mecanismos:

- **Algoritmos Simétricos**: Quando dois dispositivos querem se comunicar, eles utilizam uma chave secreta. A chave é utilizada para criptografar e descriptografar a mensagem. Para promover autenticidade e integridade, a chave pode ser utilizada para gerar um valor de checagem ou *message integrity check* (MIC).

- **Algoritmos Assimétricos**: É utilizado um par de chaves, a chave pública e a chave privada, que são matematicamente relacionadas. A chave pública é utilizada para criptografar e a privada para descriptografar. Se algum dispositivo quer se comunicar com o dispositivo A, deve criptografar a mensagem com a chave pública de A. Apenas A tem a chave privada que pode decodificar a mensagem. Esses algoritmos permitem o uso de assinaturas digitais.

- **Funções Hash**: mapeia uma entrada de tamanho arbitrário em uma saída de tamanho fixo (o valor hash). É computacionalmente impossível encontrar a entrada que mapeia um valor hash específico ou duas entradas que mapeadas geram o mesmo valor hash. Este padrão utiliza a função *Secure Hash Algorithm* (SHA-1).

- **Anonimato**: transmissões em *broadcast* não devem conter informações que possam ser usadas para que destinatários não autorizados identifiquem o veículo que as enviou, nestes casos não é feita a autenticação dos dados enviados.

2.3.5 Padrão IEEE 1609.3: Serviços de Rede

Este padrão especifica os serviços das camadas de controle de enlace lógico (*Logical Link Control* - LLC), de rede e de transporte do modelo OSI para WAVE (ALVES et al., 2009). O propósito deste padrão é prover endereçamento e serviços de entrega de dados em sistemas WAVE. Consiste em camadas de plano de dados e de plano de gerenciamento, como mostra a Figura 5 (IEEE, 2010b).

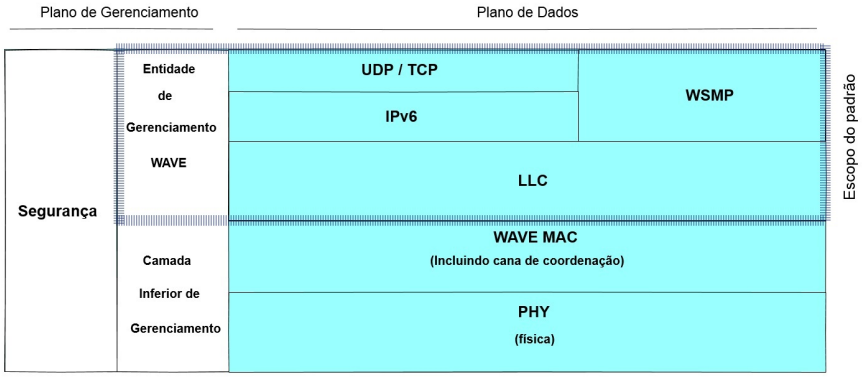


Figura 5 Escopo do padrão IEEE 1609.3 (IEEE, 2010b).

No plano de dados, a arquitetura WAVE suporta duas pilhas de protocolos: protocolo de internet versão 6 (IPv6) e protocolo de mensagem curta WAVE (*WAVE Short Message Protocol* - WSMP) (UZCATEGUI; ACOSTA-MARUM, 2009). Os componentes do plano de dados para serviços de redes WAVE apresentados no padrão IEEE 1609.3 (IEEE, 2010b) são:

- **Controle de enlace lógico**: Serviço de rede que inclui a subcamada LLC para tráfego IP e tráfego WSMP.
- **IPv6 e camadas superiores como *Transmission Control Protocol* (TCP) e *User Datagram Protocol* (UDP)**: Serviço de rede

que recebe os dados de camadas superiores para transmiti-los utilizando IPv6 e que entrega dados IPv6 recebidos para as camadas superiores.

- **WSMP**: Serviço de rede que recebe dados de camadas superiores para a transmissão através de WSMP e que entrega os dados WSM (*WAVE Short Message*) recebidos às camadas superiores.

Já no plano de gerenciamento temos a *WAVE Management Entity* (WME) que realiza as seguintes funções:

- **Requisição de serviços e atribuição de acesso de canal**: responde às requisições das camadas superiores; oferece acesso ao canal de serviço para responder às requisições de serviço; e faz anúncios de serviços WAVE, anúncio de tempo e gerenciamento geral dos dados a serem transmitidos.

- **Gerenciamento de entrega de dados**: gerencia o aceite de dados recebidos das camadas inferiores, os processa ou os passa para a entidade de gerenciamento designada.

- **Monitoramento dos anúncios de serviços WAVE**: a WME monitora e verifica serviços anunciados por outros dispositivos WAVE para uso por camadas superiores e funções de gerenciamento.

- **Configurações IPv6**: configura a pilha de protocolos IP local usando os dados recebidos de outros dispositivos WAVE.

- **Manutenção da base de informações de gerenciamento (*management information base* - MIB)**: mantém uma MIB que contém configurações e informações de estado.

2.3.6 Padrão IEEE 1609.4: Operação em Múltiplos Canais

Este padrão provê serviços que gerenciam a coordenação de canais e suportam entregas da unidade de dados de serviços MAC (*MAC service data unit* (MSDU)) (IEEE, 2011a). Um dispositivo WAVE deve monitorar um canal de controle (CCH) esperando por anúncios de serviços WAVE (WSA) que contém o número do canal de dados a ser utilizado para um determinado serviço. O dispositivo provedor do serviço escolhe o SCH de acordo com o conteúdo dos quadros de anúncios de serviços que serão transmitidos (ALVES et al., 2009).

De acordo com Uzcategui e Acosta-Marum (2009), existem quatro serviços providos por este padrão:

- **Roteamento de canais**: controla o roteamento de pacotes de dados vindos da camada de controle de enlace lógico (*Logical Link Control* (LLC)) para o canal de coordenação de operações na camada MAC que foi designado.

- **Prioridade de usuário**: serviço utilizado para disputar acesso ao meio usando a funcionalidade de acesso ao canal distribuído melhorado (*enhanced distributed channel access - EDCA*).

- **Coordenação de canais**: coordena os intervalos de canais de acordo com as operações de sincronização de canais da camada MAC, fazendo com que os pacotes desta camada sejam transmitidos no seu próprio canal de rádio frequência.

- **Transferência de dados da MSDU**: consiste em outros três serviços, o canal de controle de transferência de dados, o canal de serviço de transferência de dados e o próprio serviços de transferência de dados.

Os dispositivos WAVE monitoram o canal de serviços fazendo escutas durante períodos conhecidos como intervalos CCH (50 ms). Entre os períodos CCH, existem intervalos que são utilizados para transmissões nos SCH, os intervalos SCH (50 ms). A sincronização dos intervalos é feita utilizando uma referência de tempo absoluto (*Coordinated Universal Time* - UTC) (ALVES et al., 2009). A Figura 6 ilustra o padrão, mostrando o caminho dos dados vindos da LLC, passando pelo roteador de canais, pelo CCH ou SCH, pelo seletor de canais até a tentativa de transmissão.

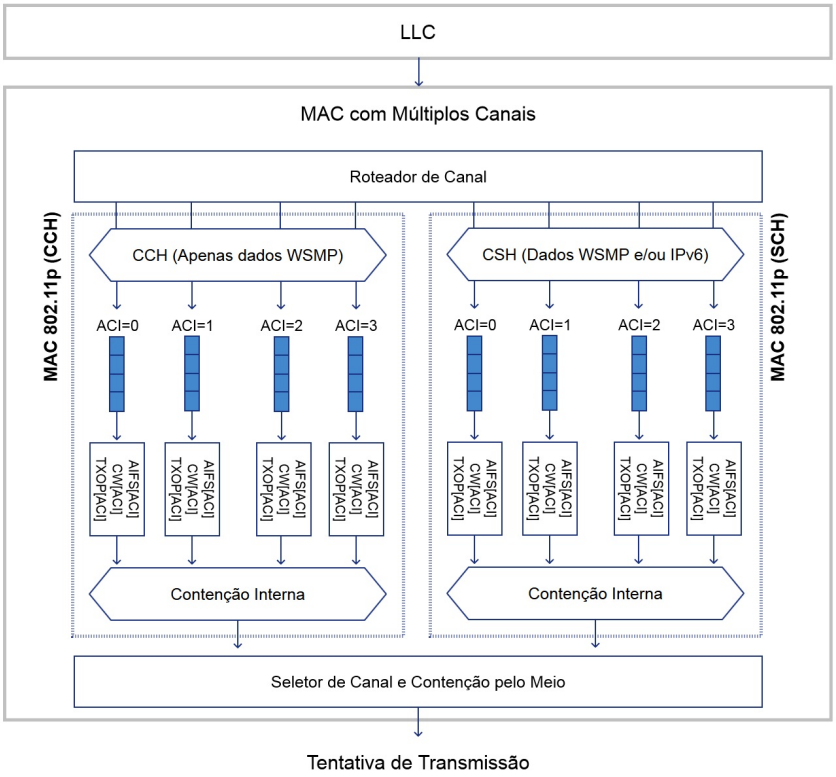


Figura 6 O padrão IEEE 1609.4.

Existem três tipos de informações trocadas no meio WAVE, qua-

dros de gerenciamento, de dados e de controle (IEEE, 2011a). Quadros de controle não são tratados neste padrão pois são usados pelo padrão IEEE 802.11. Quadros de gerenciamento são transmitidos no CCH. O principal quadro de gerenciamento é o quadro de anúncio de serviço WAVE. Quadros de dados são transmitidos nos SCH e podem conter mensagens curtas WAVE ou datagramas IPV6.

2.3.7 Padrão IEEE 1609.11: Transferência de Dados de Pagamento

O padrão IEEE 1609.11 (IEEE, 2011b) especifica a camada de serviços de pagamento eletrônico, perfil para pagamento e autenticação de identidade, além da transferência de dados de pagamento para aplicações baseadas em DSRC (*Dedicated Short-Range Communications*) em VANETs. São especificados neste padrão apenas as comunicações realizadas dentro do ambiente da VANET (entre OBUs e RSUs).

O processamento de um pagamento eletrônico necessita de funções do serviço de pagamento eletrônico (electronic payment service (EPS)). Essas funções incluem: saber qual é a origem do pagamento, realizar a comunicação do pagamento, realizar o processamento do pagamento, o armazenamento e a recuperação da informação do pagamento. O EPS detalha também tarefas de segurança como a encriptação e desencriptação dos dados e a autenticação da informação.

Este padrão poderia ser utilizado, por exemplo, para aplicações de pagamento automático de pedágios.

2.3.8 Padrão IEEE 1609.12: Alocação de Identificadores

O Padrão IEEE 1609.12 (IEEE, 2012) descreve o uso de identificadores nas VANETs, indicando o valor que deve ser alocado para o identificador no uso de sistemas WAVE. Um *Provider Service Identifier* (PSID) é um valor de tamanho variável especificado no Padrão IEEE 1609.3. Cada valor alocado é associado a uma organização que é autorizada a descrever o seu uso.

O PSID possui três funções especificadas. Um provedor de serviços pode oferecer serviços para um PSID. O WSMP entrega suas mensagens para aplicações das camadas mais altas da rede baseando-se no valor do PSID. Um certificado de segurança lista os valores de PSID que estão autorizados a acessar serviços ou mensagens (IEEE, 2012).

2.4 O protocolo de roteamento BATMAN

O BATMAN (*Better Approach To Mobile Ad-hoc Networking*) é um protocolo de roteamento para redes móveis *ad hoc* (MANET). É um aperfeiçoamento do protocolo OLSR (*Optimized Link State Routing*). No BATMAN, há uma descentralização do conhecimento sobre as rotas da rede, ou seja, um nó da rede não possui em sua tabela de rotas uma rota para cada destino na rede, cada nó conhece apenas o melhor vizinho de um salto para cada destino na rede (SANCHEZ-IBORRA; CANO; GARCIA-HARO, 2014).

Neste protocolo, cada nó da rede envia mensagens de anúncio periódicas, chamadas de OriGinator Message (OGM), para informar sua existência aos seus nós vizinhos. Cada OGM possui apenas 52 bytes com as informações de IP do nó de origem, IP do último nó que o transmitiu, um

valor de TTL (*Time to Live*), e um número sequencial (SQ) que é incrementado a cada transmissão de um novo OGM pelo nó de origem (KULLA et al., 2011).

Os nós vizinhos reenviam o OGM recebido em *broadcast*. O OGM é retransmitido até que todos nós da rede o tenham recebido pelo menos uma vez ou até que o pacote seja perdido ou até que o seu valor TTL se expire. O número de mensagens OGM recebidas de um dado nó via cada vizinho é utilizado para estimar a qualidade da rota. O BATMAN conta quantos OGMs de cada nó de origem veio por meio de cada vizinho. A melhor rota para um determinado destino é através do vizinho que enviou mais OGMs do destino. Assim, é construída uma tabela de rotas associando um vizinho a um destino. Usando o SQ, o BATMAN distingue novos OGMs recebidos de suas duplicatas, fazendo com que cada OGM seja contado apenas para o primeiro vizinho do qual ele foi recebido (SANCHEZ-IBORRA; CANO; GARCIA-HARO, 2014).

2.5 On-Board Diagnostic 2 (OBD 2)

O OBD foi criado em 1988 pela *California Air Resources Board* com o objetivo de monitorar a emissão de gases estufa emitidos pelos automóveis. Em 1994 surgiu o OBD 2, um sistema mais complexo e abrangente capaz de detectar centenas de falhas nos veículos (DINIZ et al., 2009).

O OBD 2 é um sistema de sensores que monitora motor, chassi, corpo e acessórios de carros e caminhões leves. Todos os carros fabricados no Estados Unidos a partir de primeiro de janeiro de 1996 possuem este sistema (OBD 2, 2015). No Brasil, a resolução Conama número 354 de 2004 regulamenta uma implantação gradativa do OBD 2 até primeiro de janeiro

de 2011, a partir de quando todos os carros fabricados ou importados têm que possuir o OBD 2 (DINIZ et al., 2009).

Para realizar a leitura de dados do OBD 2 são utilizados *scanners* OBD 2. Enquanto os parâmetros, ou leituras, exigidos pelos regulamentos OBD 2 são uniformes, os fabricantes de automóveis tiveram certa liberdade no protocolo de comunicações que transmitem essas leituras aos *scanners*. Devido a isso, existem cinco diferentes protocolos de comunicação OBD 2 em uso: SAE J1850 PWM, SAE J1850 VPW, ISO 9141-2, ISO 14230 KWP2000 e ISO 15765 CAN (OBD 2, 2015). A Figura 7 mostra o conector onde são encaixados os *scanners* e a Tabela 3 apresenta uma descrição de cada pino mostrando o padrão que o utiliza.

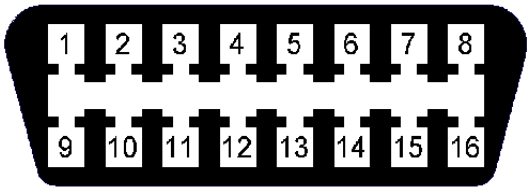


Figura 7 O conector para *scanners* do OBD 2.

Dependendo do protocolo utilizado, o formato do quadro transmitido pelo OBD 2 pode variar. As Figuras 8 e 9 mostram as variações do formato do quadro.

Figura 8 Formato do quadro do OBD 2 para os padrões SAE J1850, ISO 9141-2 e ISO 14230-4.

Os comandos enviados ao OBD 2 são definidos pelo padrão ISO

Tabela 3 Descrição dos pinos do conector para *scanners* OBD 2 (SOCIETY OF AUTOMOTIVE ENGINEERS - SAE, 2001).

Pino	Descrição
1	Varia conforme o fabricante do veículo
2	J-1850 BUS+
3	Varia conforme o fabricante do veículo
4	Dimensões do veículo
5	Fio-terra
6	CAN High (J-2284)
7	ISO 9141-2 K-Line
8	Varia conforme o fabricante do veículo
9	Varia conforme o fabricante do veículo
10	J-1850 BUS-
11	Varia conforme o fabricante do veículo
12	Varia conforme o fabricante do veículo
13	Varia conforme o fabricante do veículo
14	CAN Low (J-2284)
15	ISO 9141-2 L-Line or 2. K-Line
16	+12V (alimentação)

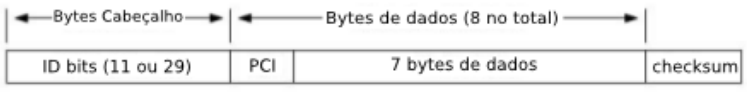


Figura 9 Formato do quadro do OBD 2 para o padrão ISO 15765-4

.

15031-6 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO, 2005).Cada comando representa uma informação que pode ser obtida. Os comandos são números em formato hexadecimal. A Tabela 4 apresenta alguns exemplos de comandos do OBD 2.

Tabela 4 Exemplos de comandos do OBD 2 (ISO, 2005).

Código	Descrição
P0460	Sensor de nível de combustível do circuito A
P0500	Sensor A de velocidade do veículo
P0520	Sensor de pressão do óleo do motor, circuito chaveado
P061C	Módulo de controle interno da performance RPM do motor
B0020	Controle do *airbag* do lado esquerdo
B0028	Controle do *airbag* do lado direito
P0070	Circuito sensor da temperatura ambiente do ar
P0115	Sensor da temperatura de refrigeração do motor, circuito 1

2.6 Dispositivos móveis e suas ferramentas

Os dispositivos móveis são *tablets* e *smartphones*. Eles executam um sistema operacional e possuem um poder de processamento comparável com o de alguns computadores. Com a integração de vários tipos de sensores embarcados e o aumento da capacidade de computação e programação, os *smartphones* tornaram-se uma plataforma viável e sofisticada que vai muito além das funções dos telefones normais. *Smartphones* modernos incluem GPS, câmera, microfone, acelerômetro, sensor de proximidade, sensor de luz ambiente e bússola (FAHMI et al., 2013). Os *smartphones* podem se conectar a outros dispositivos utilizando *wireless*, *bluetooth* e 2G/3G.

Vários sistemas operacionais foram criados para executar em dispositivos móveis. Exemplos desses sistemas operacionais são o iOS da Apple (APPLE, 2015), o Windows Phone da Microsoft (MICROSOFT..., 2015) e o Android do Google (GOOGLE, 2015). Destes apenas o Android não é um

sistema proprietário.

Os recursos dos dispositivos móveis podem ser utilizados por aplicativos, possibilitando a coleta de informações como, por exemplo, localização geográfica utilizando o GPS.

2.7 Modelos de localização geográfica

Em aplicações de VANETs, uma informação importante é a localização geográfica de veículos. Com a localização é possível, por exemplo, detectar aproximações perigosas entre veículos, guiar equipes de socorro de acidentes e permitir um monitoramento de veículos por transportadoras de cargas ou seguradoras de veículos.

Boukerche et al. (2007) apresentam técnicas de localização que podem ser utilizadas em VANETs. Mais detalhes das principais técnicas abordadas são mostrados a seguir.

2.7.1 Global Positioning System (GPS)

Atualmente, o GPS é a ferramenta de posicionamento geográfico mais usual (OTHMAN; AZIZ; ANUAR, 2011). O GPS é um sistema de localização baseado em comunicação com satélites. São utilizados 24 satélites que enviam informações em *broadcast*.

Um receptor GPS recebe as informações e, com elas, pode conhecer a localização de um satélite no momento que a informação foi enviada. Se receber a informação de posição enviada no mesmo instante por três satélites, o receptor pode calcular, com uma triangulação e baseado no tempo de chegada do sinal, sua posição geográfica atual. Para fazer a sincronização do tempo, um quarto satélite envia a data/hora na qual o sinal foi enviado, for-

mando um conjunto de coordenadas geográficas e tempo (KAPLAN, 2005).

Apesar de ser um sistema de localização geográfica muito utilizado, o GPS não é suficiente para aplicações que exigem uma localização muito precisa, pois ele apresenta um erro de localização médio de 10 a 30 metros (KAPLAN, 2005).

2.7.2 Assisted GPS (AGPS)

O AGPS é a técnica de localização utilizada em dispositivos móveis. Esta técnica utiliza a localização por GPS auxiliada, quando disponível, por uma conexão à internet. O AGPS consiste em (1) um dispositivo com conexão *wireless* e um GPS, (2) um servidor AGPS com um receptor GPS de referência que tem visada para os mesmos satélites que o aparelho simultaneamente e (3) uma infra-estrutura de rede sem fios que consiste em estações de base e um centro de comutação móvel (DJUKNIC; RICHTON, 2001). A Figura 10 ilustra a estrutura do AGPS.

O servidor pode predizer com grande precisão as informações que o dispositivo vai receber, diminuindo o tempo gasto para pegar a primeira coordenada de minutos para segundos ou menos. Além disso, o AGPS consegue processar sinais mais fracos que os receptores de GPS e possui uma precisão de 15 metros em locais abertos (DJUKNIC; RICHTON, 2001).

2.8 Detecção de acidentes de trânsito

Algoritmos de detecção de acidentes são utilizadas por fabricantes de veículos para realizar o disparo do *airbag*. Singh e Song (2010) separam esses algoritmos em duas categorias, (1) os que utilizam informações de mudanças de velocidade e (2) os que utilizam informações de sensores colocados em

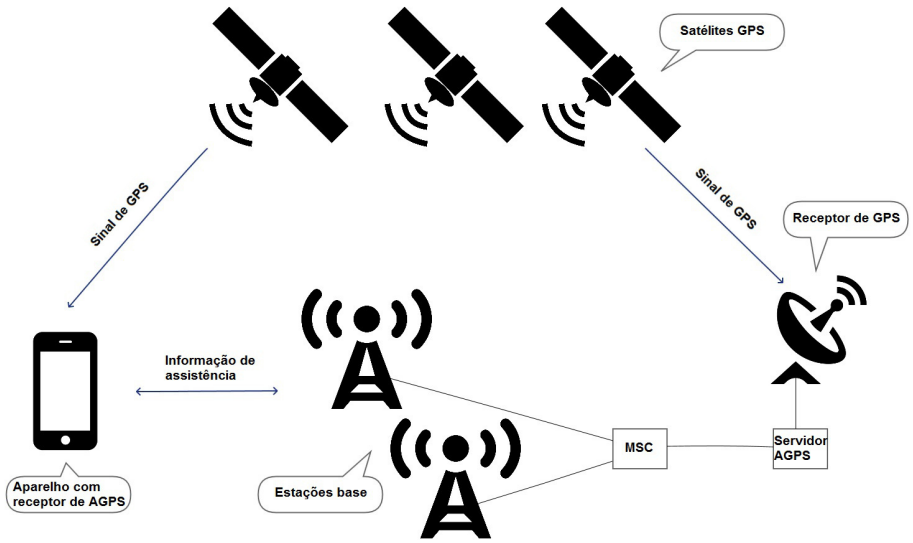


Figura 10 Estrutura utilizada no AGPS.

posições estratégicas dos veículos.

A primeira categoria utiliza o cálculo da aceleração do veículo. Um limiar é definido e qualquer aceleração (ou desaceleração) que ultrapasse esse limiar é considerada um acidente. Em algoritmos da segunda categoria, acelerômetros são colocados no veículo e, da mesma forma que na outra categoria, limiares são definidos. Se os acelerômetros detectarem uma aceleração maior que o limiar definido é considerado um acidente.

Os algoritmos da segunda categoria apresentam a vantagem de poder detectar acelerações em duas ou três dimensões, enquanto sensores de velocidade se baseiam na rotação das rodas dos veículos.

Chan (2002) utilizou acelerômetros para realizar medições de aceleração e variação de velocidade em função do tempo em batidas reais em velocidade de 48 km/h, como é apresentado na Figura 11.

A curva de velocidade mostra que o veículo chega a 0 km/h em 75

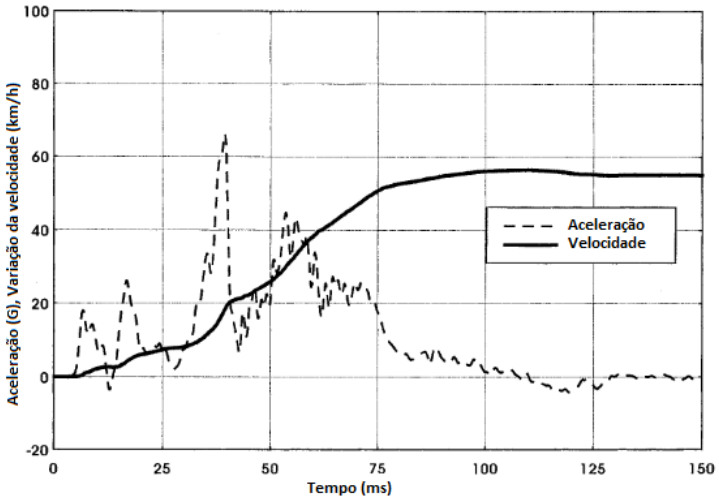


Figura 11 Características da aceleração e velocidade em batida a 48 Km/h (CHAN, 2002).

ms e depois tem uma pequena velocidade negativa. Já a aceleração tem um valor máximo de 60 G e diminui para 0 G em aproximadamente 100 ms.

Singh e Song (2009) apresentam dados de aceleração de veículos para velocidades de 14 e 40 milhas por hora. Na Figura 12 são mostrados os valores da aceleração em G antes e após passar por um filtro analógico-digital SAE J211 e a variação da velocidade do veículo, todos em função do tempo após a batida.

As batidas em velocidades de 12 a 25 milhas por hora não necessitam do disparo do *airbag* e são utilizadas para a definição do limiar de aceleração utilizado pelos algoritmos de detecção de acidentes (SINGH; SONG, 2009).

Os resultados apresentados por Singh e Song (2009) apresentaram tempo de redução da velocidade para 0 mi/h em aproximadamente 100 ms, e pico de aceleração de aproximadamente 11 G a 14 mi/h e aproximadamente 55 G a 40 mi/h, ambos após passarem pelo filtro e, assim como nos

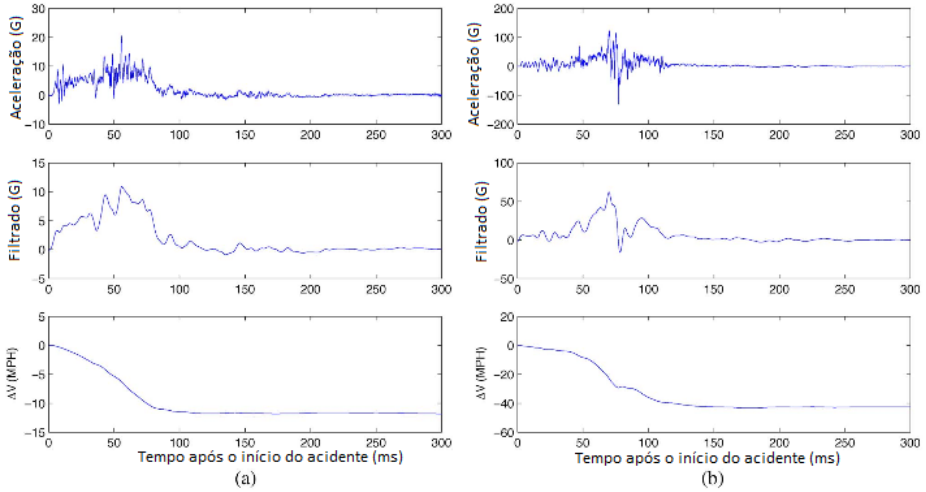


Figura 12 Características da aceleração e velocidade em batidas. (a) 14 mi/h. (b) 40 mi/h. Note que o módulo da variação da velocidade é igual a velocidade do veículo no momento da batida (SINGH; SONG, 2009).

resultados de Chan (2002), chegaram a 0 em aproximadamente 100 ms.

2.9 Disseminação de alertas na VANET

Para realizar a entrega das mensagens de segurança, é preciso definir a forma como a informação vai ser disseminada pela VANET. Para isso, são utilizadas técnicas empregadas em redes DTNs (*Delay Tolerant Networks*). DTNs são redes que, assim como as VANETs, apresentam conectividade instável, sofrendo constantemente com particionamentos e desconexões (PURI; SINGH, 2013). Por isso, os dispositivos das DTNs armazenam as informações recebidas e utilizam conexões temporárias para encaminhá-las pela rede até que a informação chegue ao seu destino. As informações são removidas da memória do dispositivo quando seu tempo de vida expira ou por razões de gerenciamento de memória (TORNELL et al., 2015).

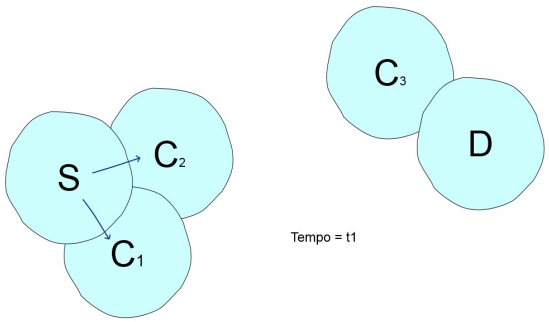
Existem vários protocolos de roteamento para DTNs, como o Epi-

dêmico (VAHDAT; BECKER, 2000), o *Spray and Wait* (SPYROPOULOS; PSOUNIS; RAGHAVENDRA, 2005), o PRoPHET (LINDGREN; DORIA; SCHELÉN, 2003) e o AntRoP (CORREIA et al., 2011). Entre os protocolos de roteamento para DTNs, o Epidêmico é o que consegue entregar a informação ao destino com menor latência. Porém, a rede pode ficar saturada pelo excesso de transmissões de pacotes de controle.

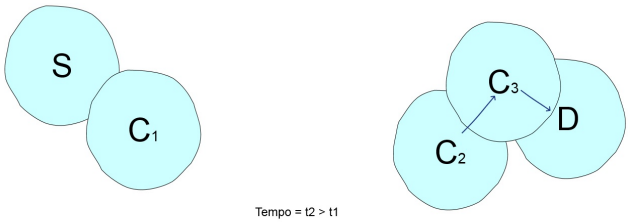
Em uma rede *ad hoc* podemos ter vários grupos de dispositivos conectados entre si. O Protocolo Epidêmico distribui as mensagens de uma aplicação entre os dispositivos de um mesmo grupo. Os dispositivos móveis do grupo podem carregar esta mensagem e se conectar a outros grupos retransmitindo a mensagem. Assim, a mensagem tem uma probabilidade de chegar ao seu destino em eventuais retransmissões (VAHDAT; BECKER, 2000).

A Figura 13 apresenta o funcionamento do Roteamento Epidêmico. Os dispositivos são representados pelas letras e seu alcance de transmissão pelos círculos. Na Figura 13(a), o dispositivo S deseja mandar uma mensagem para o dispositivo D, porém eles não estão conectados. S então transmite a mensagem para os dispositivos C1 e C2, que estão em seu raio de alcance de transmissão. Posteriormente, como é mostrado na Figura 13(b), C2 se move e entra no raio de alcance de C3 e transmite a mensagem para ele. C3 está a alcance de D e, finalmente, transmite a mensagem para ele.

Na aplicação criada neste trabalho, foi desenvolvido um algoritmo baseado no protocolo de roteamento Epidêmico para disseminar alertas na VANET. Para reduzir o número de pacotes de controle na rede, os alertas da aplicação são retransmitidos apenas enquanto o dispositivo estiver próximo



(a) Dispositivo S quer enviar uma informação à D, porém eles não estão conectados, então ele transmite a informação para seus dispositivos vizinhos.



(b) O dispositivo C2 se desloca e transmite a informação para C3 que a transmite para D.

Figura 13 O protocolo de roteamento Epidêmico (VAHDAT; BECKER, 2000).

ao local do acidente.

3 TRABALHOS RELACIONADOS

Vários trabalhos relacionados à detecção e alerta de acidentes têm sido desenvolvidos. Na literatura e no mercado são encontradas algumas aplicações de segurança de trânsito. A fabricante de automóveis Ford incluiu em seu sistema de mídia embarcado, o Sync (FORD, 2015), um serviço automático de chamada de emergência. O serviço é ativado quando detectado o acionamento do *airbag* ou do sistema de corte de combustível e realiza uma ligação para serviços de emergência utilizando um telefone celular previamente pareado ao sistema do veículo. Uma mensagem de voz informa as coordenadas do veículo para o serviço de emergência.

Thompson et al. (2010) criaram um aplicativo de detecção de acidentes baseado no acelerômetro de *smartphone* chamado WreckWatch. Quando detecta um acidente, o *smartphone* utiliza a tecnologia 3G para enviar um alerta para um servidor. O servidor processa a informação e a disponibiliza em uma aplicação *web*.

Thompson et al. (2010) apresentam ainda soluções para evitar a falsa detecção de acidentes, como, por exemplo, verificar se o *smartphone* está conectado ao veículo antes de emitir um alerta, enviar fotos do momento do acidente, tiradas automaticamente pelo *smartphone*, ao servidor e possibilitar que o usuário do aplicativo cancele um alerta de acidente antes que ele seja enviado. Isso é importante para se evitar uma mobilização desnecessária de autoridades e unidades de saúde. Essas soluções exigem que o *smartphone* esteja fixo dentro do carro, senão um falso acidente pode ser detectado.

Zaldivar et al. (2011) trazem uma solução mais confiável para a detecção de acidentes. Eles desenvolveram um aplicativo para *smartphones*

que provê serviços de emergência baseado no monitoramento da velocidade e do disparo do *airbag*. Essas informações são coletadas pelo OBD 2 e lidas pelo aplicativo. Se o *airbag* disparar ou se ocorrer uma desaceleração brusca (maior que 5 G), um acidente é detectado. O motorista tem então um minuto para cancelar a detecção, senão é tomado um procedimento definido pelo usuário como enviar uma mensagem de texto, enviar um email ou fazer uma ligação automática para serviços de emergência.

O aplicativo Waze (FIRE et al., 2012) é capaz de informar motoristas sobre um acidente próximo. Para isso o Waze utiliza informações compartilhadas por seus usuários que, ao passar pelo acidente, indicam o local. Esse aplicativo está sujeito a informações erradas, já que estas são inseridas pelos próprios usuários. Para compartilhar as informações o Waze utiliza redes de dados celulares, como a rede 3G.

A aplicação desenvolvida neste trabalho alerta motoristas próximos sobre o acidente detectado, ao contrário do sistema da Ford e dos trabalhos de Thompson et al. (2010) e Zaldivar et al. (2011), que não se preocupam em prevenir outros motoristas como forma de evitar novos acidentes. Além disso, a aplicação deste trabalho não está sujeita a informações erradas enviadas por usuários como o aplicativo desenvolvido por Fire et al. (2012), já que o acidente é detectado automaticamente. A Tabela 5 apresenta uma comparação entre os trabalhos relacionados e a solução proposta neste trabalho.

Tabela 5 Comparação entre os trabalhos relacionados e a solução proposta neste trabalho.

	Tecnologia de comunicação	**Detecção automática de acidentes?**	**Alerta outros motoristas?**
Ford Sync	Ligação de celular	Sim	Não
WreckWatch	3G	Sim	Não
Zaldivar et al. (2011)	3G	Sim	Não
Waze	3G	Não	Sim
Solução proposta	IEEE 802.11p	Sim	Sim

4 SISTEMA DE DETECÇÃO E ALERTA DE ACIDENTES

Neste trabalho é realizada uma pesquisa experimental que visa utilizar tecnologia para aumentar a segurança e eficiência do trânsito. Para isto, foi necessário integrar vários dispositivos e desenvolver softwares para eles.

Foi desenvolvido um sistema de *hardware* e *software* capaz de detectar automaticamente um acidente e emitir alertas a todos os veículos próximos e/ou para uma central de monitoramento.

O hardware inserido no veículo coleta informações como o estado do *airbag*, velocidade e localização e, em caso de acidente, envia alertas em *broadcast*. Após a disseminação do alerta, os veículos que receberam o alerta devem transportá-lo, por uma determinada distância, até outros veículos e/ou estações fixas.

Para desenvolver esse sistema, um modelo de arquitetura de comunicação foi desenvolvido. Este modelo é mostrado na Tabela 6.

Tabela 6 Modelo de arquitetura de comunicação.

Camada de Aplicação	Sistema Epidêmico
Camada de Transporte	UDP
Camada de Rede	BATMAN e IPv4
Camada de Enlace/Física	IEEE 802.11p

Para a comunicação dos dispositivos, foi utilizada uma *Routerboard* que implementa em sua camadas de enlace/física o padrão IEEE 802.11p (IEEE 802.11a modificado). Este dispositivo e sua configuração são apresentados em Barcelos et al. (2014a).

Ainda na comunicação, na formação da rede *ad hoc* e na descoberta de vizinhos (outros veículos), foi empregado o protocolo de roteamento BAT-

MAN. Esse protocolo foi escolhido com base na comparação realizada por Barcelos et al. (2014a), em que ele se mostrou mais eficiente para o uso em VANETs que outros protocolos comparados. Para manter a compatibilidade e facilidade de acesso aos serviços *web* foi utilizado o modo de endereçamento IPv4 (*Internet Protocol version 4*).

A emissão de alertas desenvolvida na aplicação foi baseada em um algoritmo epidêmico que dissemina alertas a todos os veículos dentro do raio de alcance de comunicação. O protocolo de transporte utilizado pela aplicação foi o UDP (*User Datagram Protocol*). O UDP é utilizado por não precisar de confirmação de recebimento da informação que é disseminada na rede.

O sistema implementado atua em três ambientes: veículo, vias de trânsito e internet. A Figura 14 ilustra a estrutura do sistema que será detalhado a seguir.

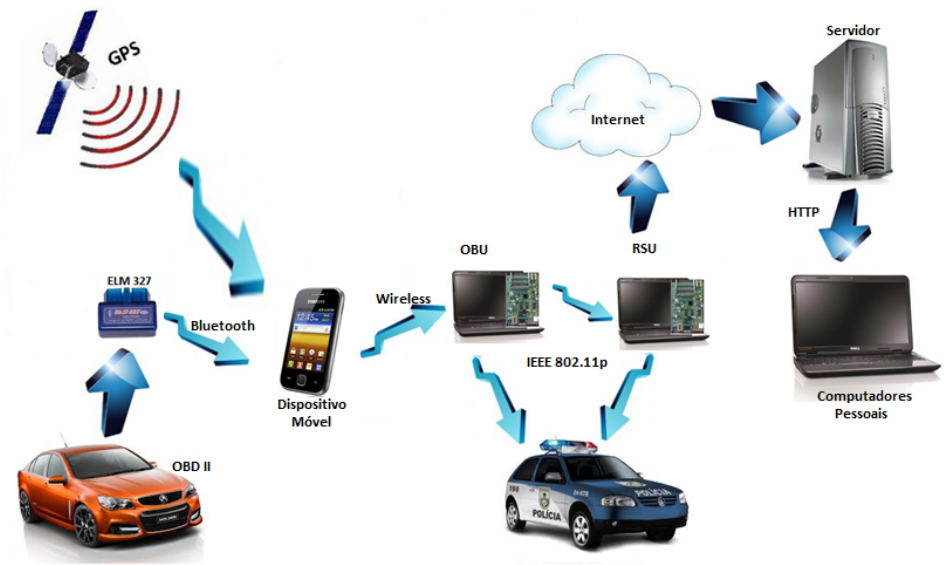


Figura 14 Estrutura do sistema.

4.1 Primeiro ambiente: o veículo

Os dispositivos deste ambiente estão destacados na Figura 15.

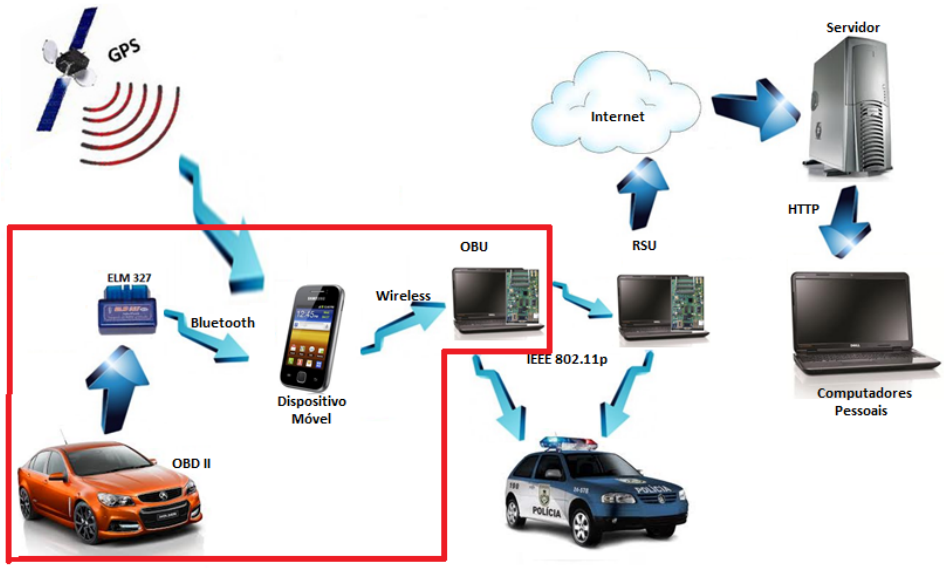


Figura 15 Primeiro ambiente: o veículo.

O veículo possui sensores e uma central de processamento de informações que disponibilizam um diagnóstico sobre o veículo, o OBD 2. O veículo possui uma interface de comunicação na qual é inserido um dispositivo conhecido como ELM 327. Esse dispositivo permite a comunicação do veículo com um dispositivo móvel usando tecnologia *bluetooth*, *wireless* ou USB. No caso foi utilizado um *smartphone* conectado via *bluetooth*.

O dispositivo móvel centraliza várias funções dentro do sistema. Além de requisitar informações ao OBD 2, ele troca informações com um OBU utilizando uma interface *wireless*. O dispositivo móvel também fornece informações como a localização do veículo que é coletada pelo seu GPS.

Para coletar os dados necessários e controlar a comunicação é utili-

zado o aplicativo Torque (HAWKINS, 2015). Este aplicativo é capaz de ler informações do OBD 2 por meio do ELM 327 utilizando tecnologia *bluetooth*, associá-las a uma coordenada de GPS e enviar esse conjunto de informações para a aplicação de detecção e alerta de acidentes que executa na OBU.

Neste trabalho a OBU é formada pela associação da *routerboard* a um *notebook* e ao *smartphone*. A inclusão do *notebook* tem a função de aumentar a capacidade de processamento da OBU, possibilitando a execução da aplicação de detecção e alertas de acidentes.

4.2 Segundo ambiente: as vias de trânsito

A Figura 16 destaca os dispositivos deste ambiente.

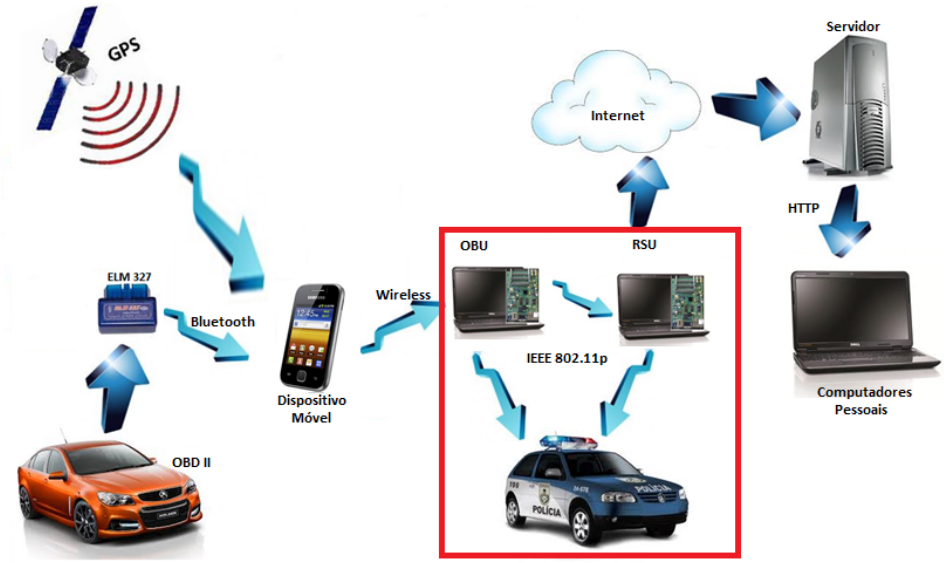


Figura 16 Segundo ambiente: as vias de trânsito

Neste ambiente prevalece a comunicação utilizando o padrão IEEE 802.11p das VANETs. Nele temos as OBUs e as RSUs que fornecem as comunicações V2V e V2I. Nessas comunicações mensagens de segurança

são enviadas entre as OBUs emitindo alertas para os motoristas quando necessário. As RSUs podem estar ligadas diretamente à internet, fazendo assim a comunicação entre esse ambiente e o ambiente de internet.

A RSU utilizada é um dispositivo idêntico à OBU, formada por uma *routerboard* e um *notebook*. Elas se diferenciam apenas pela sua função na VANET: a RSU fica posicionada nas vias de trânsito e a OBU é instalada no veículo.

Para tornar a passagem da informação pela *routerboard* da OBU transparente, foi instalada nelas uma aplicação capaz de receber informações em *broadcast* em uma determinada porta e reencaminhar essa transmissão em *broadcast* pelas interfaces de rede da *routerboard*. Com isso a aplicação que executa no *notebook* pode enviar e receber informações em *broadcast* na VANET, mesmo sem possuir *hardware* específico para se comunicar no padrão IEEE 802.11p das VANETs.

4.3 Terceiro ambiente: internet

Este ambiente é composto pela RSU, por um servidor *web* e por clientes que acessam a aplicação, como pode ser visto na Figura 17.

Ao enviar dados do ambiente de vias de trânsito para o ambiente de internet, o servidor *web* recebe esses dados, os trata e os disponibiliza às centrais de socorro ou outras pessoas interessadas, que vão monitorar essas informações e tomar as providências e precauções necessárias para prevenir ou socorrer vítimas de acidentes.

As aplicações citadas da descrição dos ambientes são detalhadas a seguir.

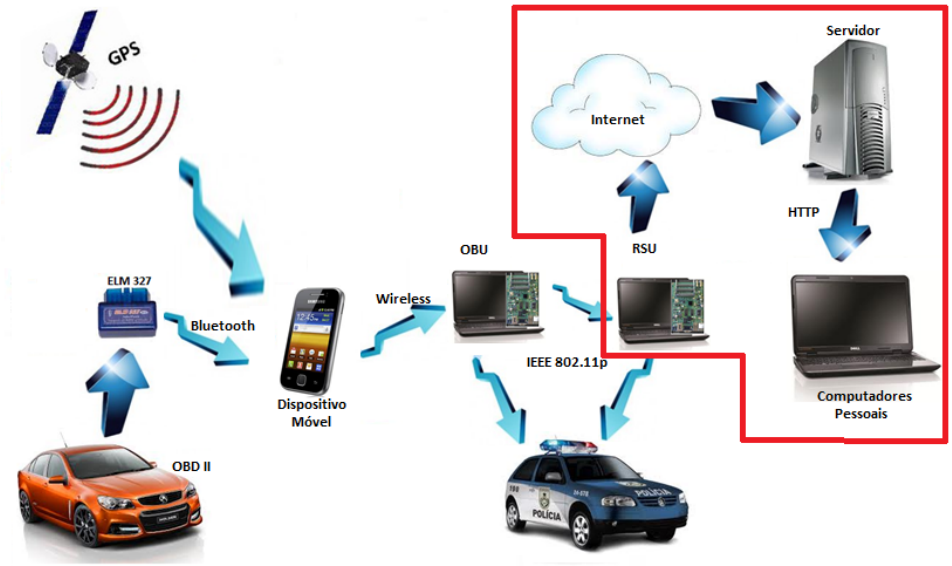


Figura 17 Terceiro ambiente: internet.

4.4 A aplicação de detecção automática e alerta de acidentes

A coleta de informações do veículo possibilita o desenvolvimento de aplicações de segurança de trânsito que utilizam essas informações. Com essas informações pode-se determinar se um veículo sofreu uma desaceleração brusca e/ou se seu *airbag* foi acionado e enviar um alerta na VANET caso isso ocorra.

Os alertas de acidentes são transmitidos por meio de mensagens JSON (*Javascript object notation*) (JSON, 2015) e salvas em um banco de dados Postgresql (2015). O JSON é utilizado por ser uma notação compacta e por possuir ferramentas que facilitam sua manipulação em várias linguagens de programação. O banco de dados Postgresql foi escolhido por ser gratuito e atender às necessidades do desenvolvimento.

Para o desenvolvimento foi utilizada linguagem Groovy (GROOVY,

2015) associada ao *framework* Grails (GRAILS, 2015). Essas ferramentas foram escolhidas por oferecer facilidades para o desenvolvimento de aplicações WEB. Para apresentar a localização do veículo, foi utilizada a API do Google Maps (GOOGLE MAPS, 2015).

A aplicação executa simultaneamente nas OBUs, nas RSUs e no servidor *web*. Nas OBUs a aplicação monitora as informações do veículo para realizar a detecção de acidente, dispara o alerta na VANET caso seja necessário e recebe/retransmite alertas de acidentes da VANET. Nas RSUs a aplicação recebe e retransmite alertas de acidentes e envia os alertas ao servidor *web*. No servidor os alertas são disponibilizados em uma interface *web*.

4.4.1 A detecção de acidentes

Para realizar a detecção de acidentes são utilizados os dados extraídos do OBD 2. O OBD 2 pode coletar informações dos *airbags* de veículos, indicando o disparo ou não deste. Essa informação deve ser lida periodicamente (nos experimentos utilizaram-se intervalos de um segundo) e, em caso de disparo do *airbag*, deve emitir um alerta de acidente.

De forma redundante, são utilizadas informações de velocidades extraídas do OBD 2 para detectar desacelerações bruscas. Se houver uma redução significativa na velocidade em um curto espaço de tempo significa que aconteceu uma desaceleração brusca, que pode indicar um acidente.

A Figura 18 apresenta o conjunto de informações enviadas pelo dispositivo móvel para a OBU em notação JSON. Cada informação enviada à OBU tem uma função dentro da aplicação:

- **id**: Identificador único do alerta no banco de dados do dispositivo

```
{
    "id": 1094,
    "carCode": "Sau1z",
    "code": "192.168.188.116usjU",
    "collectTime": 1426946384332,
    "gpsSpeed": 0,
    "gpsTime": 1426945353519,
    "isAirbagOpen": false,
    "lat": -21.227654073279584,
    "lon": -44.978678839596874,
    "obdSpeed": 0,
    "obuTime": 1426946385626
}
```


Figura 18 Informações recebidas em notação JSON pela OBU por meio do dispositivo móvel.

(OBU/RSU) atual do alerta. É um número sequencial.

- **carCode**: Código identificador da OBU do veículo ao qual a informação coletada pertence. Este dado é agregado pela OBU. Neste trabalho o IP da OBU foi utilizado para preencher este atributo, porém outras informações, como endereço MAC, poderiam ser utilizadas.

- **code**: Código único da informação coletada, formado pelo código do veículo e um conjunto de caracteres aleatórios.

- **collectTime**: Data, em formato UTC, na qual a informação foi coletada pelo dispositivo móvel.

- **gpsSpeed**: Velocidade extraída do GPS.

- **isAirbagOpen**: Informação sobre o *airbag* do veículo, coletada do OBD 2.

- **gpsTime**: Tempo, em formato UTC, extraído do GPS.

- **lat**: Latitude do veículo.
- **lon**: Longitude do veículo.
- **obdSpeed**: Velocidade coletada do OBD 2
- **obuTime**: Data, em UTC, na qual a informação chegou na OBU.

```
1  Procedure accidenteDetection();
2  car = getCarInformation();
3  speed1 = car.read(speed);
4  time1 = car.read(time);
5  while (true) do
6      if (car.hasAirbag()) then
7          airbagFired = car.read(airbag);
8          if (airbagFired) then
9              accidenteAlert();
10     car = getCarInformation();
11     speed2 = car.read(speed);
12     time2 = car.read(time);
13     acceleration = (speed2 - speed1) / (time2 - time1);
14     if (acceleration < -61.1 ) then
15         accidenteAlert();
16     speed1 = speed2;
17     time1 = time2;
```

Algoritmo 1: Detecção de acidentes.

O funcionamento da detecção de acidentes é apresentado no Algoritmo 1. A aplicação recebe informações dos *smartphones* com os dados recebidos do OBD 2 (linhas 2 a 4). É verificado se o veículo possui *airbag* (linha 6). Se possuir *airbag*, este é verificado sempre que um novo conjunto de informações do veículo é recebido. Caso o *airbag* tenha disparado, o método de emissão de alertas é chamado (linhas 7 a 9).

Após verificar o *airbag*, a velocidade é utilizada para detectar uma desaceleração brusca. Uma desaceleração brusca é um indício de que um

acidente pode ter acontecido. O cálculo da aceleração foi feito utilizando a aceleração média conforme a Equação 1.

$$a = \frac{\Delta v}{\Delta t} \tag{1}$$

Onde:

Δv é a variação da velocidade e;

Δt é a variação do tempo.

Os valores da velocidade e do tempo são coletados constantemente (linhas 10 a 12). Dois valores coletados são utilizados para o cálculo da aceleração (linha 13). Se a desaceleração calculada passar $61,1 m/s^2$ é disparado um alerta de possível acidente (linhas 14 e 15). Caso contrário, os valores da velocidade e tempo mais antigos são descartados (linhas 16 e 17) e a execução volta ao laço de repetição, onde uma coleta de informações é realizada. Esse valor foi definido com base nos trabalhos de Singh e Song (2009). Segundo eles, desacelerações coletadas de acidentes em velocidades de 19 a 40 km/h são utilizadas como limiar para o disparo ou não do *airbag* nos veículos. Posteriormente eles apresentam a medição de velocidade em uma colisão na qual a velocidade inicial era 22 km/h e a velocidade após 100 ms chegou a zero. Com esses dados podemos calcular a desaceleração média que é utilizada como limiar conforme a Equação 2:

$$a = \frac{22 km/h}{100 ms} = \frac{6,11 m/s}{0,1 s} = 61,1 m/s^2 \tag{2}$$

O Algoritmo 2 apresenta o alerta de acidentes. Se um acidente for detectado, um alerta de provável acidente é enviado por meio da VANET (linha 2). Para evitar falsos positivos, é feita a verificação da velocidade após

```
1  Procedure accidenteAlert();
2  sendProbableAccidentAlert();
3  sleep(30000);
4  car = getCarInformation();
5  if (car == null or car.read(speed) == 0) then
6      // Perguntando ao motorista sobre o acidente, aguarda a
       resposta por 30 segundos;
7      isRealAccident = driverQuestion(30000);
8      if (isRealAccident == true) then
9          stopProbableAccidentAlert();
10         sendAccidentAlert();
11     else
12         stopProbableAccidentAlert();
```

Algoritmo 2: Alerta de acidentes.

30 segundos. Se a velocidade for zero ou o equipamento parar de enviar informações, um aviso é enviado ao motorista do veículo acidentado. O motorista tem trinta segundos para indicar que foi um falso acidente (linhas 3 a 5). Se o motorista indicar que aconteceu um acidente, ou não responder, o alerta de provável acidente é cessado e um alerta de acidente passa a ser transmitido (linhas 8 à 10). Se ele indicar que não houve acidente, o alerta de provável acidente é interrompido (linha 12).

Os alertas são enviados aos veículos e RSUs que estão ao alcance do sinal da rede veicular. Nos alertas são transmitidas as coordenadas geográficas do acidente e informações sobre o veículo acidentado.

Ao receber o alerta, as OBUs dos veículos que se aproximam do local do acidente podem usar informações de coordenadas geográficas, extraídas do *smartphones*, para calcular a distância do veículo em relação ao acidente e, assim, alertar o motorista. Quando o alerta chega a uma RSU, um sistema web pode exibi-lo para unidades de socorro ou para qualquer pessoa que tenha acesso. As RSUs também disseminam o alerta de acidente para outros

veículos que trafegam no seu raio de alcance de transmissão.

A Figura 19 apresenta um exemplo do alerta recebido e salvo pela aplicação em notação JSON.


```
{
  "id": 20041,
  "alertDate": 1426946707331,
  "carCode": "192.168.188.11",
  "code": "Sau1z",
  "distance": 230,
  "ip": "192.168.188.11",
  "lat": -21.227529226159973,
  "lng": -44.978735296908035,
  "message": "Acidente detectado!",
  "messageCode": 3,
  "receivedDate": 1426948861413,
  "seen": false,
  "sendDate": 1426948861366
}
```


Figura 19 Alerta de acidente salvo em banco de dados pela aplicação em notação JSON.

Cada atributo do alerta possui uma função dentro da aplicação:

- **id**: Identificador único do alerta no banco de dados do dispositivo (OBU/RSU) que o alerta foi salvo.
- **alertDate**: Data, em formato UTC, na qual o alerta foi disparado pelo veículo acidentado.
- **carCode**: Código identificador da OBU do veículo que disparou o alerta de acidente, nos experimentos foi utilizado o endereço IP da OBU.
- **code**: Código do alerta, comum a todos os dispositivos da VANET. Utilizado para o tratamento de alertas redundantes.

- **distance**: Distância em que o veículo acidentado se encontra, no momento do recebimento do alerta, do dispositivo atual. É calculada através da comparação da coordenada geográfica do veículo acidentado com a última coordenada geográfica do veículo que recebeu o alerta.
- **ip**: IP do OBU que disparou o alerta de acidente.
- **lat**: Latitude do veículo acidentado.
- **lng**: Longitude do veículo acidentado.
- **message**: Mensagem do alerta.
- **messageCode**: Código de cada tipo de alerta. Até então, foram definidos dois tipos: provável acidente (2) e acidente confirmado (3).
- **receivedDate**: Data, em formato UTC, do recebimento do alerta pelo dispositivo atual.
- **seen**: Indica se o alerta já foi visto. Este atributo foi criado para controle dos alertas em centrais de socorro.
- **sendDate**: Data, em formato UTC, do envio do alerta pelo último dispositivo que o alerta passou antes de chegar ao dispositivo atual.

4.5 A disseminação de informações

Para disseminar informações na VANET, a OBU faz transmissões em *broadcast*. Com isso todos OBUs e RSUs que estão no raio de alcance da transmissão podem receber a informação. Porém, existem situações em que apenas enviar informações para dispositivos no raio de alcance não é

suficiente. No caso da detecção de acidentes, é essencial que um veículo que passe pelo acidente retransmita informação para outros veículos, aumentando o raio de alcance da informação. Para isso, foi utiliza transmissão epidêmica e oportunista de informações.

```
1 Procedure alertListener();
2 while (true) do
3     alert = listenerAlert();
4     if (alert.isNotRedundantAlert()) then
5         alert.showToDriver();
6         car = getCarInformation();
7         while
          (alert.isInInterestedArea(car.read(latitude),car.read(longitude)
          and alert.lifeTimeIsOver()) do
8             alert.send();
9             car = getCarInformation();
```

Algoritmo 3: Recebimento e retransmissão de alerta de acidentes.

O Algoritmo 3 mostra o recebimento e retransmissão de alertas pela OBU/RSU. A aplicação escuta transmissões na VANET (linha 3). Quando um alerta é recebido, verifica-se se ele já foi recebido antes (linha 4). Se é a primeira vez que o alerta é recebido, ele é exibido ao motorista (linha 5), senão, o alerta é ignorado. Informações do veículo são coletadas (linha 6) e, enquanto o veículo estiver dentro da distância definida como sendo de interesse da informação e ainda não tiver passado o tempo de vida configurado para um alerta de acidente (linha 7), o alerta é retransmitido (linha 8) e são coletadas novas informações do veículo (linha 9). Para os experimentos realizados neste trabalho, a distância de interesse da informação foi definida em 1 km e o tempo de vida do alerta foi ilimitado.

A seguir são detalhados os experimentos realizados.

4.6 Experimentos

Os experimentos foram realizados na avenida central da Universidade Federal de Lavras (UFLA). A avenida permite visada entre os equipamentos na maior parte de seu trajeto, porém possui obstáculos, como árvores e prédios além de outros veículos que trafegavam na avenida durante os experimentos. O percurso utilizado tem aproximadamente 1,2 Km de extensão e variações de altitude de até 20 metros. A Figura 20 apresenta o trajeto da avenida e os pontos onde equipamentos foram instalados ou veículos posicionados para os experimentos.

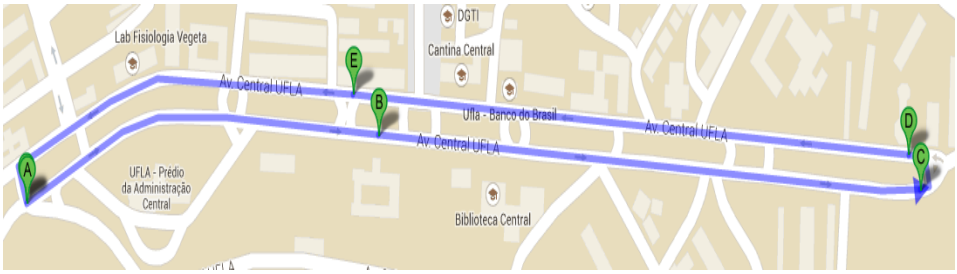


Figura 20 Avenida central da UFLA, cenário utilizado nos experimentos.

Foram realizados três experimentos, os dois primeiros com cinco repetições cada e o terceiro com 3 repetições. As configurações e materiais utilizados no experimento são apresentados na Tabela 7.

Para simular acidentes, foi utilizado um simulador de OBD 2, o OBDSim (2015). Com essa ferramenta podemos simular o disparo do *airbag* e uma desaceleração brusca. Com o OBDSim, é possível gerar dados simulados do OBD 2 de um veículo em um computador e transmitir estes dados via *bluetooth* para que a aplicação realize a detecção de acidentes.

Tabela 7 Configurações e equipamentos utilizados nos experimentos.

Configuração	Valor
PHY/MAC	IEEE 802.11p
Frequência de Transmissão	5,9 GHz
Número de experimentos	3
Número de repetições	3 a 5
Número de veículos	4
Distância máxima percorrida por repetição	2,4 Km
Número de OBUs	3
Número de RSUs	1
Distância de interesse da informação	1 km
Velocidade dos veículos	entre 30 e 40 Km/h

4.6.1 Primeiro experimento: retransmissão do alerta para uma RSU

O primeiro experimento tem o objetivo de avaliar a emissão de alertas de acidente e sua retransmissão para uma RSU.

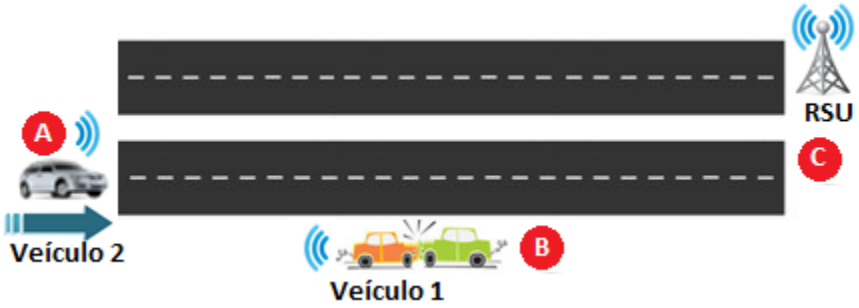


Figura 21 Cenário utilizado para o primeiro experimento.

Neste cenário, um alerta de acidente foi disparado de um veículo (1) acidentado no ponto B da Figura 21. Um outro veículo (2) sai do ponto A e se desloca até o ponto C, que tem uma RSU instalada, passando pelo ponto B. O Veículo 2 recebe o alerta de acidente emitido pelo Veículo 1 e, ao aproximar-se do ponto C, retransmite o alerta para a RSU.

4.6.2 Segundo experimento: retransmissão do alerta para um veículo em movimento

O segundo experimento, ilustrado na Figura 22, tem o objetivo de avaliar a retransmissão de alertas de acidente entre veículos em movimento.

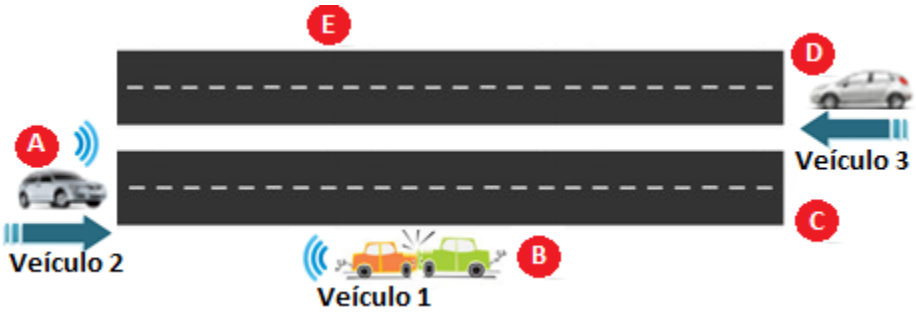


Figura 22 Cenário utilizado para o segundo experimento.

Um alerta de acidente é disparado de um veículo (1) acidentado no ponto B da Figura 22. Um Veículo (2) parte do ponto A e se desloca até um ponto C. Ao aproximar-se do ponto B o Veículo 2 recebe o alerta de acidentes. Neste período, o um Veículo (3) se desloca do ponto D até o ponto E em sentido contrário ao Veículo 2. Quando o Veículo 3 entra no raio de alcance do Veículo 2, antes de passar em B, ele recebe o alerta de acidente por meio do Veículo 2.

É interessante observar que o Veículo 3, ao receber antecipadamente a localização do acidente (ponto B), pode tomar providências de precaução como desviar-se do acidente ou reduzir a velocidade.

4.6.3 Terceiro experimento: validação da disseminação de alertas

O terceiro experimento é ilustrado na Figura 23 e tem o objetivo de validar o funcionamento da disseminação do alerta de acidentes em um cenário com mais veículos e com uma aplicação de monitoramento de acidentes.

Neste experimento, além da avenida Central da UFLA, foram utilizadas a Avenida Sul, o estacionamento próximo ao Departamento de Ciência da Computação (DCC) e algumas das vias que os interligam. Isso foi necessário para garantir um isolamento entre as OBUs/RSUs.

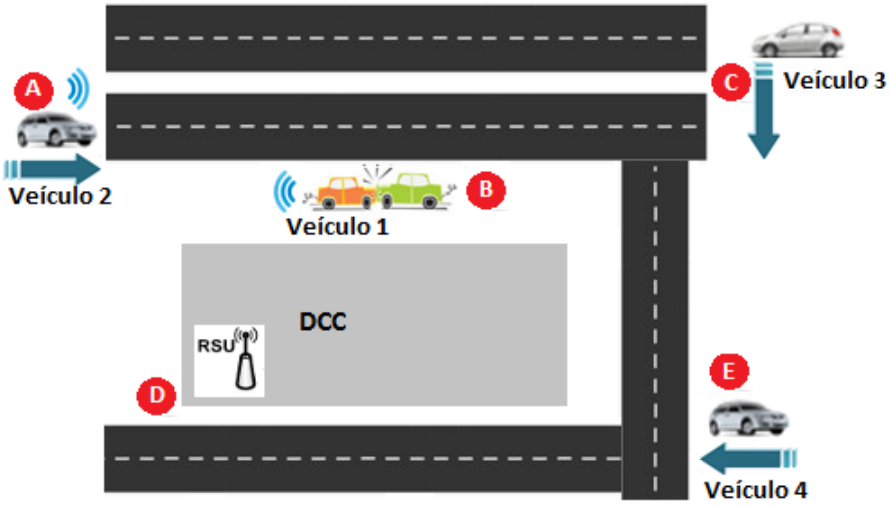


Figura 23 Cenário utilizado no terceiro experimento.

Um alerta de acidente é disparado do Veículo 1 no ponto B da Figura 23. O Veículo 2 parte do ponto A em direção ao ponto C e, ao se aproximar do Veículo 1, recebe o alerta de acidente. Simultaneamente, o Veículo 3 parte de C, se comunica com o Veículo 2 recebendo o alerta e segue em direção ao ponto D. Próximo ao ponto D, está instalada uma RSU que

recebe o alerta do Veículo 3 quando este se aproxima dela. A RSU entrega o alerta para o servidor com acesso à internet e retransmite o alerta para todos os veículos que passarem dentro do seu raio de alcance de transmissão. Uma página web é disponibilizada no servidor para que centrais de alerta possam acessá-la e verificar os alertas em tempo real. O Veículo 4 parte de E em direção ao ponto D e, ao se aproximar da RSU, também recebe o alerta de acidente.

4.7 Métricas avaliadas

Em uma aplicação de segurança de trânsito, deve-se priorizar a entrega de alertas em tempo e distância suficientes para que os motoristas próximos ao acidente sejam alertados e possam tomar as medidas cabíveis para evitar novos acidentes. A VANET foi avaliada através da medição da latência em relação à distância entre os equipamentos em todas as transmissões. Com isso é possível avaliar se a comunicação da VANET é robusta para ser utilizada em rodovias e cidades, não apenas em aplicações de detecção de acidentes, mas também para qualquer aplicação que exija tanto quanto ou menos que essa aplicação exige da VANET.

Para coletar as informações necessárias para a avaliação da rede, informações como velocidade e coordenadas geográficas são enviadas à OBU de cada veículo envolvido nos experimentos a cada segundo. A cada envio de alerta, a latência de transmissão entre os equipamentos é coletada pela OBU ou RSU que recebe o alerta. A seguir são apresentados os resultados dos experimentos.

5 RESULTADOS E DISCUSSÕES

Para a avaliação dos experimentos foram consideradas faixas de dez em dez metros para o percurso, iniciando do ponto mais distante em que foi recebido um alerta de acidente. Os valores de latência representam a média dos valores obtidos em cada faixa de cada repetição.

5.1 Primeiro experimento: retransmissão para RSU

Em cada uma das cinco repetições, as informações dos veículos foram coletadas, em média, em 3529 posições diferentes. A Figura 24 apresenta os pontos do trajeto do Veículo 2 onde cada informação foi coletada em uma das repetições realizadas.

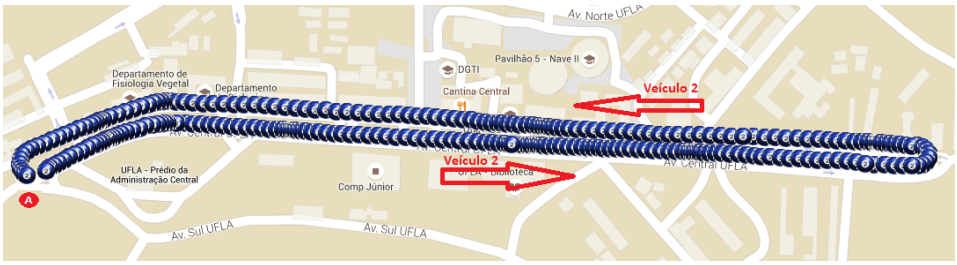
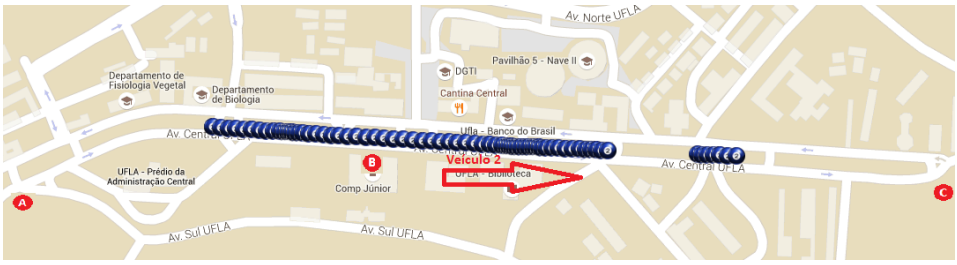
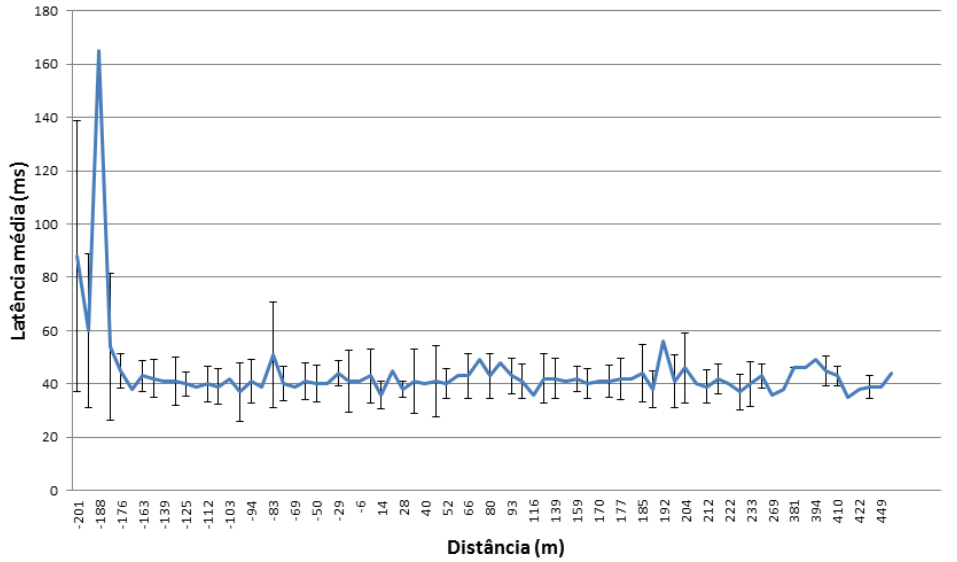


Figura 24 Pontos de coleta de informações do veículo 2 no primeiro experimento.

A Figura 25(a) mostra a parte do trajeto do experimento em que o Veículo 2 recebe os alertas de acidente enviados pelo Veículo 1. Como qualquer comunicação sem fio, podemos ter problemas de comunicação. Há um trecho dentro do raio de transmissão em que os alertas são perdidos. Isso ocorre devido aos obstáculos presentes no cenário, que impedem a comunicação entre os equipamentos. Uma conexão redundante com a tecnologia 3G poderia amenizar problemas como esse.



(a) Trecho do trajeto do primeiro experimento em que o Veículo 2 recebe os alertas de acidente enviados pelo Veículo 1.



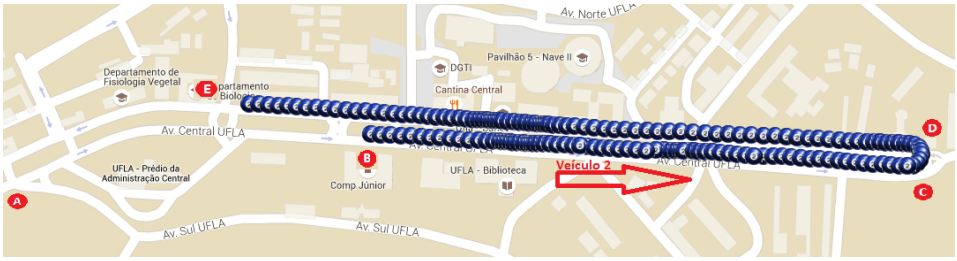
(b) Relação da latência na transmissão de alertas de acidente com a distância entre os Veículos 1 e 2 no primeiro experimento.

Figura 25 Comunicação entre os Veículos 1 e 2 no primeiro experimento.

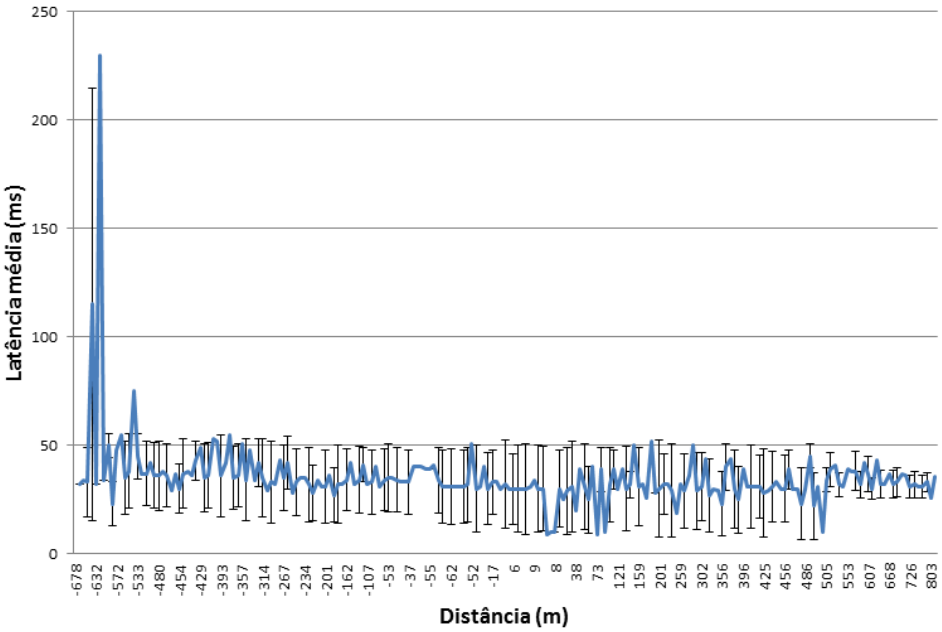
A Figura 25(b) apresenta a relação entre a latência da transmissão do alerta e a distância que o Veículo 2 se encontrava do Veículo 1. Os valores negativos da distância indicam que o Veículo 2 estava se aproximando do Veículo 1, os valores positivos indicam um afastamento. O primeiro alerta recebido pelo Veículo 2 foi, em média, a uma distância de 195 metros do

Veículo 1. Já o último alerta de acidente foi recebido, em média, a 382 metros. A latência média na disseminação de alertas foi de 44 milissegundos.

Na Figura 26(a) vemos o trecho do trajeto do Veículo 2 do qual ele retransmite o alerta para a RSU.



(a) Trecho do trajeto do primeiro experimento em que a RSU recebe os alertas de acidente retransmitidos pelo Veículo 2.



(b) Relação da latência na transmissão de alertas de acidente com a distância entre o Veículo 2 e a RSU no primeiro experimento.

Figura 26 Comunicação entre o veículo 2 e a RSU no primeiro experimento.

A Figura 26(b) apresenta a relação entre a latência e a distância na transmissão do alerta de acidentes entre o Veículo 2 e a RSU. Os valores de distância negativos indicam uma aproximação e os valores positivos indicam um afastamento. O primeiro alerta recebido pela RSU foi, em média, a uma distância de 655 metros do Veículo 2. O último alerta de acidente foi recebido, em média, a 702 metros. Nota-se uma diferença no alcance da transmissão entre o Veículo 2 e a RSU e entre os veículos 1 e 2. Isso se deve à posição onde a RSU foi colocada, que é mais elevada que a posição onde o Veículo 1 estava. A RSU está mais elevada que o Veículo 2 na maior parte do percurso que ele percorre, o que melhora o alcance da sua transmissão. A latência média na disseminação de alertas foi de 37 milissegundos.

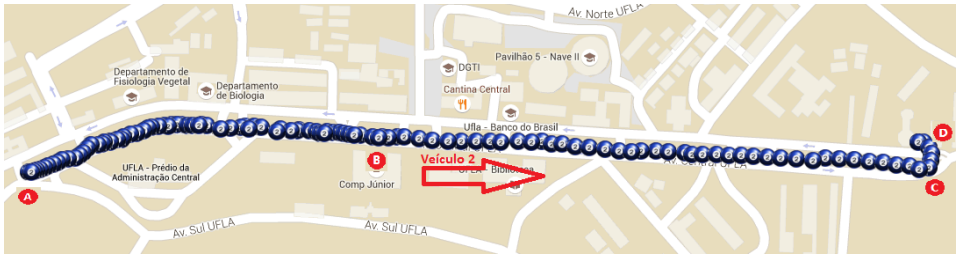
Nas transmissões nota-se uma latência maior nos primeiros pacotes recebidos. Isso acontece devido à estabilização da conexão entre os dispositivos.

O Veículo 1 emitiu um alerta de acidentes que foi recebido pelo Veículo 2. A RSU recebeu o alerta por meio de retransmissão feita pelo Veículo 2. Os alertas foram recebidos em tempo e distância suficientes para permitir uma reação do motorista do Veículo 2. A RSU recebeu o alerta assim que teve conexão estabelecida com o dispositivo que retransmitia a informação.

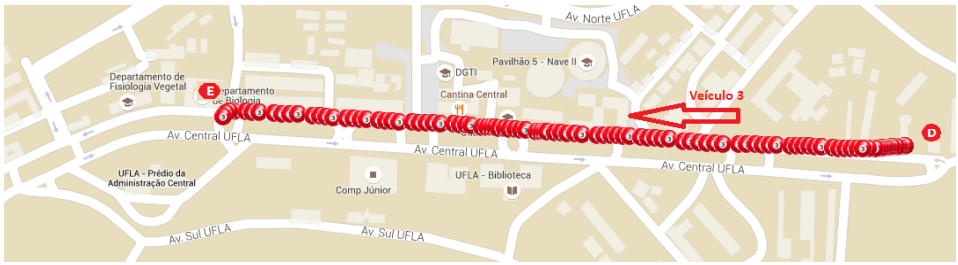
5.2 Segundo experimento: retransmissão entre veículos

No segundo experimento, foram coletadas informações dos veículos novamente em intervalos de 1 segundo. Foram coletadas em média 10.917 pacotes com informações de cada veículo. Assim como no primeiro experimento, o Veículo 2 recebe o alerta de acidente do Veículo 1 e o repassa a

outros dispositivos na VANET. Neste experimento um Veículo 3 recebe o alerta do Veículo 2. A Figura 27(a) mostra os pontos do trajeto onde informações do Veículo 2 foram recebidas. Já na Figura 27(b) são mostrados os pontos do trajeto onde informações do Veículo 3 foram recebidas.



(a) Pontos onde informações do Veículo 2 foram coletadas no segundo experimento.



(b) Pontos onde informações do Veículo 3 foram coletadas no segundo experimento.

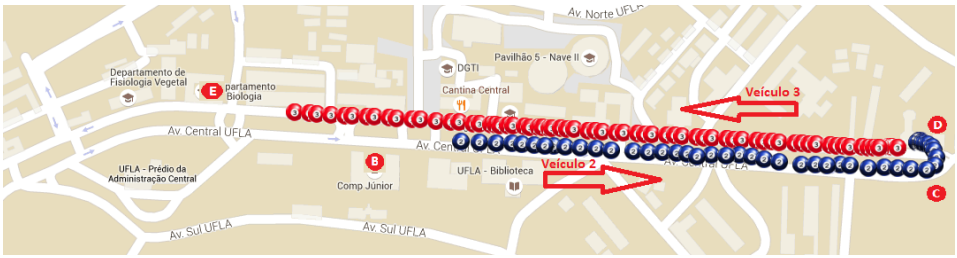
Figura 27 Coletas de dados dos veículos no segundo experimento.

A transmissão do alerta de acidente do Veículo 1 para o Veículo 2 se assemelha ao do primeiro experimento.

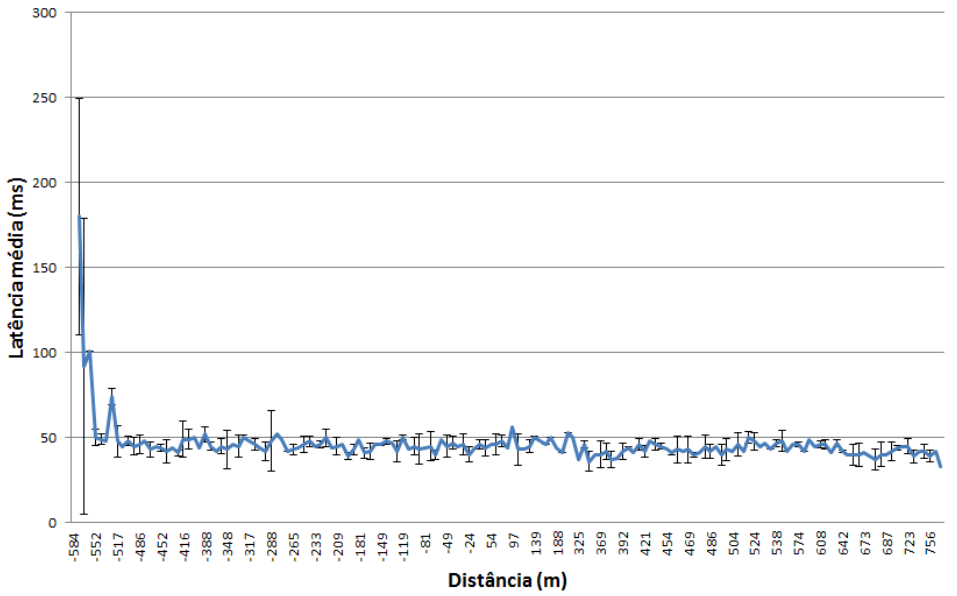
Os pontos do cenário onde o Veículo 3 (na cor vermelha) recebe a retransmissão do alerta de acidentes do Veículo 2 (na cor azul) e que o Veículo 2 envia os alertas para o Veículo 3 são mostrados na Figura 28(a).

Na Figura 28(a) podemos notar que o alcance é maior quando os veículos estão se afastando que quando estão se aproximando. O primeiro alerta é recebido pelo Veículo 3 quando ele está, em média, a uma distân-

cia de 563 metros do Veículo 2. Já o último alerta é recebido quando os veículos estão a uma distância de 741 metros entre eles. Isso é devido ao estabelecimento da conexão entre os veículos. Quando os veículos estão se afastando já existe uma conexão estabelecida entre eles e quando estão se aproximando essa conexão ainda vai ser estabelecida.



(a) Trechos dos trajetos dos Veículos 2 e 3 do segundo experimento em que o Veículo 3 (vermelho) recebe os alertas de acidente enviados pelo Veículo 2 (azul).



(b) Relação entre a distância entre os Veículos 2 e 3 e a latência no envio do alerta entre eles.

Figura 28 Comunicação entre os veículos no segundo experimento.

A Figura 28(b) apresenta a relação entre a distância e a latência na comunicação entre os Veículos 2 e 3. Os valores de distância negativos indicam uma aproximação entre os veículos, os valores positivos indicam um afastamento. A latência da comunicação foi, em média, de 49 milissegundos. Assim como no primeiro experimento, vemos uma oscilação na latência dos primeiros alertas recebidos devido à estabilização da conexão entre os dispositivos.

Observou-se que o Veículo 3 recebeu o alerta de acidente retransmitido por meio do Veículo 2, e que a retransmissão aumentou o raio de alcance do alerta.

5.3 Terceiro experimento: validação da disseminação de alertas

Neste experimento foi testada a disseminação do alerta de acidentes com quatro veículos. O Veículo 1 simula o veículo acidentado. O alerta foi emitido em *broadcast* e recebido pelo Veículo 2. A Figura 29(a) mostra a rota percorrida pelo Veículo 2.

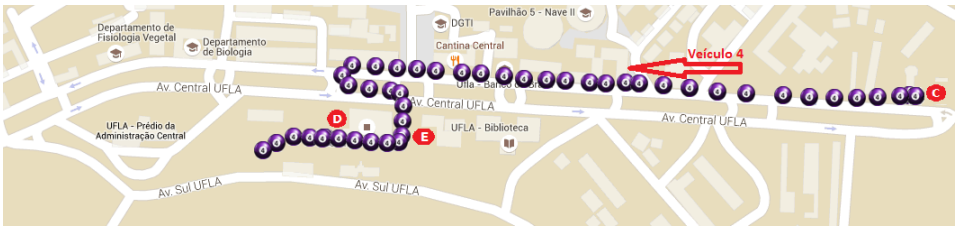
O Veículo 2 retransmitiu o alerta enquanto estava dentro da área de interesse da informação, que foi configurada em 1000 metros. O Veículo 3 recebeu o alerta do Veículo 2 e depois o retransmitiu para a RSU. A Figura 29(b) apresenta a rota percorrida pelo Veículo 3.

A RSU retransmite então o alerta para um Veículo 4, que transitou próximo a ela como apresentado na Figura 29(c).

Quando chega à RSU, o alerta é salvo em um banco de dados e disponibilizado em uma página web que pode ser acessada por centrais de socorro a acidentes. A página de alertas é mostrada na Figura 30. Nela podemos ver uma lista de todos os alertas recebidos e, ao selecionar um

(a) Dados coletados do Veículo 2 no terceiro experimento.

(b) Dados coletados do Veículo 3 no terceiro experimento.



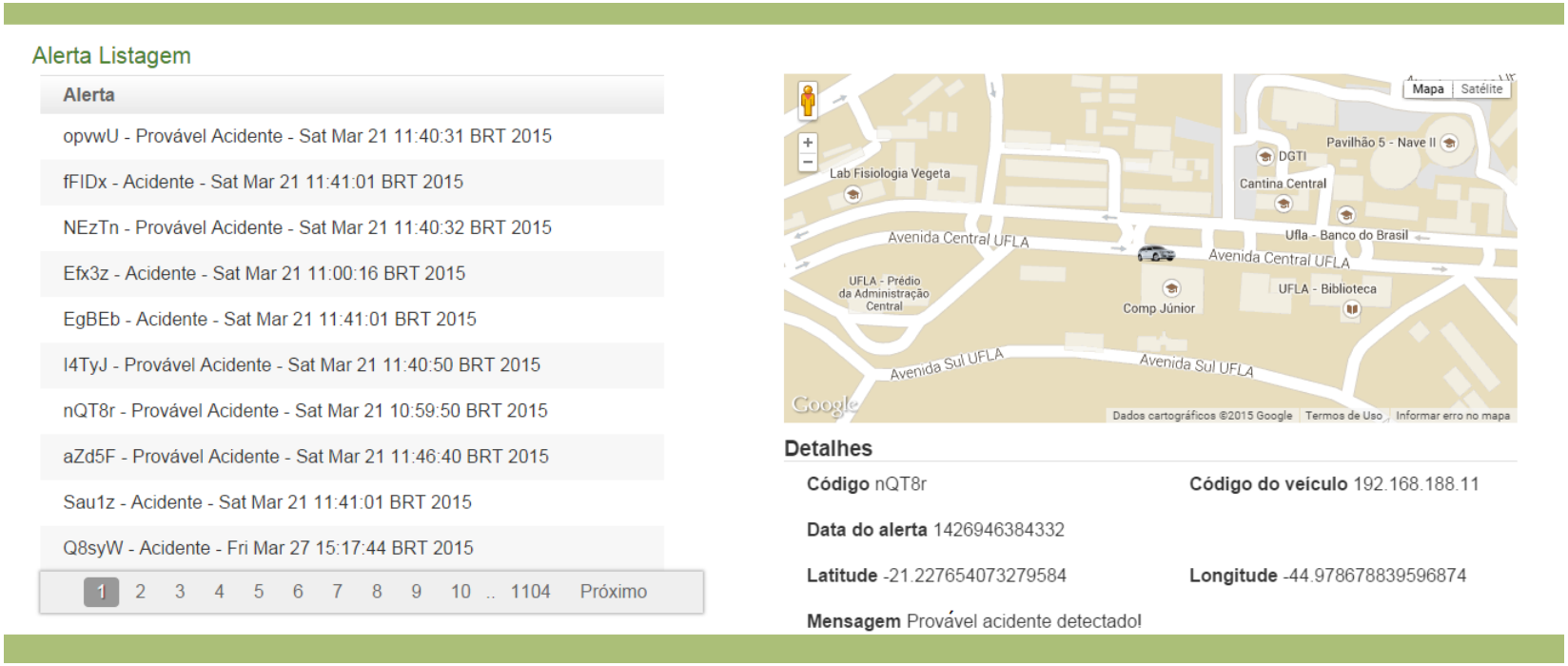
(c) Dados coletados do Veículo 4 no terceiro experimento.

Figura 29 Pontos do trajeto em que foram coletados dados dos veículos.

deles, vemos a localização e os detalhes do veículo acidentado.

Os experimentos mostraram que a VANET construída por Barcelos et al. (2014a) usando o padrão IEEE 802.11p pode ser utilizada para disseminar alertas de acidente de trânsito obedecendo os requisitos de qualidade de serviço estabelecidos por Ibanez et al. (2011). A disseminação de

Figura 30 Página *web* disponibilizada para centrais de socorro.



informações em VANETs pode ter seu alcance ampliado com a utilização de aplicações epidêmicas e oportunistas.

6 CONCLUSÕES E TRABALHOS FUTUROS

Neste trabalho foi criada uma aplicação para prover segurança no trânsito realizando a detecção automática e alerta de acidentes em tempo real.

A integração de múltiplos dispositivos possibilita a comunicação da VANET de acordo com os padrões IEEE 802.11p e IEEE 1609.

A aplicação de detecção e alerta de acidentes de trânsito desenvolvida se mostrou eficiente. Os dados dos veículos foram coletados e, através deles, foi possível detectar acidentes automaticamente.

Um alerta é emitido continuamente na VANET sempre que um acidente é detectado. O alerta é recebido por OBUs/RSUs que estão dentro do raio de alcance da transmissão e retransmitido por eles até que eles estejam a uma distância configurada como fora do raio de interesse da informação do acidente. Quando um veículo está fora do raio de interesse da informação, a transmissão do alerta é suspensa. Isso controla o aumento de dados armazenados e o aumento do número de transmissões na VANET.

Nos cenários avaliados, a aplicação cumpriu os requisitos de qualidade de serviço para aplicações de segurança em VANETs, tendo apresentado valores de latência menores que 100 milissegundos e alcances superiores a 150 metros.

Este trabalho mostrou resultados que possibilitam a utilização de VANETs para outras aplicações de segurança de trânsito, como violação de semáforo e aviso de excesso de velocidade antes de uma curva por exemplo.

Futuramente, pretende-se validar este trabalho com outras aplicações de segurança de trânsito e também com aplicações de monitoramento de veículos de frota e de transporte de passageiros. Pretende-se também

aprimorar o hardware utilizado para que se possa ter um equipamento mais compacto, a ponto de ser incorporado de forma mais eficiente aos veículos, que possa se comunicar utilizando os padrões das VANETs e processar as aplicações desenvolvidas. Além disso, pode-se melhorar a interface do sistema com o usuário, facilitando o entendimento das informações apresentadas por ele. Outra melhoria que pode ser feita é a indicação do sentido do movimento do veículo nas informações transmitidas pela VANET. Pode-se ainda avaliar o comportamento da aplicação desenvolvida com outros algoritmos de roteamento.

REFERÊNCIAS

AHMED, S. A. M. et al. Overview of Wireless Access in Vehicular Environment (WAVE) protocols and standards. **Indian Journal of Science and Technology**, Bangalore, v. 6, n. 7, p. 4994-5001, 2013.

ALVES, R. S. et al. Redes veiculares: princípios, aplicações e desafios. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 27., 2009, Recife. **Anais...** Recife: SBRC, 2009. p. 199-254.

APPLE IOS. Disponível em: <https://www.apple.com/br/ios/>. Acesso em: 10 mar. 2015.

BARCELOS, V. P. et al. Sistema de monitoramento de veículos usando dispositivos no padrão IEEE 802.11p. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS, 32., 2014, Florianópolis. **Anais...** Florianópolis: UFSC, 2014a. p. 460-467.

BARCELOS, V. P. et al. Vehicle monitoring system using IEEE 802.11p device and android application. In: IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS, 19., 2014, Madeira. **Proceedings...** Madeira: Universidade da Madeira, 2014b. p. 1-7.

BOUKERCHE, A. et al. Localization systems for wireless sensor networks. **IEEE Transactions on Wireless Communications**, New York, v. 14, n. 6, p. 6-12, Dec. 2007.

CHAN, C. Y. On the detection of vehicular crashes-system characteristics and architecture. **IEEE Transactions on Vehicular Technology**, New York, v. 51, n. 1, p. 180-193, Jan. 2002.

CORREIA, L. H. A. et al. Antrop - protocolo de roteamento bio-inspirado em colônia de formiga tolerante a falhas e desconexões aplicado às redes emergenciais. In: BRAZILIAN SYMPOSIUM ON COMPUTER NETWORKS AND DISTRIBUTED SYSTEMS, 29., 2011, Campo Grande. **Proceedings...** Campo Grande: SBRC, 2011. p. 175-188.

DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTE. **Anuário estatístico das rodovias federais 2010**. Brasília, 2010. 683 p.

DINIZ, I. S. et al. Scanner automotivo wireless. In: CONGRESSO INTERNACIONAL E EXPOSIÇÃO SUL-AMERICANA DE AUTOMAÇÃO - BRAZIL AUTOMATION ISA, 13., 2009, São Paulo. **Proceedings...** São Paulo, 2009. 1 CD-ROM.

DJUKNIC, G.; RICHTON, R. Geolocation and assisted gps. **Computer**, Ottawa, v. 34, n. 2, p. 123-125, Feb. 2001.

FAHMI, P. N. A. et al. 3D-to-2D projection algorithm for remote control using smartphone: enhancing smartphone capability for costless wireless audio visual consumer appliance control. In: INTERNATIONAL CONFERENCE ON ADVANCED INFORMATION NETWORKING AND APPLICATIONS WORKSHOPS, 27., 2013, Barcelona. **Proceedings...** Barcelona: WAINA, 2013. p. 1044-1049.

FIRE, M. et al. Data mining opportunities in geosocial networks for improving road safety. In: CONVENTION OF ELECTRICAL AND ELECTRONICS ENGINEERS IN ISRAEL, 27., 2012, Eilat. **Proceedings...** Eilat: IEEE, 2012. p. 1-4.

FORD, M. C. **Sync**. Disponível em: <http://www.ford.com/technology/sync/>. Acesso em: 10 mar. 2015.

GOOGLE. **Android**. Disponível em: <http://www.android.com/>. Acesso em: 10 mar. 2015.

GOOGLE MAPS. Disponível em: <https://developers.google.com/maps/>. Acesso em: 10 mar. 2015.

GRAILS. **Grails Framework**. Disponível em: <http://grails.org/>. Acesso em: 10 mar. 2015.

GROOVY. Disponível em: <http://groovy.codehaus.org/>. Acesso em: 10 mar. 2015.

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

HARTENSTEIN, H.; LABERTEAUX, K. P. **VANET - Vehicular Applications and Inter-Networking Technologies**. Chichester: Wiley, 2010. v. 1, 431 p.

HAWKINS, I. **Torque:** engine performance and diagnostic tool for automotive professionals and enthusiasts. Disponível em: <http://torque-bhp.com/>. Acesso em: 10 mar. 2015.

IBANEZ, A. G. et al. A performance study of the 802.11p standard for vehicular applications. In: INTERNATIONAL CONFERENCE ON INTELLIGENT ENVIRONMENTS, 7., 2011, Nottingham. **Proceedings...** Nottingham: Nottingham Trent University, 2011. p. 165-170.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Guide for Wireless Access in Vehicular Environments (WAVE):** architecture: IEEE Std 1609.0-2013. New York, 2014. 78 p.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE 1609 working group public site**. Disponível em: <http://vii.path.berkeley.edu/1609wave/>. Acesso em: 10 mar. 2015.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **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 802.11p New York, 2010a. 51 p.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Standard for wireless access in vehicular environments security services for applications and management messages:** IEEE P1609.2/D17. New York, 2013. 289 p.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Standard for wireless access in vehicular environments (WAVE):** identifier allocations: IEEE Std 1609.12-2012. New York, 2012. 20 p.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Standard for wireless access in vehicular environments (WAVE):** multi-channel operation: IEEE Std 1609.4-2010. New York, 2011a. 89 p.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Standard for wireless access in vehicular environments (WAVE):** networking services: IEEE Std 1609.3-2010. New York, 2010b. 144 p.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Standard for wireless access in vehicular environments (WAVE):** over-the-air electronic payment data exchange protocol for intelligent transportation systems (its): IEEE Std 1609.11-2010. New York, 2011b. 62 p.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Trial-use standard for wireless access in vehicular environments (WAVE):** resource manager: IEEE Std 1609.1-2006. New York, 2006. 71 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 15031-6:** road vehicles: communication between vehicle and external equipment for emissions-related diagnostics-part 6: diagnostic trouble code definitions. Geneva, 2005. 136 p.

JSON. Disponível em: <http://www.json.org>. Acesso em: 10 mar. 2015.

KAPLAN, E. **Understanding GPS:** principles and applications. 2nd ed. Norwood: Artech House, 2005. 726 p.

KULLA, E. et al. Performance evaluation of OLSR and BATMAN protocols for vertical topology using indoor stairs testbed. In: INTERNATIONAL CONFERENCE ON BROADBAND AND WIRELESS COMPUTING, COMMUNICATION AND APPLICATIONS, 6., 2011, Barcelona. **Proceedings...** Barcelona: BWCCA, 2011. p. 159-166.

LINDGREN, A.; DORIA, A.; SCHELÉN, O. Probabilistic routing in intermittently connected networks. **SIGMOBILE Mobile Computing and Communications Review**, Toronto, v. 7, n. 3, p. 19-20, 2003.

MICROSOFT. **Windows Phone**. Disponível em: <http://www.windowsphone.com/pt-br>. Acesso em: 10 mar. 2015.

MIKROTIK. **Routerboard**. Disponível em: <http://routerboard.com/>. Acesso em: 10 mar. 2015.

OBD 2. Disponível em: <http://www.obdii.com/>. Acesso em: 10 mar. 2015.

OBDSIM. Disponível em: <http://icculus.org/obdgpslogger/obdsim.html>. Acesso em: 10 mar. 2015

OTHMAN, Z.; AZIZ, W.; ANUAR, A. Evaluating the performance of gps survey methods for landslide monitoring at hillside residential area: static vs rapid static. In: INTERNATIONAL COLLOQUIUM ON SIGNAL PROCESSING AND ITS APPLICATIONS, 7., 2011, Penang. **Proceedings...** Penang: IEEE, 2011. p. 453-459.

POSTGRESQL. Disponível em: <http://www.postgresql.org/>. Acesso em: 10 mar. 2015.

PURI, P.; SINGH, M. A survey paper on routing in delay-tolerant networks. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND COMPUTER NETWORKS, 8., 2013, Chaumuhan. **Proceedings...** Chaumuhan: ISCON, 2013. p. 215-220.

SANCHEZ-IBORRA, R.; CANO, M. D.; GARCIA-HARO, J. Performance evaluation of BATMAN routing protocol for VoIP services: a QoE perspective. **IEEE Transactions on Wireless Communications**, New York, v. 13, n. 9, p. 4947-4958, Sept. 2014.

SINGH, G.; SONG, H. Comparison of hidden markov models and support vector machines for vehicle crash detection. In: INTERNATIONAL CONFERENCE ON METHODS AND MODELS IN COMPUTER SCIENCE, 2., 2010, New Delhi. **Proceedings...** New Delhi: ICM2CS, 2010. p. 1-6.

SINGH, G.; SONG, H. Using hidden markov models in vehicular crash detection. **IEEE Transactions on Vehicular Technology**, New York, v. 58, n. 3, p. 1119-1128, Mar. 2009.

SOCIETY OF AUTOMOTIVE ENGINEERS. **Diagnostic connector equivalent to ISO/DIS 15031-3**. Warrendale, 2001. 23 p.

SPYROPOULOS, T.; PSOUNIS, K.; RAGHAVENDRA, C. S. Spray and wait: an eficient routing scheme for intermittently connected mobile networks. In: ACM SIGCOMM WORKSHOP ON DELAY-TOLERANT NETWORKING, 5., 2005, New York. **Proceedings...** New York: ACM, 2005. p. 252-259.

THOMPSON, C. et al. Using smartphones to detect car accidents and provide situational awareness to emergency responders. In: CAI, Y. et al. (Ed.). **Mobile wireless middleware, operating systems, and applications**. Chicago: Springer, 2010. p. 29-42. (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 48).

TORNELL, S. et al. DTN protocols for vehicular networks: an application oriented overview. **IEEE Communications Surveys Tutorials**, New York, v. 17, n. 2, p. 868-887, 2015.

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

VAHDAT, A.; BECKER, D. **Epidemic routing for partially-connected ad hoc networks:** technical report CS-200006. Duke: Duke University, 2000. Disponível em: <https://scholar.google.com/citations?view_op=view_citation&hl=pt-R&user=r3aWCRUAAAAJ&citation_for_view=r3aWCRUAAAAJ:u5HHmVD_uO8C>. Acesso em: 10 nov. 2014.

VANDENBERGHE, W.; MOERMAN, I.; DEMEESTER, P. On the feasibility of utilizing smartphones for vehicular ad hoc networking. In: INTERNATIONAL CONFERENCE ON ITS TELECOMMUNICATIONS, 11., 2011, Saint Petersburg. **Proceedings...** Saint Petersburg: ITST, 2011. p. 246-251.

WORLD HEALTH ORGANIZATION. **Global status report on road safety**. Geneva, 2013. 318 p.

ZAFOUNE, Y.; KANAWATI, R.; MOKHTARI, A. Mobile agents localization in ad hoc networks: a comparative study of centralized and distributed approaches. In: INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATIONS TECHNOLOGY, 5., 2007, Dhaka. **Proceedings...** Dhaka: ICICT, 2007. p. 269-275.

ZALDIVAR, J. et al. Providing accident detection in vehicular networks through obd-ii devices and android-based smartphones. In: CONFERENCE ON LOCAL COMPUTER NETWORKS, 36., 2011, Bonn. **Proceedings...** Bonn: IEEE, 2011. p. 813-819.

ZHAO, Y. Mobile phone location determination and its impact on intelligent transportation systems. **Intelligent Transportation System**, Piscataway, v. 1, n. 1, p. 55-64, Mar. 2000.