Capítulo

5

Redes Veiculares: Princípios, Aplicações e Desafios

Rafael dos S. Alves[1], Igor do V. Campbell[1], Rodrigo de S. Couto[1], Miguel Elias M. Campista[1], Igor M. Moraes[1], Marcelo G. Rubinstein[2], Luís Henrique M. K. Costa[1], Otto Carlos M. B. Duarte[1] e Michel Abdalla[3]

[1]GTA/PEE/COPPE - UFRJ - Rio de Janeiro, Brasil
[2]PEL/DETEL/FEN - UERJ - Rio de Janeiro, Brasil
[3]Crypto Team - École Normale Supérieure & CNRS - Paris, França

Abstract

Vehicular networks are composed by vehicles and fixed devices placed along the road. Due to characteristics like high node mobility, unstable links and strict latency requirements, many MANET protocols perform poorly on vehicular networks. This short-course aims to present the principles and challenges on the development of vehicular networks. The architecture, network standards, and main applications and projects are described. Additionally, routing, medium access, and physical layer are shown. Finally, general challenges and field experiments are shown in order to motivate future research.

Resumo

Redes veiculares são redes formadas por veículos automotores e por equipamentos fixos geralmente localizados às margens de ruas ou de estradas. Devido a características como alta mobilidade dos nós, enlaces intermitentes e requisitos estritos de latência, muitos protocolos utilizados em redes ad hoc móveis não apresentam desempenho satisfatório em redes veiculares. O objetivo deste minicurso é apresentar os princípios e os desafios presentes no desenvolvimento de redes veiculares. As arquiteturas, os padrões de redes e as principais aplicações e projetos são descritos. O roteamento, o acesso ao meio e a camada física também são focados. Por fim, são apresentados os desafios e experimentos de campo com o intuito de motivar o estudo na área.

5.1. Introdução

Os veículos automotores vêm incorporando diferentes avanços tecnológicos que melhoram a experiência do condutor e dos passageiros. Alguns exemplos são a utilização de sistemas de frenagem, sensores capazes de detectar e advertir o condutor da proximidade de veículos e alarmes de velocidade acima do permitido. Em geral, esses sistemas são baseados em sensores e atuadores cada vez mais sofisticados, que fazem com que o veículo possa detectar sinais no ambiente e informar ao condutor. Esses sistemas, entretanto, são restritos à interação entre o veículo e o condutor.

O próximo passo da evolução tecnológica consiste em sistemas de comunicação que possibilitem a interação entre diferentes veículos. O objetivo principal desses sistemas é possibilitar a comunicação de usuários móveis e oferecer as condições necessárias para que aplicações com diferentes requisitos sejam atendidas satisfatoriamente. Tais aplicações compõem um Sistema Inteligente de Transporte (*Intelligent Transportation System* - ITS) que opera em um ambiente formado por usuários no trânsito. Exemplos dessas aplicações incluem a monitoração cooperativa do tráfego, o auxílio a cruzamentos sem sinalização ou a prevenção de colisões. Além das aplicações específicas de trânsito, vislumbra-se o acesso à Internet em qualquer lugar e a qualquer instante [Li e Wang 2007].

Os sistemas de comunicação entre veículos formam as chamadas redes veiculares. Essas redes são formadas entre veículos automotores ou entre os veículos e a infraestrutura fixa localizada às margens de ruas ou de estradas. As redes veiculares se diferenciam de outras redes sem-fio principalmente pela natureza dos nós, que são compostos por automóveis, caminhões, ônibus etc., com interfaces de comunicação sem-fio, e por equipamentos fixos no entorno das vias. Os nós destas redes apresentam alta mobilidade e trajetórias que acompanham os limites das vias públicas de acesso.

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

Este capítulo apresenta as características das redes veiculares, os principais desafios dessas redes e os principais trabalhos da área. Inicialmente são discutidos os principais padrões em desenvolvimento. Em seguida, o tema é desenvolvido a partir das aplicações até as camadas mais baixas. Por fim, são apresentados resultados práticos obtidos em experimentos de campo.

5.2. Arquiteturas das Redes Veiculares

A arquitetura das redes veiculares define a forma como os nós se organizam e se comunicam. Atualmente, existem três arquiteturas principais: ad hoc puro (*Vehicular Ad hoc NETwork* - VANET), infraestruturada ou híbrida [Alves et al. 2008]. Na arquitetura ad hoc, os veículos comunicam-se sem qualquer suporte externo ou elemento centralizador. Para tanto, os veículos funcionam como roteadores e encaminham tráfego através de múltiplos saltos. Embora essa seja a configuração mais simples, por não exigir ne-

nhum tipo de infraestrutura, ela tem como principal desvantagem a conectividade da rede que depende da densidade e do padrão de mobilidade dos veículos. Para evitar problemas de conectividade, a arquitetura infraestruturada emprega nós estáticos distribuídos ao longo das ruas ou estradas. Esses nós estáticos funcionam como pontos de acesso de redes IEEE 802.11 também em modo infraestruturado. Eles centralizam todo o tráfego da rede, servindo como nós intermediários das comunicações. A vantagem do modo infraestruturado é o aumento da conectividade e a possibilidade da comunicação com outras redes, como por exemplo, a Internet. A conectividade da rede, entretanto, só é garantida mediante um número grande de elementos fixos, o que pode elevar os custos da rede. A arquitetura híbrida é uma solução intermediária entre a ad hoc e a infraestruturada. Na arquitetura híbrida, uma infraestrutura mínima é utilizada para aumentar a conectividade da rede e prover serviços como os de interconexão. Entretanto, há também a possibilidade dos veículos se comunicarem por múltiplos saltos. Nas redes veiculares, o modo ad hoc é conhecido por V2V (*Vehicle-to-Vehicle*) e o modo infraestruturado tem como sinônimo o termo V2I (*Vehicle-to-Infrastructure*). Atualmente alguns pesquisadores referem-se às redes veiculares em geral como VANETs, mesmo quando existe infraestrutura. A Figura 5.1 apresenta as diversas arquiteturas das redes veiculares.

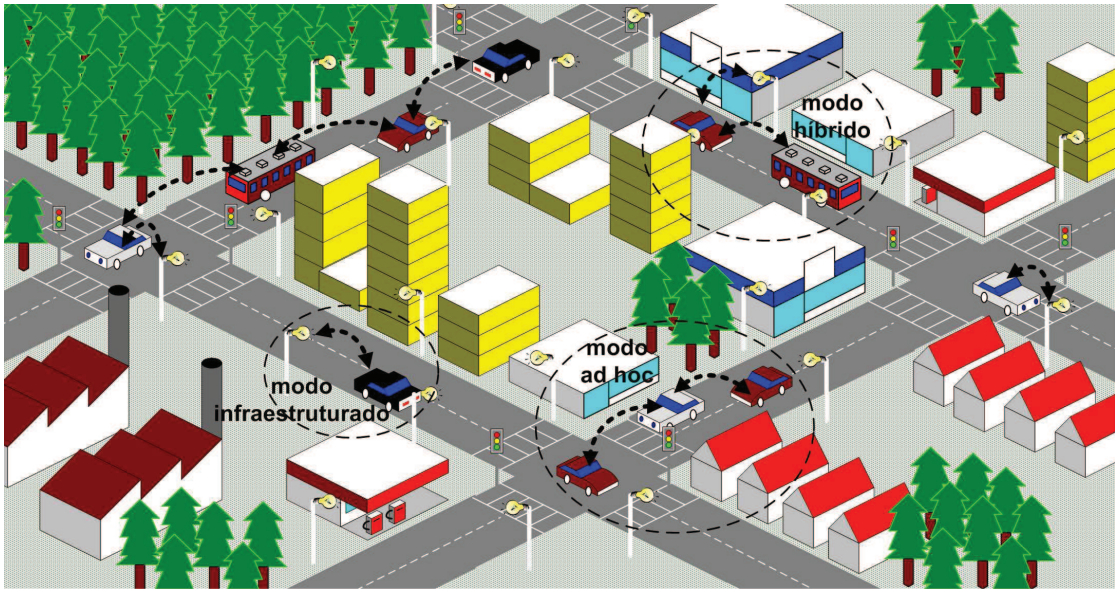


Figura 5.1. O cenário de uma rede veicular.

5.3. Padrões de Redes Veiculares

Os primeiros esforços de padronização das redes veiculares começaram nos Estados Unidos. Em 1999, a FCC (*Federal Communications Commission*) alocou 75 MHz do espectro de frequências, na faixa de 5,9 GHz, para aplicações DSRC (*Dedicated Short Range Communications*). A alocação de canais DSRC está representada na Figura 5.2. A faixa DSRC é livre, porém licenciada: essa faixa é restrita em termos das aplicações e tecnologias utilizadas, porém não é cobrada taxa pela sua utilização. Em outras partes do mundo, também existem esforços para reservar partes do espectro de frequências para comunicações veiculares. Na Europa, as autoridades governamentais estão estudando a

alocação de 30 MHz na faixa de 5 GHz para destiná-los a comunicações veiculares ligadas a segurança e aplicações móveis [Jiang e Delgrossi 2008].

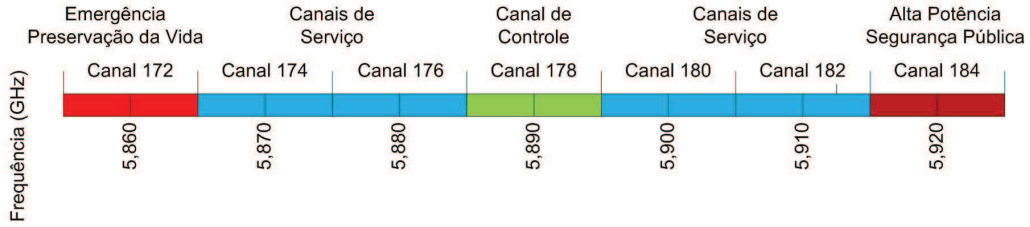


Figura 5.2. Alocação de espectro para aplicações DSRC.

5.3.1. A Arquitetura WAVE

Em 2004, o IEEE iniciou a padronização das comunicações em redes veiculares dentro do grupo de trabalho IEEE 802.11. O padrão, ainda em fase de desenvolvimento, é conhecido como IEEE 802.11p WAVE. A arquitetura WAVE (*Wireless Access in the Vehicular Environment*) é definida em seis documentos: IEEE P1609.1, IEEE P1609.2, IEEE P1609.3, IEEE P1609.4, IEEE 802.11 e IEEE 802.11p. O padrão IEEE 802.11p define as camadas físicas e de controle de acesso ao meio (MAC) para redes veiculares, e é baseado no padrão de redes locais IEEE 802.11a, que opera em uma faixa de frequências próxima à alocada para as redes veiculares. Além disso, a arquitetura WAVE designa uma família de padrões que não se restringe às camadas MAC e física, como apresentado na Figura 5.3. Os padrões da família IEEE 1609 definem outras camadas da pilha de protocolos, incluindo uma camada de rede alternativa à camada IP, características de segurança para aplicações DSRC e operação em múltiplos canais de comunicação.

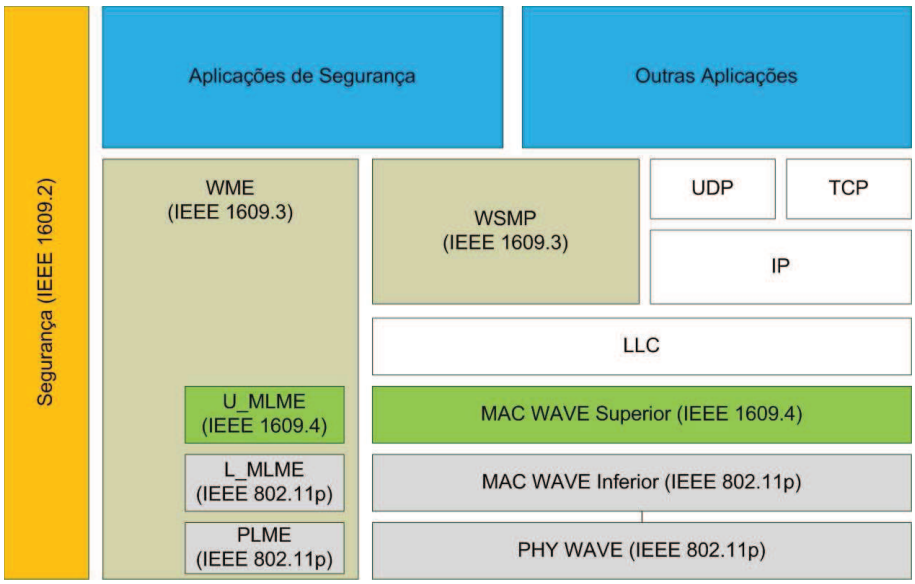


Figura 5.3. A pilha de protocolos WAVE.

Os documentos da família IEEE 1609 definem um conjunto de padrões para a comunicação em ambientes veiculares de comunicação sem-fio, ou ambientes WAVE. O

objetivo principal do IEEE 1609 é prover um conjunto padronizado de interfaces para que diferentes fabricantes de automóveis possam prover comunicações entre veículos (V2V) ou entre veículos e a infraestrutura de comunicação (V2I). Esse passo é importante para que haja interoperabilidade entre todos os dispositivos fabricados. Além da padronização das interfaces, o padrão deve considerar que os veículos estão em altas velocidades e, portanto, as comunicações devem ser completadas em intervalos curtos de tempo para que os requisitos dos Sistemas Inteligentes de Transporte sejam atendidos. A Tabela 5.1 descreve a nomenclatura utilizada nos padrões da família IEEE 1609.

Tabela 5.1. Nomenclatura resumida da arquitetura WAVE.

Dispositivo WAVE	Dispositivo que implementa a subcamada MAC e a camada física de acordo com o padrão WAVE
Unidade de Bordo (*On Board Unit* – OBU)	Dispositivo WAVE móvel capaz de trocar informação com outras OBUs ou RSUs
Unidades de Acostamento (*Road Side Unit* – RSU)	Dispositivo WAVE estacionário que suporta a troca de informação com OBUs
WBSS (*WAVE Basic Service Set*)	Conjunto de estações WAVE consistindo de um provedor de WBSS e zero ou mais usuários de WBSS
WSM (WAVE *Short Message*)	Mensagem curta WAVE, enviada pelo protocolo WSMP
Provedor de WBSS	Dispositivo iniciador de um WBSS ou emissor de WSMs
Usuário de WBSS	Dispositivo associado a um WBSS ou destinatário de WSMs

A arquitetura WAVE é definida pelos padrões da família IEEE 1609, além do IEEE 802.11. O padrão IEEE P1609.1 especifica serviços e interfaces da aplicação de Gerenciamento de Recursos da arquitetura WAVE. O IEEE P1609.2 define formatos e processamento seguros de mensagens. O IEEE P1609.3 especifica os serviços das camadas de rede e de transporte, incluindo o endereçamento e o roteamento. Além disso, o padrão 1609.3 define a MIB (*Management Information Base*) para a pilha WAVE. O padrão IEEE P1609.4 define modificações no padrão IEEE 802.11, para a operação em múltiplos canais. Finalmente, o adendo IEEE 802.11p [Jiang e Delgrossi 2008] define as diferenças específicas do controle de acesso ao meio em ambientes de comunicação WAVE com relação ao IEEE 802.11 tradicional.

Nas subseções a seguir, são descritos em mais detalhes cada um dos padrões.

5.3.1.1. IEEE P1609.1 – Gerente de Recursos

Na arquitetura WAVE, as Unidades de Acostamento (RSUs) são geralmente dispositivos estáticos que hospedam aplicações e provêem serviços, enquanto as Unidades de Bordo (OBUs) executam aplicações que utilizam determinado serviço. Além disso, dispositivos remotamente conectados às Unidades de Acostamento podem também oferecer algum tipo de serviço às Unidades de Bordo, como por exemplo, em uma rede cabeada. O padrão IEEE P1609.1 [IEEE Std 1609.1 2006] especifica serviços e interfaces da aplicação Gerente de Recursos (*Resource Manager* – RM) da arquitetura WAVE, que tipicamente é executada em uma Unidade de Acostamento. O RM se comunica com outra aplicação, executada em uma Unidade de Bordo, chamada de Processador de Comandos de Recursos (*Resource Command Processor* – RCP). Além disso, o Gerente de

Recursos também se comunica com Aplicações do Gerente de Recursos (*Resource Manager Applications* – RMAs), que são aplicações executadas em dispositivos remotamente conectados à Unidade de Acostamento. A função principal do Gerente de Recursos é multiplexar pedidos de múltiplas RMAs, cada uma das quais pode estar se comunicando com RCPs executando em múltiplas Unidades de Bordo. Essa comunicação permite a RMAs ter acesso a recursos, como memória, interfaces de usuários e interfaces com outros dispositivos no veículo, controlados pelo RCP.

O objetivo principal do padrão IEEE 1609.1 é favorecer a interoperabilidade de aplicações WAVE, de forma a simplificar a Unidade de Bordo (OBU) e como consequência reduzir seu custo e/ou aumentar o desempenho. O custo é reduzido, pois a OBU não é obrigada a interpretar mensagens de aplicação. O processamento pode ser movido para a Unidade de Acostamento (RSU) ou para um dispositivo remoto conectado à RSU.

5.3.1.2. IEEE P1609.2 – Segurança

O padrão IEEE P1609.2 [IEEE Std 1609.2 2006] define formatos e processamento de mensagens seguros. O padrão 1609.2 define também as circunstâncias nas quais devem ser usadas mensagens seguras e como essas mensagens devem ser processadas, de acordo com o propósito da troca de mensagens. O padrão define a utilização de ferramentas de segurança tradicionais, como Infraestrutura de Chaves Públicas (PKI) e certificação. O padrão define, por exemplo, como a chave pública de um usuário é usada para criptografar uma mensagem ou como é realizada a autenticação do usuário, sem anonimato.

Além das entidades definidas na Tabela 5.1, o padrão define um subconjunto das Unidades de Bordo, chamados OBUs de Segurança Pública (*Public Safety* OBUs – PSOBUs). As PSOBUs equipam veículos ligados à segurança pública, como viaturas de polícia ou da autoridade de trânsito. As PSOBUs são responsáveis por operar aplicações específicas relacionadas à segurança pública no trânsito, como o controle de sinais de trânsito. O padrão 1609.2 também define as Autoridades de Certificação, entidades responsáveis por autorizar/desautorizar outras entidades, através da emissão/revogação de certificados. O padrão descreve uma aplicação, o Gerente de Segurança, responsável por gerenciar o certificado raiz e armazenar as listas de certificados revogados.

5.3.1.3. IEEE P1609.3 – Serviços de Rede

O padrão IEEE P1609.3 [IEEE Std 1609.3 2007] especifica os serviços das camadas de controle de enlace lógico (*Logical Link Control* – LLC), de rede e de transporte. A comunicação WAVE pode utilizar o IPv6 ou mensagens curtas WAVE (*WAVE Short Messages*), uma alternativa que tem como objetivo maior eficiência. Além disso, o padrão 1609.3 define a MIB (*Management Information Base*) para a pilha WAVE. Como ilustrado na Figura 5.3, a pilha de protocolos WAVE possui um plano de gerenciamento e um plano de dados, descritos a seguir.

O plano de dados define os protocolos de comunicação responsáveis pelo envio de dados gerados pelas aplicações assim como tráfego gerado entre as entidades do plano de

gerenciamento em máquinas diferentes, ou entre entidades de gerenciamento e aplicações.

O plano de gerenciamento é responsável pela configuração e manutenção do sistema. Os serviços do plano de dados são utilizados para transmissão de informação entre os dispositivos. Entidades de Gerenciamento específicas são definidas para algumas camadas, como por exemplo, a Entidade de Gerenciamento da Camada Física (*Physical Layer Management Entity* – PLME) e a Entidade de Gerenciamento da Camada MAC (*MAC Layer Management Entity* – MLME). A Entidade de Gerenciamento WAVE (*WAVE Management Entity* – WME), ilustrada na Figura 5.3 reúne os serviços de gerenciamento. A Entidade de Gerenciamento WAVE fornece interfaces de gerenciamento para todas as entidades do plano de dados, embora isso não esteja explícito na figura.

O plano de dados definido no padrão 1609.3 consiste em quatro serviços: o controle de enlace lógico, o protocolo de rede IPv6, os protocolos de transporte UDP (*User Datagram Protocol*) e TCP (*Transmission Control Protocol*), e o protocolo WSMP (*WAVE Short Message Protocol*), que ocupam as camadas de transporte e de rede.

O plano de gerenciamento implementa os seguintes serviços: registro de aplicações, gerenciamento de WBSSs, monitoramento da utilização de canais, configuração do IPv6, monitoramento do indicador de potência de recepção do canal (*Received Channel Power Indicator* – RCPI) e manutenção da base de dados de gerenciamento.

Protocolos de Comunicação

A arquitetura WAVE possui duas pilhas de protocolos, uma padrão da Internet, baseada no IPv6, e outra baseada no protocolo WSMP, projetado para a comunicação em ambientes veiculares. As mensagens do WSMP podem ser enviadas em qualquer dos canais DSRC, enquanto datagramas IP só podem ser enviados nos canais de serviço (*Service Channels* – SCHs). Além desses tipos de tráfego, quadros de gerenciamento são enviados no canal de controle (*Control Channel* – CCH), sendo seus formatos definidos no padrão IEEE 1609.4. O protocolo WSMP permite que as aplicações controlem diretamente características da camada física, como o canal e a potência de transmissão utilizados para enviar mensagens. A aplicação emissora também fornece o endereço MAC do dispositivo de destino, apesar da possibilidade do uso do endereço de difusão.

Envio de Informação

Há dois tipos de canal de comunicação na arquitetura WAVE, um canal de controle CCH e múltiplos canais de serviço SCH. Por padrão, os dispositivos WAVE operam no canal de controle CCH, que é reservado para aplicações de alta prioridade e mensagens de controle. A utilização dos canais SCH é acordada entre dispositivos dentro de um WBSS. O envio e o recebimento de informação nos canais de controle e de serviço são coordenados, baseados em intervalos de sincronização. Um intervalo de sincronização é composto por um período CCH seguido por um período SCH. No intervalo CCH, os dispositivos monitoram o canal de controle. Durante o intervalo SCH, dispositivos participando de um WBSS trocam mensagens através do canal de serviço especificado para aquele WBSS.

Aplicações WAVE podem enviar informações a outros dispositivos dentro ou fora do contexto de um WBSS. No entanto, fora do contexto de um WBSS, as aplicações podem enviar apenas mensagens curtas WAVE (WSMs), e apenas no canal de controle

(CCH). Já no contexto de um WBSS, é possível o envio de datagramas IPv6 ou WSMs, no canal de serviço associado (SCH) ao WBSS. Um WBSS, de forma similar a um grupo de comunicações multidestinatárias (*multicast*), é estabelecido para cada aplicação específica e deve ser anunciado para que outros dispositivos possam associar-se a ele. Um WBSS pode ser permanente ou temporário. No primeiro caso ele é anunciado periodicamente no canal de controle, já no segundo caso ele é anunciado uma única vez. De forma semelhante a um grupo *multicast*, um WBSS existe apenas enquanto pelo menos um dispositivo WAVE o estiver utilizando.

No contexto de um WBSS, os dispositivos podem ser provedores ou usuários, conforme visto na Tabela 5.1. O provedor do WBSS é responsável por enviar anúncios da existência do próprio WBSS. Os parâmetros do WBSS, incluindo aplicações identificadas por PSIDs (*Provider Service Identifiers*), são incluídos em uma mensagem de anúncio WAVE (WAVE *announcement frame*), enviada no canal de controle. A mensagem de anúncio WAVE indica a existência de aplicações fornecendo serviços. Um usuário que se associa a um WBSS tem acesso a todos os serviços anunciados nesse WBSS.

Endereçamento e Identificação

Na arquitetura WAVE, são utilizados endereços MAC de 48 bits como em outras redes da família IEEE 802. Endereços MAC ponto-a-ponto (*unicast*) e de difusão (*broadcast*) são obrigatórios, enquanto endereços *multicast* são opcionais. Na arquitetura WAVE, o endereço MAC é utilizado principalmente para o envio de informação para uma interface física, através do enlace de rádio. No entanto, endereços MAC são utilizados para outras finalidades. Por exemplo, mensagens de anúncio de serviço podem incluir o endereço MAC do provedor daquele serviço.

Cada dispositivo executando a pilha IP, estação ou roteador, possui pelo menos um endereço IPv6. Endereços IPv6 podem possuir escopos diferentes, na arquitetura WAVE, um dispositivo pode ter endereços locais ao enlace (link-local) e endereços globais. Um endereço IPv6 global usa o mesmo prefixo que a rede IP à qual o dispositivo está conectado, e permite que pacotes com esse endereço de destino sejam roteados através de múltiplas redes. Endereços locais, por outro lado, não precisam ser únicos globalmente e só podem ser usados no escopo de uma única rede (não-roteáveis). Na arquitetura WAVE, o endereço IP do provedor de serviço aparece nas mensagens de anúncio de serviço, caso o protocolo IP seja utilizado. Cada aplicação é unicamente identificada por um número identificador de provedor de serviço (*Provider Service Identifier* – PSID). O PSID e um contexto do provedor de serviço (*Provider Service Context* – PSC) são incluídos nos anúncios de serviço WAVE. O PSC está associado a um identificador PSID e contém informação adicional específica ao serviço, como por exemplo, um número de versão.

Finalmente, uma aplicação deve se registrar com a entidade de gerenciamento WAVE (WAVE *Management Entity* – WME), mostrada na Figura 5.3. A aplicação pode se registrar como provedor ou usuário do serviço, de acordo com as definições da Tabela 5.1.

Internet Protocol version 6

Conforme definido no padrão IEEE 1609.3 [IEEE Std 1609.3 2007], os serviços de rede da arquitetura WAVE devem suportar o protocolo IP versão 6 [Deering e Hinden 1998]. O endereço local ao enlace deve ser obtido a partir do endereço MAC do disposi-

tivo, conforme a RFC 4862 [Thomson et al. 2007]. O padrão também define que a Entidade de Gerenciamento (WME) da Unidade de Bordo (OBU) deve calcular o endereço IPv6 global através de um mecanismo de configuração sem estado, também descrito na RFC 4862. A OBU utiliza para tanto o seu endereço MAC e o prefixo de rede incluído em um anúncio de roteamento WAVE, recebido de uma Unidade de Acostamento (RSU).

WAVE Short Message Protocol

O protocolo WSMP (*WAVE Short Message Protocol*) é uma opção à utilização dos protocolos TCP/UDP e IPv6 em ambientes WAVE. A justificativa de um serviço de rede alternativo é a maior eficiência no ambiente WAVE, onde se espera que a maioria das aplicações exija latência muito baixa e seja não-orientada a conexão. Dessa forma, o WSMP provê um serviço de envio de datagramas à aplicação, substituindo os protocolos de transporte e de rede do modelo OSI.

A função de encaminhamento de mensagens curtas (WSM) do protocolo WSMP é simples. Ao receber um pedido de envio de mensagem da aplicação, o WSMP verifica se o tamanho dos dados é menor que o máximo definido na MIB da Entidade de Gerenciamento, WME. Em seguida, o WSMP repassa a mensagem para a subcamada LLC. No destino, ao receber uma indicação da camada LLC, o WSMP simplesmente repassa a mensagem para a aplicação de destino, baseado no identificador de serviço PSID.

5.3.1.4. IEEE P1609.4 – Operação de Múltiplos Canais

A arquitetura WAVE define a utilização de um canal de controle (CCH) e múltiplos canais de serviço (SCH) [IEEE Std 1609.4 2006]. Ao ser ligado, um dispositivo WAVE deve monitorar o CCH à espera de anúncios de serviço WAVE (WSA) que contém o número do SCH a ser utilizado para um determinado serviço. Senão, no caso em que o dispositivo WAVE é o provedor do serviço, ele deve escolher o SCH de acordo com o conteúdo dos quadros de anúncio de serviço que ele próprio transmite. Além disso, dispositivos WAVE devem monitorar o canal de controle durante períodos de tempo conhecidos como intervalos CCH, à espera de outros anúncios de serviço.

Sincronização

Dispositivos WAVE com apenas uma interface de rádio não podem monitorar o CCH enquanto utilizam um SCH. Nesses casos, é necessária a sincronização entre os dispositivos para que o intervalo CCH seja comum a todos. Assim, são definidos intervalos CCH e SCH utilizando uma referência de tempo absoluto, o UTC (*Coordinated Universal Time*), que é encontrado em dispositivos GPS (*Global Positioning System*) [Hofmann-Wellenhof et al. 2008]. Uma vez sincronizados, os dispositivos WAVE com apenas um rádio são capazes de monitorar o CCH em intervalos específicos. Os intervalos CCH e SCH ocorrem periodicamente, um intervalo CCH seguido de um intervalo SCH. Os tamanhos dos intervalos CCH e SCH são definidos na MIB IEEE 1609.4.

Subcamada MAC

Os padrões IEEE P1609.4 e IEEE 802.11p definem algumas modificações na subcamada MAC descrita no padrão IEEE 802.11 para utilizar os múltiplos canais de

comunicação da arquitetura WAVE.

Primeiramente, é definido um serviço de roteamento de canais para que pacotes de dados vindos da subcamada LLC sejam roteados para um canal específico de acordo com a operação de múltiplos canais na subcamada MAC. Devem existir subcamadas MAC separadas para o canal de controle e de serviço, como no exemplo da Figura 5.4. Os pacotes de dados podem ter prioridades diferentes de acordo com categorias de acesso (AC – *Access Category*) definidas no padrão IEEE 802.11e. Cada categoria de acesso possui parâmetros de controle do acesso ao meio diferentes, como tempos entre quadros e valores mínimo e máximo de janela de contenção.

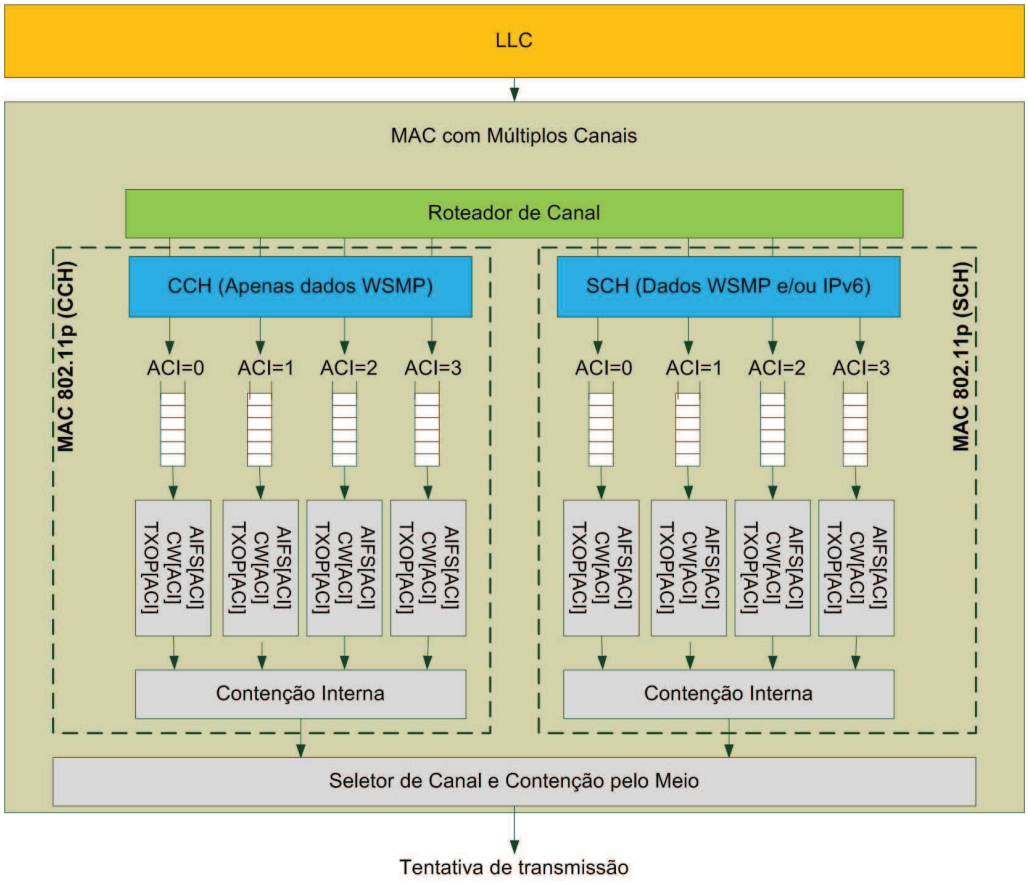


Figura 5.4. Subcamada MAC com múltiplos canais WAVE.

Há dois tipos de quadros na arquitetura WAVE, de dados e de gerenciamento. O principal quadro de gerenciamento é o anúncio WAVE, definido no IEEE 802.11p, que só pode ser transmitido no canal de controle, CCH. Outros quadros de gerenciamento do IEEE 802.11 podem ser transmitidos em um canal de serviço, SCH. Quadros de dados, por outro lado, podem conter mensagens curtas WAVE (WSM) ou datagramas IPv6, o que é indicado no campo `EtherType` do quadro. WSMs podem ser transmitidas no CCH ou SCH, enquanto datagramas IPv6 só são permitidos no SCH. O cabeçalho das WSMs contém o canal, o nível de potência e a taxa de transmissão associados com o pacote, o que permite que a aplicação controle esses parâmetros de camada física para cada WSM individualmente. Além disso, a troca de informações em um SCH só é permitida a dispositivos associados a um WBSS, o que não é necessário no CCH.

5.3.1.5. IEEE 802.11p

O padrão IEEE 802.11p é uma extensão da família de protocolos IEEE 802.11. O IEEE 802.11p se baseia principalmente na extensão "a" do IEEE 802.11, porém, opera na faixa DSRC de 5,9 GHz.

Fundamentos do IEEE 802.11

No padrão IEEE 802.11, um conjunto de estações se comunicando entre si através de um ponto de acesso (AP) é denominado um conjunto básico de serviço, ou BSS (*Basic Service Set*). O conjunto BSS serve para controlar o acesso a recursos e serviços do AP, e para que uma interface de rádio filtre os quadros transmitidos por outras estações que não pertencem ao BSS. Para entrar em um BSS, uma estação deve primeiramente ouvir sondas transmitidas pelo AP, e então executar diversos passos incluindo processos de autenticação e associação. O modo ad hoc de operação segue um procedimento interativo semelhante para o estabelecimento de um IBSS (*Indenpendent BSS*). Os usuários de uma rede IEEE 802.11 identificam um BSS através de uma SSID (*Service Set Identification*) anunciada nas sondas. Por outro lado, as interfaces de rádio identificam um BSS no nível MAC através do BSSID (BSS *Identification*), que é um campo da sonda com formato semelhante ao endereço MAC. Cada BSS deve ser identificado por um BSSID único, que em uma rede infraestruturada é frequentemente escolhido como o endereço MAC do ponto de acesso. Em um IBSS, normalmente é utilizado um endereço MAC administrado localmente, formado por um número aleatório de 46 bits, e 2 bits identificando o endereço como "individual" (em vez de "grupo") e "local" (em vez de "universal"). O padrão IEEE 802.11 define um BSSID especial, com todos os 48 bits em 1. O BSSID coringa pode ser utilizado apenas em quadros de gerenciamento, de tipo *probe request*.

WAVE BSS

A extensão IEEE 802.11p simplifica a entrada de um nó em um BSS (*Basic Service Set*) dada a dinamicidade das redes veiculares. De acordo com o padrão, uma estação em modo WAVE pode transmitir e receber quadros de dados com o BSSID coringa, sem a necessidade de estar associada a um BSS. Nesse modo, podem ser enviadas mensagens urgentes no canal de controle CCH, como mencionado na Seção 5.3.1.3.

As aplicações que demandam o envio de mensagens urgentes podem gastar um tempo excessivo com a associação a um BSS no IEEE 802.11 original. Por exemplo, o tempo entre a entrada em contato e a saída de alcance entre um carro e uma RSU instalada em um poste pode ser por volta de uma dezena de segundos. Nesse caso, os poucos segundos que geralmente são necessários para uma estação se associar a um ponto de acesso no protocolo IEEE 802.11 podem ser excessivos, comparados ao tempo total disponível para a comunicação, o que foi demonstrado em experimentos descritos na literatura [Hadaller et al. 2007].

O padrão IEEE 802.11p define um novo tipo de BSS, o WAVE BSS (WBSS - Tabela 5.1), para reduzir o tempo de associação. Uma estação (RSU ou OBU) cria uma WBSS simplesmente enviando um quadro de anúncio, que pode ser repetido periodicamente ou não (Seção 5.3.1.3). Esse quadro contém todas as informações necessárias para que uma estação conheça os serviços oferecidos naquele WBSS e decida por se asso-

ciar ou não. Caso a estação decida se associar, ela completa o processo de entrada em um WBSS baseada apenas na recepção de um quadro de anúncio. Os processos de associação e autenticação de entrada em um BSS no IEEE 802.11 original foram eliminados, reduzindo a sobrecarga de tempo. Porém, é deixado para as camadas superiores o gerenciamento do grupo referente àquele WBSS assim como a implementação de mecanismos de segurança.

A utilização do BSSID coringa é permitida mesmo para uma estação que pertença a um WBSS, ou seja, configurada com um BSSID específico. Uma estação pertencente a um WBSS pode enviar quadros com o BSSID coringa de forma a alcançar todos os nós em sua vizinhança, por exemplo, em casos onde a segurança esteja em jogo. Por outro lado, estações pertencentes a um WBSS e que, portanto configuraram a camada MAC para filtragem pelo BSSID correspondente, são capazes de receber quadros de outras redes se enviados com o BSSID coringa.

Modificações na Camada Física

O padrão IEEE 802.11p faz poucas alterações na camada física do IEEE 802.11, de forma que sejam mínimas as modificações necessárias no projeto de uma interface de rádio IEEE 802.11a. Se por um lado as modificações no padrão da camada MAC acarretam na maioria das vezes modificações de *software*, grandes modificações na camada física foram evitadas na extensão IEEE 802.11p para que não fosse necessária uma nova tecnologia de radiotransmissão, por exemplo, com novas técnicas de modulação.

A camada física do IEEE 802.11p realizou três modificações principais em relação ao IEEE 802.11a [Jiang e Delgrossi 2008]. A primeira, no IEEE 802.11p os canais têm largura de 10 MHz em vez dos 20 MHz definidos no IEEE 802.11a. Utilizando canais mais estreitos, compensa-se o maior espalhamento do atraso RMS esperado em ambientes veiculares. A divisão por dois na largura do canal é facilmente implementada utilizando OFDM, envolvendo basicamente dobrar os parâmetros de temporização. A segunda modificação diz respeito a requisitos de desempenho do receptor de rádio mais restritivos que no IEEE 802.11a, em especial com relação à rejeição de canais adjacentes. Dessa forma, espera-se reduzir a interferência entre canais, problema significativo em cenários onde há grande densidade de veículos. A terceira modificação, específica à utilização dos rádios IEEE 802.11p nos EUA, no espectro DSRC, define quatro máscaras de transmissão dedicadas a quatro classes de operação distintas.

Apresentados os esforços atuais de padronização das comunicações veiculares. Nas próximas seções, o foco deste capítulo é alterado para os principais desafios e o estado atual de pesquisa na área. Essa abordagem é organizada a partir da camada de aplicação até a camada física.

5.4. Aplicações e Projetos

As aplicações de redes veiculares podem ser divididas em três classes: segurança no trânsito, entretenimento e assistência ao motorista. As aplicações de segurança possuem caráter preventivo e emergencial, onde o principal desafio é divulgar rapidamente as informações para que o condutor tenha tempo para reagir. Nessa classe de aplicações destacam-se a divulgação de informações sobre acidentes, sobre ocorrências no trânsito

e sobre condições adversas de ruas e estradas. Em geral, em aplicações de segurança, a divulgação é limitada aos nós localizados próximos ao perigo. A classe das aplicações de entretenimento inclui adaptações de aplicações da Internet para redes veiculares. Nessa classe se destacam os sistemas de compartilhamento de conteúdo como músicas e filmes por exemplo. Por fim, as aplicações de assistência ao motorista envolvem o recebimento de informações que auxiliem o condutor em buscas ou automatizem serviços. São exemplos aplicações de divulgação de informações turísticas, localização de postos de abastecimento, controle de frotas e cobrança automatizada de pedágio. Nas aplicações de entretenimento e de assistência, a latência de transmissão não é o requisito crítico. Por outro lado, esquemas de divulgação e recebimento das informações devem ser os mais abrangentes possíveis. Além disso, as aplicações de entretenimento possuem diferentes requisitos e devem ser analisadas caso a caso. Assim, uma questão de projeto é determinar se as aplicações de entretenimento devem usar o mesmo canal de comunicação ou um canal separado das aplicações de segurança e assistência ao motorista [Hartenstein e Laberteaux 2008]. A seguir, são apresentadas as principais aplicações e projetos relacionados a redes veiculares.

5.4.1. Segurança no Trânsito

A promessa de aumento de segurança no trânsito tem sido um dos principais incentivos ao desenvolvimento das redes veiculares. Em geral, as aplicações de segurança têm por objetivo reduzir o número e a gravidade dos acidentes através da troca de informações entre os veículos. Essas informações podem ser apresentadas ao motorista ou utilizadas para acionar um sistema ativo de segurança. Essas aplicações impõem requisitos estritos de latência e confiabilidade para as mensagens, exigindo características diferenciadas dos protocolos de camadas inferiores. Além disso, as aplicações precisam ser robustas à inserção de mensagens falsas e lidar com informações conflitantes.

Muitos acidentes de trânsito podem envolver veículos parados, lentos ou desgovernados. Uma maneira de evitar esses acidentes é através do emprego de mensagens periódicas que indiquem a posição, a velocidade e a direção dos veículos. Outra abordagem é a utilização de mensagens assíncronas disparadas somente quando um mecanismo de emergência é acionado. O CCA (*Cooperative Collision Avoidance*) [Biswas et al. 2006] é um exemplo de aplicação nessa categoria que tem por objetivo evitar colisões utilizando uma abordagem cooperativa. O CCA envia mensagens em múltiplos saltos avisando aos motoristas da ocorrência de uma situação de emergência. Essa abordagem também pode ser utilizada em situações em que o motorista não possui visão completa. Por exemplo, o motorista pode ter ciência de veículos a sua frente através de sondas em situações de neblina ou de chuvas intensas.

Nos casos em que o acidente não pôde ser evitado, a utilização de mensagens informando a ocorrência evita que veículos próximos à colisão se envolvam no acidente, o que agravaria a situação. Além disso, o envio das mensagens pode acelerar o chamado aos serviços de emergência sem a necessidade da intervenção humana. Em situações onde três ou mais veículos se deslocam em uma via expressa e o primeiro da fila freia de forma brusca, cada veículo só conheceria a situação de perigo após o carro imediatamente à sua frente também frear. Nesse caso, a propagação da informação estaria condicionada à atenção dos motoristas e ao tempo de reação de cada um deles que varia entre 0,7 e

1,5 segundos [Green 2000]. Um sistema de aviso poderia alertar todos os outros veículos com pequeno atraso, possibilitando maior tempo para redução da velocidade.

Existem ainda aplicações onde a troca de informações entre veículos permite a realização segura de manobras no trânsito, prevenindo acidentes. Por exemplo, em situações em que os veículos precisam realizar uma mudança de faixa, mensagens podem ser trocadas para evitar colisões laterais [Chen e Cai 2005].

Além das comunicações entre veículos, as comunicações com a infraestrutura podem reduzir o número de colisões em cruzamentos [VSCC 2005]. Através de sondas periódicas, os veículos podem avisar RSUs instaladas em cruzamentos sobre sua posição e velocidade. Com esses dados, a RSU pode calcular uma possível colisão e alertar os envolvidos sobre o risco iminente. Outra abordagem é o envio de sondas pelas RSUs informando o estado de sinais, avisando motoristas desatentos sobre a possível violação da sinalização. Tipicamente, avisos são colocados em locais com curvas acentuadas para que o motorista reduza a velocidade. Entretanto, a escolha da velocidade depende somente do julgamento do motorista. Nessa situação, uma RSU próxima à curva poderia inferir se a velocidade utilizada pode representar perigo, baseando-se em informações como características do veículo, condições do tempo e da estrada, e a geometria da curva.

Algumas instituições promoveram esforços conjuntos de pesquisa e desenvolvimento de aplicações de segurança no trânsito. O projeto CarTALK 2000 [Reichardt et al. 2002] teve como objetivos finais projetar, testar e avaliar sistemas para segurança na direção utilizando tanto comunicações entre veículos quanto entre veículos e infraestrutura. O projeto abordou problemas relacionados tanto à direção segura quanto ao conforto do condutor. O projeto CarTALK 2000 foi realizado em conjunto com o projeto FleetNet – *Internet on the Road* [Franz et al. 2005]. Este projeto desenvolveu trabalhos que cobriam aspectos das camadas física, de acesso ao meio e de roteamento, além de aplicações tendo como direção o aumento da segurança no trânsito.

O projeto de pesquisa PreVENT [Schulze et al. 2005] tem como um dos objetivos a congregação de organizações nacionais europeias e suas iniciativas de transporte seguro. A visão do projeto é criar uma zona segura ao redor dos veículos através do desenvolvimento, integração e demonstração de um conjunto de funções de segurança complementares. Ainda no contexto europeu, o SAFESPOT [Vivo et al. 2007] é um projeto de pesquisa que visa entender de que forma veículos e vias inteligentes podem cooperar para aumentar a segurança das estradas. O COMeSafety é um projeto que visa coordenar e consolidar diversos esforços de pesquisa voltados para segurança em redes veiculares desenvolvidas no contexto europeu [COMeSafety 2009]. Além disso, busca-se harmonização entre projetos de pesquisa ao redor do mundo e a disseminação das informações aos interessados (fabricantes de automóveis e de dispositivos de comunicação, autoridades nacionais, operadores de vias e o público em geral).

Nos Estados Unidos, o projeto VSC (*Vehicle Safety Communications*) [VSCC 2005] reuniu indústrias e instituições governamentais para identificar aplicações de segurança e determinar seus requisitos. Por outro lado, o projeto PATH [Shladover et al. 1991] é uma colaboração entre o Departamento de Trasportes da Califórnia (Caltrans), a Universidade da Califórnia, outras instituições acadêmicas públicas e privadas, e a indústria. O principal objetivo é usar tecnologia para aumentar a capacidade e a segurança das au-

toestradas, e reduzir congestionamentos, poluição do ar e consumo de energia.

5.4.2. Entretenimento

A maioria das aplicações de entretenimento propostas para redes veiculares está associada à ubiquidade de acesso à Internet. A cada dia, os usuários se tornam mais dependentes da rede e desejam acessá-la a qualquer instante e em qualquer lugar. Por isso, é necessário adaptar as aplicações mais usadas na Internet de acordo com as características das redes veiculares. Dentre as principais aplicações destacam-se os serviços de mensagens instantâneas, a troca de músicas e filmes e a distribuição de áudio e vídeo.

Muitas aplicações para redes veiculares defendem o uso da arquitetura ad hoc por dispensar elementos centralizadores e por possibilitar a comunicação entre veículos sem o intermédio de pontos de acesso. Além disso, no caso infraestruturado, manter a rede totalmente conectada requer um alto custo de instalação e manutenção [Lee et al. 2007]. A partir desses argumentos, muitas aplicações de entretenimento preferem utilizar os sistemas par-a-par ao modelo cliente-servidor, que é centralizado. A questão é que frequentemente essas aplicações necessitam de acesso à Internet, que só é possível através de pontos fixos de interconexão ligados a uma infraestrutura cabeada. Esses pontos fixos são nós especiais que também pertencem à rede veicular e são chamados de *gateways*.

Na Internet, uma das aplicações típicas e de grande sucesso é o compartilhamento de conteúdo baseado em sistemas par-a-par. Nas redes veiculares, essa aplicação é chamada de aplicação carro-a-carro (*Car-to-Car* - C2C) [Prinz et al. 2008]. A ideia básica é que os veículos troquem pedaços de arquivos desejados entre si, como ocorre no protocolo BitTorrent [Cohen 2008] usado na Internet. Para isso, os nós interessados em um dado arquivo se auto-organizam, constroem uma rede sobreposta (*overlay*) na camada de aplicação e trocam pedaços desse arquivo entre si. Um nó pode receber pedaços do arquivo de diferentes fontes ao mesmo tempo. O BitTorrent em sua forma tradicional não é eficiente para redes sem-fio, porque a diferença entre as topologias da rede sobreposta e da rede física pode aumentar o número de comunicações que usam múltiplos saltos. Logo, um nó vizinho de outro nó na rede sobreposta pode estar mais distante desse nó na rede física. Para reduzir esse problema, o BitTorrent deve ser adaptado. Busca-se, então, mapear a topologia da rede sobreposta e a da rede física para reduzir o número de comunicações através de múltiplos saltos e, assim, aumentar a eficiência da rede durante a transferência de arquivos.

Uma das propostas de sistemas par-a-par para compartilhamento de conteúdo em redes veiculares é o SPAWN [Nandan et al. 2005]. Diz-se que tal protocolo é adaptado para as redes sem-fio, pois utiliza mecanismos diferentes dos do BitTorrent para a descoberta de novos pares, para a seleção de pares e para o encaminhamento dos pedaços dos arquivos. A Figura 5.5 ilustra o funcionamento do SPAWN.

Quando um novo nó entra no alcance de um *gateway* ele solicita o arquivo desejado (passo 1). Se o *gateway* possui tal arquivo em seu *cache*, um pedaço do arquivo é enviado para o nó juntamente com uma lista de nós que recentemente solicitaram esse mesmo arquivo (passo 2). Esse processo centralizado de descoberta de pares é similar ao do BitTorrent. Enquanto um nó está no alcance do *gateway*, ele recebe novos pedaços (passo 3). Ao sair do alcance do *gateway*, um nó busca novos pares para trocar os pedaços

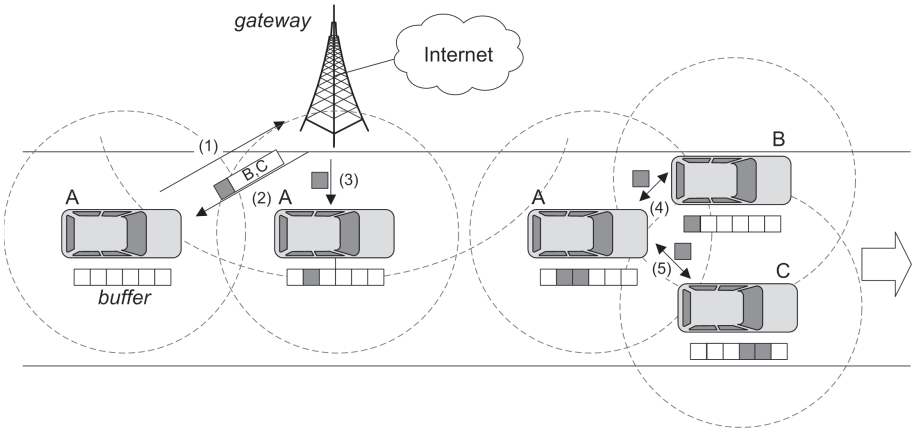


Figura 5.5. O funcionamento do SPAWN [Nandan et al. 2005].

do arquivo. Entretanto, o conjunto de pares enviado pelo *gateway* pode não ser suficiente para o funcionamento eficiente do sistema. Por isso, introduz-se um mecanismo descentralizado de descoberta de pares que aproveita a característica de difusão das transmissões sem-fio. Esse é o diferencial para o protocolo BitTorrent tradicional. Com o SPAWN, os nós enviam mensagens de atualização em difusão contendo o identificador do arquivo e um mapa de *buffer*, que indica quais pedaços desse arquivo o nó possui. Como as mensagens são enviadas usando a difusão implementada pela camada MAC, os nós dentro do alcance da transmissão escutam tais mensagens e podem assim descobrir os outros pares do sistema. Vale ressaltar que o protocolo implementa mecanismos para controlar a frequência de envio de mensagens de atualização [Nandan et al. 2005]. No exemplo da Figura 5.5, o nó A ao sair do alcance do *gateway* troca pedaços com os nós B e C (passos 4 e 5). O SPAWN define ainda um algoritmo de seleção de pares baseado na distância entre os nós. Esse é o ponto-chave do protocolo. Além do identificador de arquivo e do mapa de *buffer*, as mensagens de atualização contêm uma estampilha de tempo, que indica quando foram originadas, e uma lista de identificadores dos nós que processaram essa mensagem anteriormente. Com isso, é possível determinar a distância em número de saltos de um nó para um dado par que possui um pedaço desejado. Um nó seleciona como parceiros os nós dos quais está mais próximo. A justificativa para adotar tal estratégia está relacionada ao desempenho das redes sem-fio de múltiplos saltos, principalmente do TCP (Seção 5.7.3). Quanto menor o número de saltos, mais eficiente é o TCP. O SPAWN também se baseia na distância dos pares para implementar diferentes algoritmos de escalonamento de pedaços a serem solicitados. Para isso, o algoritmo clássico do BitTorrent, que solicita primeiro os pedaços menos populares, é adaptado. No SPAWN, os pedaços mais raros ainda são os primeiros solicitados, mas a distância dos nós que possuem tais pedaços é usada como critério de desempate. Busca-se com isso diminuir o número de saltos necessários para aumentar o reuso espacial e reduzir a sobrecarga de roteamento.

O CarTorrent [Lee et al. 2007] é uma extensão do SPAWN. Nesse protocolo, as mensagens de atualização têm seu alcance limitado, ou seja, são encaminhadas somente até atingirem os nós localizados a k saltos de distância do nó que originou a mensagem. Assim como no SPAWN, a distância também é adotada como critério de desempate no algoritmo de escalonamento. Por outro lado, no CarTorrent, os nós podem enviar

solicitações de arquivos para outros nós da rede e não somente para os *gateways*. Um nó ao receber uma solicitação a encaminha para o *gateway* caso esteja dentro do seu alcance. Do contrário, a mensagem é armazenada até que haja conexão com um *gateway*. O CarTorrent foi implementado e avaliado em uma rede de testes real [Lee et al. 2007].

O CodeTorrent [Lee et al. 2006] é outro protocolo par-a-par de compartilhamento de conteúdo em redes veiculares. Com esse protocolo, um nó escolhe como parceiros[1] somente os seus vizinhos de um salto na rede física para evitar a comunicação em múltiplos saltos. O principal problema dessa restrição é que nem sempre os vizinhos de um nó estão interessados nos mesmos pedaços do arquivo. Para contornar esse problema, aproveita-se a comunicação em difusão característica das redes sem-fio e utiliza-se a codificação de rede (*network coding*). Dessa forma, no CodeTorrent, os nós trocam quadros codificados (*coded frames*) e não mais pedaços do arquivo. Um quadro codificado c é definido como uma combinação linear dos n pedaços que compõem o arquivo armazenado pela fonte. Além disso, o cabeçalho de cada quadro c contém um vetor de codificação para que o receptor consiga decodificar o quadro recebido. Dessa forma, para recuperar os n pedaços do arquivo, um nó tem que receber mais de n quadros codificados com vetores de codificação linearmente independentes entre si. Devido à comunicação em difusão, os vizinhos que não estão envolvidos diretamente em uma transmissão entre dois nós também "escutam" os quadros codificados enviados e, dessa forma, recebem mais quadros do que requisitam. Quanto mais quadros recebidos, maior a probabilidade de se obter n vetores de codificação linearmente independentes e, consequentemente, maior é a velocidade de transferência de um arquivo. Essa é a principal vantagem do uso da codificação de rede.

O V3 [Guo et al. 2005] é um sistema para difusão de vídeo ao vivo veículo-a-veículo (V2V). Diferentemente dos sistemas de compartilhamento de conteúdo descritos anteriormente, a requisição do vídeo não é enviada inicialmente para um *gateway* localizado às margens da via. Toda a comunicação se dá entre os próprios veículos. Os grandes desafios dessa proposta estão relacionados à frequência de particionamento da rede e à mobilidade e à transitoriedade das fontes de vídeo. Para suplantar esses desafios, o V3 implementa uma estratégia de armazenar-transportar-e-encaminhar (*store-carry-and-foward*) para transmitir o vídeo em redes particionadas e um mecanismo de sinalização para monitorar continuamente as fontes de vídeo. A Figura 5.6 ilustra o funcionamento do sistema V3. Assume-se que os veículos possuem câmeras, dispositivos de GPS e espaço suficiente para armazenar o vídeo transmitido. No cenário ilustrado, o veículo r deseja receber o vídeo capturado na região A. Veículos que estão momentaneamente nessa região podem capturar o vídeo e transmiti-lo para r. Entretanto, cada veículo permanece em A por um curto período de tempo e, por isso, o receptor r deve receber o vídeo de múltiplas fontes para manter a continuidade da reprodução. O V3 funciona da seguinte forma. O receptor r envia uma mensagem de requisição do vídeo na direção da região A. Um veículo ao receber uma requisição deve determinar em que zona se encontra. Primeiramente, ele calcula se está na zona de encaminhamento, ou seja, entre o receptor e a região de destino. Se ele se encontra nessa zona, a requisição é encaminhada para todos os veículos que estão dentro do alcance do seu rádio. Caso contrário, a requisição é armazenada, e o veículo recalcula a zona em que se encontra a cada α unidades de tempo. Se o veículo

[1] Um nó só troca pedaços de um arquivo com os seus parceiros.

se encontra na região de destino *A*, que é a região física da qual *r* deseja receber o vídeo, e recebe a requisição ele inicia a captura do vídeo e o envia de volta para o receptor *r*. Os veículos que estão entre *r* e *A* e que receberam a requisição também se preparam para iniciar a transmissão de vídeo assim que entrarem na região de destino.

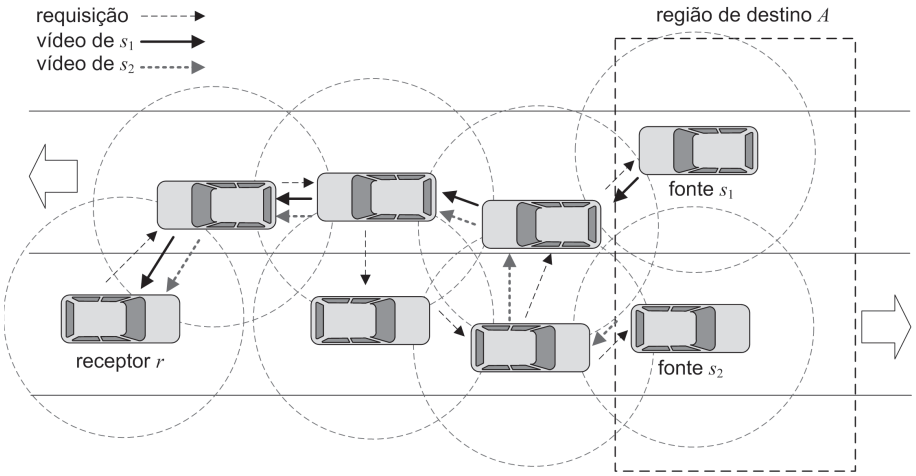


Figura 5.6. O funcionamento do sistema V3 [Guo et al. 2005].

O V3 define uma zona de encaminhamento, na qual um veículo deve estar para ser capaz de encaminhar o vídeo, ou seja, entre a região de destino e o receptor. Como visto anteriormente, o vídeo é transmitido segundo a estratégia armazenar-transportar-e-encaminhar. Primeiramente, um veículo fonte encaminha o vídeo para os veículos que estão no seu raio de alcance. Um veículo que recebe e armazena o vídeo se torna um veículo de dados. Porém, nem todos os veículos de dados encaminham o vídeo. Um veículo de dados *d* só encaminha o vídeo que possui para outro veículo *v*, se *d* estiver na zona de encaminhamento e se *v* não armazena nenhum dos dados que serão enviados por *d*. Se o encaminhamento de *d* para *v* for bem sucedido, *v* se torna um veículo de dados e tentará encaminhar o vídeo para os veículos dentro do seu alcance. Esse processo é repetido até que o vídeo alcance o veículo receptor *r*.

Atualmente, existem diversos projetos que desenvolvem aplicações de entretenimento para redes veiculares [Reichardt et al. 2002, Festag et al. 2008]. Um dos projetos é o Drive-thru Internet [Ott e Kutscher 2004] desenvolvido pela Universidade de Tecnologia de Helsinki cujo objetivo é prover acesso à Internet a usuários em veículos que trafegam em estradas a velocidades que podem atingir 200 km/h. Outro projeto liderado pela Daimler-Chrysler desenvolve uma aplicação de distribuição de rádio cujo objetivo principal é aumentar o número de estações disponíveis para os usuários, permitindo também o acesso a estações de rádio disponibilizadas na Internet [Ramsey 2009]. O projeto prevê também a criação de estações pelos próprios usuários de dentro dos veículos para, por exemplo, disponibilizar o conteúdo de seus tocadores de músicas pessoais para outros usuários.

5.4.3. Assistência ao Motorista

A principal finalidade das aplicações de assistência ao motorista é auxiliar a condução do veículo a partir da disponibilização de informações úteis. Essas informações

são adquiridas a partir de serviços que podem ser oferecidos ao condutor em momentos oportunos ou podem ser de fácil acesso através de procedimentos de busca. Dentre alguns exemplos pode-se citar: aviso de estacionamentos, disseminação de informações de vias, controle de tráfego, auxílio a cruzamentos, condução conjunta de veículos, localização em mapas, aumento da visibilidade e veículos sem condutor humano.

Dentre as aplicações desta classe, as aplicações de indicação de vagas de estacionamento vêm recebendo bastante atenção. Um dos argumentos utilizados é que além de conveniente, ela pode reduzir os problemas de congestionamento nas cidades. Um trabalho realizado em uma cidade no distrito de Munique, Alemanha revela que 44% de todo o tráfego de veículos é devido à busca de lugares para estacionar. Isso pode gerar prejuízos anuais da ordem de milhões de Euros e ainda provocar muitas horas perdidas no trânsito [Caliskan et al. 2006]. Panayappan et al. desenvolveram uma solução para controle e divulgação de vagas de estacionamento [Panayappan et al. 2007]. Essa solução divide uma área onde há vagas de estacionamento em pequenas zonas, de forma que cada zona seja gerenciada por uma Unidade de Acostamento (RSU). Cada RSU controla a posição e o estado das vagas na zona em que se encontra e, quando um veículo se aproxima dela, ela informa sua posição, obtida através de um receptor GPS, e verifica para onde o motorista pretende ir. Assim, a RSU verifica se existe alguma vaga livre próxima ao destino pretendido e, caso exista, informa ao motorista. Quando um veículo se encaminha para alguma vaga, ele verifica a presença de outros veículos ocupando outras vagas utilizando sensores ao redor do veículo. As informações coletadas sobre o estado das vagas próximas são enviadas à RSU. Quando um veículo sai de uma vaga, ele informa à RSU a liberação.

Um dos problemas da aplicação de Panayappan et al. é não considerar o número mínimo de usuários necessários para que o sistema funcione. Caliskan et al., por outro lado, propõem uma solução para informar aos motoristas a disponibilidade de vagas de estacionamento de forma eficiente mesmo quando apenas 5% dos veículos utilizam redes veiculares [Caliskan et al. 2006]. Essa solução utiliza uma Unidade de Acostamento localizada em áreas onde há vagas para o estacionamento. Essas unidades verificam a disponibilidade das vagas e disseminam a informação. Tais informações são divididas em informações atômicas, que representam a disponibilidade e a localização de cada vaga, e informações agregadas, que representam a disponibilidade de um conjunto de vagas em uma mesma área. A informação atômica é disseminada periodicamente em difusão pelas RSUs para os veículos que se encontram dentro de alcance, que a repassam para os veículos que estiverem próximos. As informações atômicas vão sendo agregadas pelos veículos e passadas para os veículos que estão mais distantes daquela área de estacionamento para que estes obtenham apenas a informação da existência ou inexistência de vagas naquela área. A vantagem da agregação das informações é a redução do consumo de banda passante.

Outra aplicação importante de auxílio ao motorista é a disseminação de informações sobre as condições das vias. Essas aplicações buscam reduzir o tempo de espera dos motoristas em congestionamentos, apresentando rotas alternativas que evitam áreas com tráfego lento. Essas aplicações possuem ainda o efeito indireto de redução da poluição ambiental e podem ser utilizadas para evitar áreas de risco.

O TrafficView é um sistema de disseminação de dados de tráfego de veículos [Nadeem et al. 2004]. Nessa aplicação, cada veículo mantém informações próprias sobre posição e velocidade, além das recebidas de outros nós da rede. No TrafficView, cada nó dissemina todas as informações conhecidas apenas aos nós vizinhos, que de tempos e tempos repetem a mesma operação. Cada nó adquire as informações próprias de posição e velocidade através de um GPS e de uma interface OBD (*On-Board Diagnostic System*). Tais informações são enviadas em períodos de transmissão e quando um veículo as recebe, ele as verifica e as grava em uma base de dados caso elas sejam mais recentes que as já existentes. Como as informações recebidas podem ser uma agregação da posição e da velocidade de mais de um veículo, a verificação da validade é realizada para cada caso. As informações armazenadas passam por um módulo de interface de usuário que apresenta as informações utilizando mapas e áudio.

O SOTIS (*Self-Organizing Traffic Information System*) é um sistema para o monitoramento e disseminação da situação do tráfego [Wischhof et al. 2003]. O objetivo do SOTIS é semelhante ao do TrafficView, mas foi desenvolvido com base em sistemas de informação de tráfego (*Traffic Information Systems* - TISs) convencionais, que utilizam sensores nas pistas, central de informações e estação de transmissão de rádio FM ou redes de telefonia celular. A utilização de redes veiculares, ao invés de um sistema centralizado, provê diversas vantagens aos TISs, tais como eliminação da necessidade de muitos sensores nas pistas, o funcionamento do sistema em áreas sem sensores, a redução do tempo de divulgação das informações de tráfego, entre outras. Nesse sistema, os veículos transmitem pacotes periódicos contendo as seguintes informações: posição e velocidade do veículo, identificação da via em que o veículo se encontra, estampilha de tempo indicando a hora em que o pacote foi transmitido, identificação da via analisada, início e fim do trecho e hora em que a análise foi realizada. A frequência de envio dos pacotes pode variar de acordo com a prioridade da informação. Na ocorrência de emergências, um pacote contendo a hora, o tipo e a descrição da emergência é enviado imediatamente, de forma que o protocolo de controle de acesso ao meio garanta o acesso imediato ao canal de comunicação.

Rizvi et al. propõem uma aplicação que utiliza redes veiculares para informar aos motoristas a aproximação de veículos de emergência (*Emergency Service Vehicles* - ESVs), facilitando a passagem deles até seus destinos [Rizvi et al. 2007]. Cada ESV envia periodicamente mensagens em difusão contendo o identificador do veículo, o tipo de ESV (carro de polícia, ambulância etc.), seus pontos de origem e de destino, a identificação da rota (lista das vias pertencentes àquela rota), a velocidade ideal para alcançar o destino, sua posição atual e a estampilha de tempo de envio da mensagem pelo ESV. Dessa forma, os veículos recebem informações completas sobre o ESV que está se aproximando, auxiliando aos motoristas a tomarem a melhor decisão com antecedência.

Outro tipo de aplicação bastante útil é o de auxílio em cruzamentos, onde as redes veiculares servem para obter a posição dos veículos e realizar a comunicação com elementos de sinalização como semáforos [VSCC 2005]. Com essas informações, a aplicação calcula a velocidade ideal para que o motorista alcance cada cruzamento sem que precise aguardar o semáforo abrir ou algum veículo passar. A vantagem dessa aplicação é redução do tempo de viagem, do desgaste do veículo e dos gastos de combustível.

As aplicações de condução conjunta de veículos (*vehicle platooning*) são utilizadas para os veículos que viajam juntos, reduzindo o espaço entre eles [Tank e Linnartz 1997]. Por reduzir o espaço entre os veículos, o conjunto de veículos permite uma viagem mais segura e com menores chances de ocorrências de congestionamentos. Essas aplicações realizam a troca de informações de posição e velocidade dos veículos do conjunto, permitindo um controle rápido e preciso da distância entre os veículos.

A utilização de mapas para identificação de rotas já é bastante comum em veículos graças a equipamentos receptores de GPS cada vez mais avançados. Além disso, existem trabalhos que propõem aplicações para redes veiculares que utilizam os mapas digitais , apresentando a ocorrência de colisões de veículos, a posição de postos de combustível, a movimentação de veículos próximos do usuário e muitos outros recursos [VSCC 2005]. A combinação de aplicações diversas com os mapas digitais permite a transferência de informações para os motoristas de forma bastante conveniente, como por exemplo, evitando que o motorista se distraia.

As aplicações de aumento de visibilidade mostram aos motoristas a posição de veículos, construções e objetos na pista em situações de pouca visão, como em fortes neblinas [VSCC 2005]. A apresentação das informações é feita com a adição de informações visuais às imagens reais, sem que a visão do motorista seja prejudicada. Atualmente, já existem veículos que utilizam sistemas desse tipo com mecanismos para visão noturna. As redes veiculares podem contribuir nas aplicações desse tipo ao acrescentarem informações além do campo de visão do motorista. Tais informações podem ser recebidas, por exemplo, através de comunicações por múltiplos saltos.

O último tipo de aplicação para a assistência do motorista apresentada é a condução de veículos sem a intervenção humana. Tais sistemas são bastante sofisticados, pois permitem o tráfego de veículos de maneira totalmente autônoma. Esses sistemas obtêm informações pela rede sobre as condições de trânsito e utilizam sistemas cognitivos para identificá-las e tomar as melhores decisões para alcançar seus destinos. Apesar de já existirem projetos para o desenvolvimento de sistemas desse tipo, como o projeto europeu Eureka-PROMETHEUS [Xie et al. 1993], a solução para o pleno funcionamento desses sistemas em vias de tráfego normais ainda está distante.

5.5. Roteamento

O cálculo de rotas em redes veiculares é uma tarefa desafiadora devido à alta mobilidade dos nós da rede e à instabilidade dos enlaces sem-fio. A seguir, os principais protocolos de roteamento encontrados na literatura são classificados em: topológicos, geográficos, oportunísticos e de disseminação de informações.

5.5.1. Baseado em Topologia

Os protocolos baseados em topologia encontram o melhor caminho entre qualquer par origem-destino da rede. Tipicamente, o melhor caminho é aquele que oferece o menor custo de acordo com as métricas utilizadas. Esses protocolos podem ser divididos em proativos, reativos e híbridos. Os protocolos proativos mantêm uma lista periodicamente atualizada de rotas para cada um dos nós da rede. Por outro lado, os protocolos reativos só constroem a rota quando há dados a enviar. Os protocolos híbridos usam uma

solução intermediária, por exemplo, atualizando sob demanda as rotas mais utilizadas. O grande número de protocolos de roteamento baseados em topologia já desenvolvidos para as redes ad hoc móveis aliado às semelhanças entre essas redes e as redes veiculares tornou a utilização de protocolos das redes ad hoc a solução mais simples. Porém, alguns trabalhos têm criticado o baixo desempenho desses protocolos no contexto das redes veiculares [Taleb et al. 2007, Naumov et al. 2006].

A utilização de protocolos propostos para as redes ad hoc móveis acarreta uma alta carga de controle devido à alta mobilidade dos nós nas redes veiculares. De acordo com [Naumov et al. 2006], entre 70 e 95% do tráfego gerado pelo protocolo AODV (*Ad hoc On-Demand Distance Vector*) [Perkins et al. 2003] é dedicado à difusão de mensagens de requisição de rota quando testado em ambientes veiculares. Para reduzir esse problema, Naumov et al. propõem um mecanismo de difusão, chamado de PGB (*Preferred Group Broadcasting*), que reduz o número de mensagens de controle. No PGB cada nó, ao receber uma mensagem, classifica-se em um dos três grupos definidos (PG, IN e OUT). Os nós do grupo IN são os mais próximos, os do grupo OUT os mais distantes e do grupo PG, de distâncias intermediárias ao nó de origem. Em seguida, cada nó aguarda um período, dependente de sua classificação, antes de decidir por retransmitir a mensagem.

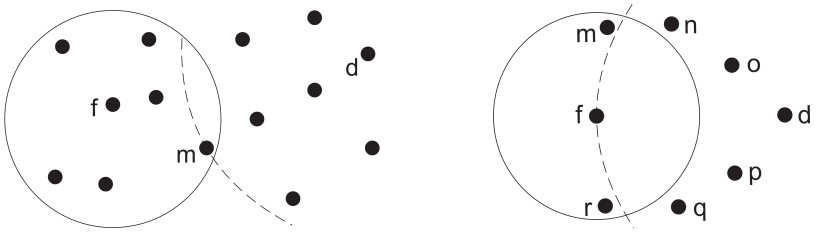
O PBR (*Prediction-Based Routing*) [Namboodiri e Gao 2007] é outro exemplo de protocolo baseado em topologia. Ele tem como principal objetivo prover acesso à Internet aos nós da rede veicular. Para tal, assume-se que parte dos veículos possui uma interface conectada a uma rede de acesso como WiMax ou celular 3G. Esses veículos atuam como *gateways* móveis, acessados em múltiplos saltos pelos outros nós da rede. A construção da rota é realizada sob demanda através de pacotes de requisição de rota, nos quais cada nó intermediário insere informações de posição, de velocidade e de sentido. Para reduzir o número de pacotes em difusão, os nós intermediários só encaminham um pacote de requisição se este for mais novo que o último recebido para o par fonte-destino. Caso o número de sequência seja igual a outro já recebido, a mensagem só é encaminhada se todos os nós presentes na rota se deslocarem no mesmo sentido. Com isso, rotas com mais nós no mesmo sentido têm preferência. O algoritmo também prevê o tempo de vida de uma rota, utilizando para isso o menor tempo de vida previsto para os enlaces da rota. O tempo de vida de um enlace é estimado pela área de alcance de rádio dos dois nós, a distância entre eles, suas velocidades e suas direções de deslocamento. Ao receber uma requisição de rota, um *gateway* adiciona suas informações e ajusta o campo de tempo de vida para o valor máximo. Isso é necessário, pois nos casos em que a velocidade dos carros é muito próxima, o valor previsto para o tempo de vida do enlace pode ser muito alto. Em seguida, o *gateway* envia uma resposta de rota para o nó que gerou a requisição utilizando a rota descrita no pacote. Cada nó intermediário calcula o tempo de vida do enlace entre ele e seu predecessor e, caso seja menor que o armazenado na resposta de rota, o nó ajusta o valor de tempo de vida do pacote. Assim, garante-se que o tempo de vida previsto para a rota seja o mínimo entre os tempos de vida previstos para os enlaces. Depois da construção da rota, o nó fonte inicia a transmissão de dados e um temporizador baseado no tempo de vida estimado para a rota. O temporizador é utilizado para que uma nova requisição de rota seja enviada antes que a rota expire, evitando interrupções nas transmissões.

5.5.2. Baseado em Posicionamento

O objetivo do roteamento baseado em posicionamento, ou geográfico, é prover escalabilidade em ambientes de alta mobilidade, já que nessa abordagem não é necessário manter informações sobre as rotas para todos os nós da rede. Esse cenário é exatamente o encontrado nas redes veiculares, dessa forma grande parte dos algoritmos de roteamento é do tipo geográfico. Em geral, os protocolos de roteamento geográficos assumem que todos os nós presentes na rede possuem algum sistema de localização tal como GPS ou Galileo [Hein et al. 2002]. Além disso, alguns utilizam informações sobre a topologia das vias de circulação através de mapas digitais.

Nos protocolos de roteamento geográficos, um nó fonte envia os pacotes de dados em direção à localização do destinatário por múltiplos saltos. Para tanto, o nó precisa conhecer a posição de seus vizinhos, normalmente por sondas enviadas periodicamente, e a posição do destinatário, em geral utilizando um serviço de localização. Um exemplo de serviço de localização é o RLS (*Reactive Location Service*) [Kasemann et al. 2002]. O nó executando o RLS envia uma requisição de posição contendo o identificador do nó destinatário além de sua própria localização e do seu identificador. A requisição é inundada até que o destinatário seja alcançado ou o TTL (*Time-To-Live*) presente na requisição expire. Quando o destinatário é alcançado, uma resposta de localização é enviada ao nó emissor, contendo as informações presentes na requisição e a sua localização [Camp 2005].

O GPSR (*Greedy Perimeter Stateless Routing*) [Karp e Kung 2000] é um protocolo de roteamento geográfico desenvolvido originalmente para redes ad hoc móveis. O GPSR utiliza um algoritmo guloso para realizar o encaminhamento (*greedy forwarding)* no qual cada nó encaminha os pacotes de dados para o vizinho mais próximo do destinatário. Por exemplo, na Figura 5.7(a) o nó fonte *f* deseja enviar dados ao nó destino *d*. O círculo em torno de *f* indica sua área de alcance de rádio. Assim, o nó *m* é, entre os vizinhos de *f*, o mais próximo de *d* (o arco tracejado indica a distância entre *m* e *d*) e é escolhido para encaminhar os dados. Cada nó conhece a posição de seus vizinhos através do envio de sondas ou através de mensagens de dados (*piggyback*). Essa estratégia de encaminhamento possui a vantagem de exigir que cada nó mantenha somente informações acerca de seus vizinhos de um salto, aumentando a escalabilidade do protocolo de roteamento.

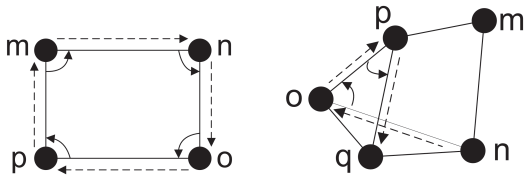


(a) Estratégia geral. (b) Ótimo local.

Figura 5.7. Encaminhamento guloso.

Em algumas situações, o encaminhamento guloso atinge um ponto chamado de ótimo local (ou máximo local), no qual o encaminhamento não é possível. A Figura 5.7(b) apresenta um exemplo de ótimo local. O nó *f* deseja encaminhar uma mensagem em direção ao nó *d*, entretanto o nó *d* não possui nenhum vizinho mais próximo de *f* que ele mesmo (o arco tracejado descreve a distância entre *d* e *f* e o círculo representa a área

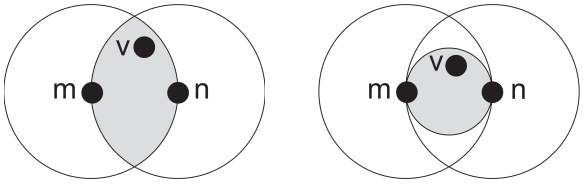
de alcance de rádio de f). Em situações como essa um mecanismo de recuperação é necessário. Para tanto, o GPSR possui uma forma de operação chamada de modo perímetro. Ao perceber a ocorrência de um ótimo local, uma marca é adicionada ao pacote indicando a operação no modo perímetro. Em seguida, o pacote é encaminhado segundo a regra da mão direita, um método utilizado para percorrer grafos apresentado na Figura 5.8(a). Partindo do nó m em direção a n, o próximo arco que deve ser atravessado é o seguinte no sentido anti-horário a partir do arco (m,n), ou seja, o arco (n,o). O percurso completo pelo grafo é $m \rightarrow n \rightarrow o \rightarrow p \rightarrow m$. No exemplo da Figura 5.7(b), o percurso de recuperação utilizado é a sequência $f \rightarrow m \rightarrow n \rightarrow o \rightarrow d$.



(a) Funcionamento. (b) Falha.

Figura 5.8. Regra da mão direita.

A utilização da regra da mão direita para recuperação de ótimos locais limita-se a grafos planares. Define-se grafo planar aquele em que não existem cruzamentos entre arcos em sua representação no plano. Em alguns casos, porém, o grafo que representa a rede não é planar. Nessas situações, um algoritmo de planarização é necessário. Por exemplo, no grafo da Figura 5.8(b), partindo do arco (n,o), parte da sequência percorrida pela regra da mão direita é $n \rightarrow o \rightarrow p \rightarrow q$, o que impossibilita que o nó m seja alcançado. O RNG (*Relative Neighborhood Graph*) e o GG (*Gabriel Graph*) [Jaromczyk e Toussaint 1992] são dois grafos planares utilizados no GPSR. Algoritmos distribuídos de remoção de arcos são executados para construir grafos RNG ou GG conexos. Em um grafo RNG existe um arco (m,n) se a distância entre os vértices m e n for menor ou igual à distância entre um vértice v e qualquer dos vértices m e n. Na Figura 5.9(a), o arco entre m e n é eliminado se existir algum outro nó na região achurada. Em um grafo GG existe um arco (m,n) se não existem outros vértices no círculo com diâmetro igual à distância entre m e n e que passa por esses dois vértices. A Figura 5.9(b) apresenta a interpretação geométrica desta definição. Pode-se observar que um grafo RNG é um subgrafo de um grafo GG.

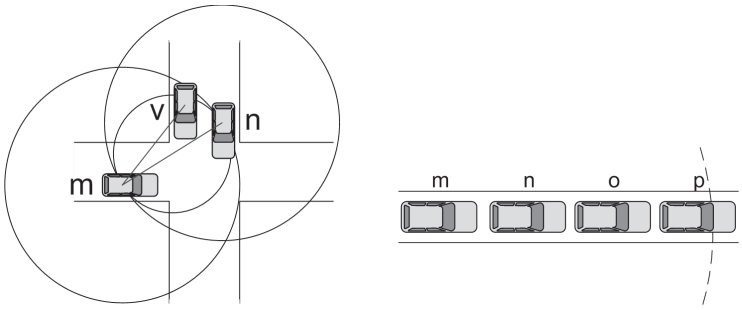


(a) Grafo RNG. (b) Grafo GG.

Figura 5.9. Grafos planares.

A utilização de algoritmos de planarização como GG e RNG em redes veiculares possibilita o uso da regra da mão direita, mas pode levar à eliminação de enlaces essenciais à comunicação ocasionando desconexão da rede. Por exemplo, na Figura 5.10(a) o enlace entre m e n é eliminado devido à presença de v. Entretanto, a comunicação não

ocorre, pois existe um obstáculo entre m e v. Outro problema associado à utilização de grafos planares é a utilização de rotas com número excessivo de saltos. Por exemplo, na Figura 5.10(b), a comunicação poderia ocorrer diretamente entre m e p. Entretanto, o caminho percorrido é $m \rightarrow n \rightarrow o \rightarrow p$, já que os outros enlaces são removidos. Além disso, a utilização da regra da mão direita torna a escolha da rota tendenciosa em certa direção, que em muitos casos pode não ser a melhor.



(a) Desconexão. (b) Excesso de saltos.

Figura 5.10. Problemas com grafos planares em redes veiculares.

Para contornar os problemas da necessidade de uso de grafos planares em redes veiculares, o GSR (*Geographic Source Routing*) [Lochert et al. 2003] utiliza informações de mapas digitais para calcular a rota, ou seja, um conjunto de cruzamentos que deve ser percorrido pelo pacote, criando assim uma rede sobreposta. A rota é calculada com o algoritmo de Dijkstra. O roteamento pode ser realizado pela fonte, adicionando a rota ao cabeçalho do pacote, ou salto a salto. Além disso, entre dois cruzamentos, o encaminhamento guloso é utilizado, de forma similar ao realizado pelo GPSR, já que nessa situação não devem existir obstáculos no caminho. Além disso, caso algum ótimo local seja atingido, o protocolo retorna ao encaminhamento guloso tradicional.

De modo similar ao GSR, o SAR (*Spatially-Aware packet Routing*) [Tian et al. 2003] busca sobrepor as fraquezas do GPSR utilizando um modelo espacial que associa mapas digitais a grafos tendo como vértices lugares significativos e como arcos as vias que os interconectam. O roteamento é realizado pela fonte, utilizando como peso para os arcos as características das vias como comprimento ou velocidade média. Três estratégias de recuperação são propostas: o armazenamento da mensagem até que o encaminhamento seja possível ou um temporizador expire, o encaminhamento pelo modo guloso, ou o cálculo de um novo caminho a partir da posição em que o ótimo local é atingido.

O A-STAR (*Anchor-Based Street and Traffic Aware Routing*) [Seet et al. 2004] também utiliza os cruzamentos entre as vias (chamadas nesse contexto de âncoras) para realizar o encaminhamento dos pacotes. O A-STAR utiliza informações acerca das rotas de ônibus no roteamento, priorizando as vias que fazem parte destas rotas sob o argumento de que essas vias possuem densidade maior de veículos, o que, em princípio, propicia maior conectividade. A recuperação de máximos locais é realizada calculando um novo caminho de âncoras para o pacote. Além disso, a via na qual o máximo local ocorre é marcada como "fora de serviço" temporariamente. Essa informação é adicionada aos pacotes de dados, informando outros nós. Para evitar a circulação de dados na rede por tempo indeterminado, há um número máximo de recuperações permitido.

O método para encaminhamento de mensagens utilizado pelo GPCR (*Greedy Perimeter Coordinator Routing*) [Lochert et al. 2005] é chamado de encaminhamento guloso restrito. Cada nó, ao realizar o encaminhamento, seleciona nós qualificados, definidos como os nós próximos à linha formada pelo nó encaminhador e seu antecessor. Se algum dos nós qualificados é um coordenador (nó localizado em um cruzamento), ele recebe a mensagem. Caso contrário, o nó mais distante é selecionado. Um requisito do algoritmo descrito é o conhecimento pelo nó de sua condição de coordenador. O GPCR não utiliza informações de mapas digitais, dessa forma, duas estratégias são propostas. Na primeira, cada nó envia mensagens de controle periódicas com a posição e a lista de vizinhos; assim, um nó *k* considera-se em um cruzamento caso dois de seus vizinhos, *m* e *n*, estejam em área de alcance mútuo, mas não listem um ao outro como vizinhos. Essa situação indica que *m* e *n* estão separados por um obstáculo e assim é provável que *k* esteja em um cruzamento. A segunda estratégia utiliza a correlação entre as posições dos vizinhos. Valores próximos de 1 indicam uma relação linear entre a posição dos vizinhos. Logo o nó em questão está provavelmente em uma rua. Já valores próximos de 0 mostram uma relação não linear entre as posições dos vizinhos. Logo, o nó deve se encontrar em um cruzamento. A recuperação de ótimos locais pode ser realizada em um cruzamento ou em vias. No primeiro caso, a rua pela qual o pacote deve ser transmitido é escolhida segundo a regra da mão direita, enquanto no segundo caso o encaminhamento guloso é utilizado.

O protocolo CAR (*Connectivity-Aware Routing*) [Naumov e Gross 2007] não depende de um serviço de localização. Para descobrir a posição do nó, uma versão adaptada do PGB (*Preferred Group Broadcasting*) é utilizada. Um identificador para a requisição é adicionado à mensagem para evitar ciclos. O CAR utiliza um marcador geográfico que é armazenado e encaminhado entre os veículos para disseminar informações sobre um nó que tenha mudado sua posição. Esse marcador, chamado de guarda, é uma mensagem temporária contendo uma identificação, TTL, um raio de propagação e alguma informação de estado. As guardas estáticas (*standing guards*) são fixas em coordenadas geográficas específicas, enquanto que as guardas móveis (*traveling guards*) têm coordenadas, tempo e vetor de velocidade iniciais.

O LOUVRE (*Landmark Overlays for Urban Vehicular Routing Environments*) cria uma rede sobreposta, tendo como nós os cruzamentos entre as vias [Lee et al. 2008]. Além disso, só existe um arco entre dois nós se a via que une os cruzamentos respectivos possuir densidade veicular maior que um limiar pré-definido. O comprimento das vias é utilizado como peso para os arcos, sob o argumento de que vias menores implicam um menor número de saltos. Cada nó envia em suas mensagens de controle informações de densidade das vias pelas quais trafegou. O cálculo da densidade das vias é realizado por cada nó a partir do número de mensagens de controle recebidas. Os autores utilizam a premissa de que o número de veículos nas vias é relativamente estático tanto em horários com baixa movimentação quanto em horários críticos [Wisitpongphan et al. 2007]. Caso a informação da densidade de uma determinada via possua alguma inconsistência, um ótimo local pode ser atingido. Os autores sugerem duas estratégias de recuperação. Na primeira, direcionada a aplicações sensíveis a atraso, os pacotes são enviados para o cruzamento anterior e direcionados para o segundo melhor cruzamento. Caso não existam alternativas o pacote é descartado. Em aplicações tolerantes a atrasos, o pacote é armazenado até que o encaminhamento seja possível.

5.5.3. Oportunístico

Com a adoção gradual das redes veiculares, os veículos na fase inicial poderão experimentar interrupções do serviço e frequentes desconexões. Esses problemas são semelhantes aos enfrentados pelas redes tolerantes a atrasos e desconexões (DTN - *Delay Tolerant Networks*) [Oliveira et al. 2007] que devido à escassez de nós na rede, não possuem garantias de estabelecimento de caminhos fim-a-fim entre pares origem-destino. Esta seção tem por objetivo apresentar protocolos de roteamento adaptados para estes cenários, que podem ocorrer em redes veiculares. De acordo com [Wisitpongphan et al. 2007], mesmo com 100% de penetração de mercado, a probabilidade de desconexão em uma via expressa em períodos de menor movimento é de 35%.

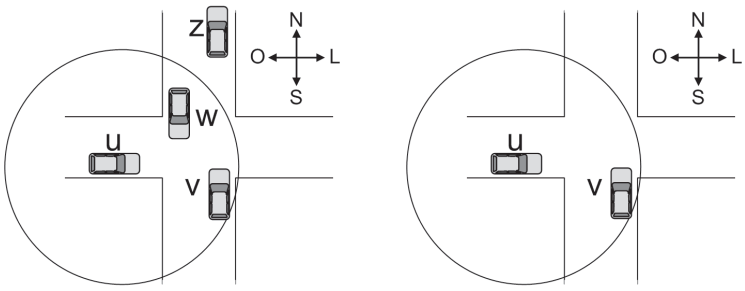
O algoritmo MoVe (*Motion Vector*) [LeBrun et al. 2005] utiliza a velocidade e a trajetória dos vizinhos para predizer qual veículo chegará mais perto de uma Unidade de Acostamento (RSU), que o algoritmo assume ser o destino da mensagem. Veículos carregando mensagens enviam sondas com estas informações periodicamente. Ao receber uma resposta, o nó calcula a distância entre as posições previstas entre o nó e a RSU e o nó decide por encaminhar ou não a mensagem. LeBrun et al. analisaram o algoritmo e encontraram resultados melhores que o encaminhamento guloso em redes esparsas, porém pior onde se utiliza a movimentação prevista de linhas de ônibus.

O MaxProp [Burgess et al. 2006] armazena todos os pacotes até que o destinatário seja alcançado, seu temporizador expire ou uma confirmação de entrega seja encaminhada por um terceiro nó. Porém, a capacidade de armazenamento é limitada, por isso, o MaxProp define mecanismos para priorização de pacotes. Quando dois nós se encontram, todas as mensagens destinadas ao nó encontrado são enviadas. Em seguida, informações de roteamento são trocadas. Para esvaziar *buffers* na rede, mensagens de reconhecimento de pacotes originados por outros nós são trocadas na sequência. Além disso, os pacotes são divididos em dois grupos, o primeiro contendo mensagens com número de saltos percorridos menor que um limiar, os primeiros a serem transmitidos. A ordenação desse primeiro grupo é realizada segundo o número de saltos percorridos, dando prioridade a pacotes mais novos na rede. O segundo grupo é formado por pacotes a serem descartados, organizados segundo a probabilidade de entrega. Para evitar que o mesmo nó receba um pacote duas vezes, um identificador é adicionado ao pacote.

O algoritmo SKVR (*Scalable Knowledge-Based Routing*) [Ahmed e Kanere 2006] se beneficia do conhecimento prévio da rota dos ônibus. O SKVR utiliza dois níveis de hierarquia em busca de maior escalabilidade. Um nível interdomínio (entre rotas de ônibus) e outro intradomínio (entre veículos em uma rota de ônibus). Para realizar o roteamento interdomínios, o algoritmo utiliza o conhecimento prévio das rotas dos ônibus. A mensagem é encaminhada para algum veículo que pertença à rota do destino ou a algum veículo que eventualmente cruza a rota do destino. Em último caso, cópias da mensagem são encaminhadas para parte dos vizinhos do nó. Já para o encaminhamento intradomínio, cada nó ao encaminhar a mensagem precisa decidir em que sentido da rota a mensagem deve ser encaminhada. Para tal, uma lista de nós encontrados dentro da rota é mantida. Assim, se o nó destino estiver na lista, a mensagem é enviada no sentido oposto.

O VADD (*Vehicle-Assisted Data Delivery*) [Zhao e Cao 2008] utiliza a mobilidade previsível das redes veiculares, restrita a vias e condições de tráfego, aliada à técnica

carry and forward. O VADD possui três modos de operação dependendo da posição do nó carregando o pacote: interseção, linha reta e destino. O modo de interseção é utilizado quando o nó encontra-se em uma interseção e precisa realizar uma decisão acerca do encaminhamento. A primeira decisão nesse modo é o sentido para o qual a mensagem deve ser encaminhada, que é baseada na distância ao destino, atraso esperado de entrega e probabilidade de entrega. Se nenhum nó puder encaminhar a mensagem no sentido de maior preferência, o segundo sentido é o escolhido. Esse procedimento é repetido até que um sentido seja possível. Caso não haja nenhuma, o nó mantém o pacote em seu *buffer* até que haja alguma oportunidade de encaminhamento. A segunda decisão no modo interseção é qual nó deve encaminhar a mensagem para um dado sentido. Desse fato, surgem as variações do protocolo. Na Figura 5.11(a), o veículo *u* deseja encaminhar o pacote no sentido norte e existem dois nós possíveis. O nó *w*, movendo-se no sentido sul e nó *v*, movendo-se no sentido norte. Utilizando o protocolo L-VADD (*Location first probe* VADD), o nó *w* será escolhido por estar mais próximo do destino, o que poderia reduzir o atraso de entrega com o nó *w* encaminhando a mensagem imediatamente para *z*. Entretanto, essa abordagem pode provocar ciclos no roteamento. Na Figura 5.11(b) o nó *u* deseja encaminhar o pacote para o norte, mas como não há candidatos o sentido leste é verificado. Como não existem candidatos o sentido sul é escolhido e o nó *v* recebe a mensagem. Imediatamente *v* verifica seus vizinhos na direção norte e descobre que *u* está mais próximo e o encaminha a mensagem. Assim, está configurado um ciclo entre *u* e *v*.



(a) Seleção do próximo salto. (b) Ciclo no encaminhamento.

Figura 5.11. Funcionamento do VADD.

O protocolo D-VADD (*Direction first probe* VADD) encaminha a mensagem para o nó que se desloca no sentido preferencial, garantindo a inexistência de ciclos. Na Figura 5.11(a), o nó escolhido pelo D-VADD é o nó *v* que se move no sentido preferencial. Devido ao atraso imposto pelo D-VADD, resultado dos longos caminhos escolhidos, o H-VADD (*Hybrid probe* VADD) é proposto. Esse protocolo comporta-se inicialmente como o L-VADD e, caso algum ciclo seja detectado, passa a comportar-se como o D-VADD.

5.5.4. Disseminação

Os protocolos de roteamento das classes anteriores calculam rotas ponto-a-ponto (*unicast*). Entretanto, a disseminação de informação é essencial para diversas aplicações em redes veiculares. Por exemplo, algumas aplicações de assistência ao motorista exigem que informações sobre condições das vias sejam disseminadas em uma determinada região. Assim, alguns protocolos foram projetados para disseminação eficiente de informação.

O objetivo do UMB (*Urban Multi-hop Broadcast protocol*) [Korkmaz et al. 2004] é diminuir o excesso de carga de controle em difusão, evitar o problema do terminal escondido e aumentar a confiabilidade na difusão em múltiplos saltos em áreas urbanas. O protocolo possui dois modos de operação: na difusão direcional, o nó mais distante da origem é selecionado para continuar a difusão. Já no modo de interseção, o protocolo assume que repetidores são instalados nos cruzamentos para encaminhar a difusão. Além disso, um mecanismo semelhante ao RTS/CTS (*Request-To-Send*/*Clear-To-Send*) do IEEE 802.11 é utilizado para evitar o problema do terminal escondido.

O SODAD (*Segment-Oriented Data Abstraction and Dissemination*) é um método para disseminação de informações de entretenimento ou de assistência ao motorista [Wischhof et al. 2005]. No SODAD, a estrada é divida em segmentos e informações coletadas pelos veículos são associadas aos segmentos. A frequência de difusão das informações é variada de acordo com dois tipos de eventos: *provocation*, por exemplo, a recepção de dados desatualizados, que reduzem o tempo entre duas difusões, e *mollification*, que aumentam o tempo entre difusões. A adaptação dinâmica da frequência de difusão ajuda a evitar sobrecarga da rede. Entretanto, sugestões de coordenação entre os veículos para evitar colisões de mensagens não são apresentadas. Assim, a escalabilidade é um problema, já que uma alta frequência de difusão em um segmento pode resultar em um alto número de transmissões sem sucesso, devido ao maior número de colisões de pacotes.

Maihofer e Eberhardt utilizam um tipo especial de comunicação multidestinatária conhecida como difusão por área (*geocasting*). Essa abordagem limita a difusão das mensagens ao grupo de nós localizados em uma região geográfica, chamada de zona de relevância (*Zone Of Relevance* – ZOR) para a mensagem. Esquemas de cache e de seleção de vizinhos são utilizados para lidar com a alta mobilidade das redes veiculares. A principal ideia do *Cached Geocast* [Maihofer e Eberhardt 2004] dentro da ZOR é adicionar um armazenamento provisório à camada de roteamento para mensagens que não podem ser encaminhadas imediatamente. A mensagem é encaminhada quando novos vizinhos entram na região de alcance do nó.

Uma forma diferente de *geocasting* é explorada em [Maihofer et al. 2005], chamada *Abinding Geocast*. Nessa abordagem, a mensagem deve ser entregue a todos os nós dentro da ZOR em um determinado espaço de tempo (*geocast lifetime*). Aplicações como propagandas baseadas em posicionamento ou baseadas em *publish-and-subscribe* justificam por essa abordagem. Maihofer et al. propõem três soluções: utilização de um servidor para armazenar as mensagens; eleição de um nó dentro da ZOR para armazenar as informações, ou seja, para agir como servidor; ou armazenamento, por cada um dos nós, das informações destinadas a sua localização e da lista de vizinhos.

5.5.5. Resumo

A Tabela 5.2 resume as propostas de roteamento apresentadas nesta seção segundo algumas de suas características principais.

5.6. Acesso ao Meio e Camada Física

Os protocolos de acesso ao meio físico utilizados em redes ad hoc móveis também necessitam de adaptações de forma a serem usados de forma eficiente em redes veicula-

Tabela 5.2. Protocolos/algoritmos de roteamento para redes veiculares, suas características e suas dependências.

Protocolo/ Algoritmo	Posição	Paradigma de Comunicação	Classificação	Mapas	Serviço de Localização	*Buffer*
PBR	√	ponto-a-ponto	topológico			
GPSR	√	ponto-a-ponto	geográfico		√	
GSR	√	ponto-a-ponto	geográfico	√	√	
SAR	√	ponto-a-ponto	geográfico	√	√	√
A-STAR	√	ponto-a-ponto	geográfico	√	√	
GPCR	√	ponto-a-ponto	geográfico		√	
CAR	√	ponto-a-ponto	geográfico			√
LOUVRE	√	ponto-a-ponto	geográfico	√	√	√
MoVe	√	ponto-a-ponto	oportunístico		√	√
MaxProp	√	ponto-a-ponto	oportunístico			√
SKVR		ponto-a-ponto	oportunístico			√
VADD	√	ponto-a-ponto	oportunístico	√	√	√
UMB	√	difusão	disseminação	√		√
SODAD	√	difusão	disseminação	√		√
Cached Geocast	√	difusão por área	disseminação			√
Abinding Geocast	√	difusão por área	disseminação	√		√

res, principalmente devido à alta mobilidade e consequente rápida mudança de topologia. Além disso, aplicações como as de segurança no trânsito exigem o envio contínuo de informações em difusão com confiabilidade e baixa latência, características nem sempre presentes nos protocolos para as redes ad hoc. Dessa forma, surgiram protocolos específicos para redes veiculares. Alguns desses protocolos aumentam o desempenho da rede através de modificações na camada física. Esses protocolos podem ser classificados em função do uso de múltiplos canais, do uso de antenas direcionais e da necessidade de confiabilidade, de baixa latência e de transmissão em difusão. A seguir os principais protocolos para redes veiculares são apresentados, de acordo com a classificação proposta.

5.6.1. Múltiplos Canais

O desempenho de uma rede pode aumentar com a utilização de múltiplos canais, já que cada canal está associado a um domínio de colisão diferente e a banda passante disponível aumenta com o número de canais. Múltiplos canais são empregados por vários protocolos de acesso ao meio para redes veiculares. Especificamente, a separação entre as comunicações das aplicações voltadas para segurança e as comunicações dos outros tipos de aplicações é interessante. Costuma-se utilizar um canal de controle para as aplicações de segurança e canais de serviço para as outras aplicações, como no padrão WAVE (Seção 5.3.1).

Mak et al. propõem um protocolo de acesso ao meio baseado no modo centralizado PCF (*Point Coordination Function*) do IEEE 802.11, considerando a arquitetura de múltiplos canais do WAVE [Mak et al. 2005] e a utilização de uma única interface de rádio por veículo. O objetivo do protocolo é possibilitar a utilização de aplicações que não envolvem segurança, sem comprometer o desempenho das aplicações relacionadas à segurança. O protocolo é utilizado na vizinhança de pontos de acesso espalhados por uma

estrada. O protocolo divide no tempo o canal de controle em uma parte com disputa e outra parte sem disputa, como no PCF. Durante o período livre de contenção, cada veículo é consultado (*polling*) pelo ponto de acesso e pode transmitir suas mensagens de segurança. O intervalo entre dois períodos livres de contenção é escolhido de forma a não comprometer as aplicações de segurança, ou seja, corresponde à menor latência dessas aplicações. No período de contenção, os veículos podem transmitir dados das aplicações não voltadas para segurança. Fora da região de alcance dos pontos de acesso, outro protocolo ad hoc, por exemplo, que seja baseado no modo distribuído DCF (*Distributed Coordination Function*) do IEEE 802.11, deve ser usado.

O protocolo *Vehicular MESH Network* (VMESH) [Zang et al. 2007] também utiliza a arquitetura de múltiplos canais do WAVE visando aplicações sensíveis à vazão em cenários de redes densas. Um esquema de sinalização (sonda) sincronizado e distribuído é utilizado de forma que os nós conheçam seus vizinhos e façam reservas de canais dinamicamente. O protocolo provê melhor qualidade de serviço para aplicações que não são de segurança através do conhecimento da vizinhança e de um acesso sem disputa nos canais de serviço (SCHs). Em comparação com o acesso ao meio do WAVE, o protocolo VMESH apresenta algumas diferenças. O VMESH emprega superquadros que contêm múltiplos intervalos de sincronização do IEEE 1609. Cada intervalo do canal de controle (CCH) é ainda dividido em duas partes: período de sinalização e período de segurança. O período de segurança é usado somente para as aplicações de segurança. Já o período de sinalização consiste em um número de *slots* para o envio de sondas. Cada dispositivo tem de escolher um único *slot* desse período e transmitir a sua sonda em todos os intervalos CCH. O acesso aos *slots* do período de sinalização é realizado através do protocolo R-ALOHA (*Reservation ALOHA*). Através das sondas é realizada uma reserva dinâmica nos canais de serviço de forma a aumentar o desempenho das aplicações sensíveis à vazão. Essa reserva é realizada através de negociação entre o transmissor, o(s) receptor(es) e os vizinhos. Dessa forma o acesso aos canais de serviço é um acesso múltiplo por divisão de tempo (*Time Division Multiple Access* - TDMA).

5.6.2. Antenas Direcionais

Nas redes veiculares, em função das trajetórias dos veículos, o uso de antenas direcionais pode ser apropriado. Por exemplo, pode-se diminuir a interferência causada por veículos em pistas vizinhas. Em uma rede veicular com infraestrutura distribuída à direita ao longo de ruas ou estradas, um sistema de antenas direcionais pode inibir a comunicação na região à esquerda do nó, minimizando a interferência entre veículos em sentidos opostos. No caso da infraestutura estar localizada em cima de pontes ou viadutos cruzando a estrada, podem ser utilizadas antenas exclusivas para cada faixa de rolamento, diminuindo a interferência entre veículos trafegando no mesmo sentido, porém em faixas diferentes [Dobias e Grabow 1994]. Além disso, tanto em redes infraestruturadas quanto em redes ad hoc, o maior alcance obtido com antenas direcionais pode aumentar o tempo de contato entre os nós, aumentando o montante de dados transferidos durante um contato.

A arquitetura MobiSteer [Navda et al. 2007] utiliza um sistema de antenas de feixe direcionado para aumentar o desempenho do IEEE 802.11 na comunicação entre veículos e pontos de acesso distribuídos em uma rodovia. O objetivo principal da arquitetura é selecionar o melhor ponto de acesso e o melhor direcionamento de feixe em cada ponto de

uma rodovia, de modo a maximizar a vazão. No MobiSteer, os veículos usam antenas direcionais e os pontos de acesso empregam antenas omnidirecionais, em função dos vários veículos que podem utilizar um mesmo ponto de acesso simultaneamente e dos diversos pontos de acesso com antenas omnidirecionais que já estão implantados atualmente.

Subramanian et al. utilizam a arquitetura MobiSteer na comunicação direta entre dois veículos se movendo no mesmo sentido ou em sentidos opostos [Subramanian et al. 2008]. Foi desenvolvido um protocolo que troca coordenadas de GPSs de modo a determinar continuamente os feixes de visada direta entre os dois veículos. Dessa forma consegue-se aumentar as taxas físicas de dados proporcionando ganhos de desempenho.

5.6.3. Confiabilidade, Baixa Latência e Transmissão em Difusão

Aplicações de segurança no trânsito, apesar de normalmente enviarem pequena quantidade de informação, necessitam de confiabilidade, de baixa latência e de transmissão em difusão [Menouar et al. 2006].

Xu et al. propõem protocolos aleatórios de acesso ao meio para redes veiculares no modo ad hoc como extensões à subcamada MAC [Xu et al. 2004], também considerando a arquitetura de múltiplos canais do WAVE. Além disso, supõem que o canal de controle é utilizado para o envio de mensagens de segurança. A ideia principal dos protocolos é repetir o envio de cada mensagem diversas vezes, de forma a diminuir a probabilidade de falha no recebimento da mensagem. Cada transmissor envia as mensagens em *slots* de tempo diferentes dentro do tempo de vida da mensagem.

Shankar e Yedla também propõem extensões à subcamada MAC de forma a aumentar a qualidade do serviço no envio em difusão de mensagens de segurança [Shankar e Yedla 2007]. Contudo consideram a extensão IEEE 802.11e e redes veiculares tanto no modo ad hoc quanto no modo infraestruturado. O principal problema tratado pelo protocolo proposto corresponde ao envio múltiplo de mensagens de segurança iguais por diversos veículos em uma mesma área, o que causa desperdício de banda passante. O protocolo proposto utiliza informações de posicionamento de forma a reduzir a redundância na difusão de mensagens de segurança. Um nó verifica o identificador da mensagem e a proximidade do receptor com o transmissor da mensagem. Caso estejam próximos, o nó não retransmite a mensagem.

Um esquema de comunicação multicanal baseado em agrupamentos e integrado com protocolos de acesso ao meio, para redes ad hoc veiculares é proposto em [Zhang et al. 2006]. No esquema proposto, um veículo eleito como líder do agrupamento coleta/entrega mensagens de segurança dentro do próprio agrupamento e encaminha as mensagens consolidadas para outros líderes de agrupamentos. O veículo líder do agrupamento também controla a associação de canais para os veículos pertencentes ao agrupamento transmitirem mensagens não relativas à segurança. O esquema emprega diferentes métodos de acesso. Para mensagens de segurança é utilizado dentro de um agrupamento TDMA no *upstream* e difusão no *downstream*. O modo DCF do IEEE 802.11 é usado entre veículos líderes dos agrupamentos. O esquema de comunicação utiliza ainda a arquitetura de múltiplos canais do WAVE: o canal CCH é usado para controle (mensagens de segurança) interagrupamentos, o canal SCH 174 é utilizado para dados (mensagens não relativas à segurança) interagrupamentos, o canal SCH 172 serve para controle

intra-agrupamento e os canais SCH 176, 180, 182 e 184 são usados para dados intra-agrupamento. Com isso consegue-se aumentar a vazão mantendo a garantia de entrega das mensagens de segurança.

Alguns protocolos de acesso ao meio que levam em consideração qualidade de serviço provêem prioridade de forma estatística. Peng e Cheng propõem um esquema distribuído para acesso ao meio que emprega um escalonamento de pacotes (mensagens) de segurança baseado em prioridades de forma determinística [Peng e Cheng 2007]. O esquema é voltado para redes ad hoc veiculares e utiliza um único canal de controle no qual são enviados pulsos para marcar o uso do canal de dados para o envio das mensagens de segurança. Os pulsos são sinais de um único tom com pausas de tamanhos aleatórios. O esquema funciona da seguinte forma. Logo que um pacote de segurança chega à subcamada MAC, se o canal de controle estiver livre por um determinado período de tempo, o nó cria um temporizador de *backoff*. Quando o temporizador expira, o nó começa a transmitir pulsos no canal de controle. Em seguida, o nó começa a difundir a mensagem no canal de dados. Se um nó detecta um pulso antes do temporizador expirar, o temporizador é cancelado e o nó retorna a monitorar o canal de controle. Durante a transmissão da mensagem de segurança, se um nó detectar um pulso de outro nó enquanto estiver em pausa, ele aborta a transmissão e libera os dois canais.

O protocolo ADHOC MAC [Borgonovo et al. 2004] é composto pelo método de acesso TDMA dinâmico e pelo protocolo RR-ALOHA (*Reliable Reservation ALOHA*), que estabelece um canal de sinalização em difusão de forma totalmente distribuída. A partir desse canal, todos os nós conhecem a atividade de seus vizinhos de dois saltos, através do status (livre ou ocupado) de cada *slot*, e então podem evitar colisões, visando principalmente combater o problema do terminal escondido.

5.6.4. Resumo

A Tabela 5.3 apresenta os principais protocolos/arquiteturas/esquemas utilizados em redes veiculares classificados em função das características citadas anteriormente.

Tabela 5.3. Protocolos/arquiteturas/esquemas de acesso ao meio e camada física para redes veiculares e suas características.

Protocolo/arquitetura/esquema	Múltiplos canais	Antenas direcionais	Confiabilidade
De Mak et al.	√		√
VMESH	√		√
MobiSteer		√	
De Subramanian et al.		√	
De Xu et al.	√		√
De Shankar e Yedla			√
De Zhang et al.	√		√
De Peng e Cheng	√		√
ADHOC MAC			√

5.7. Desafios

As redes veiculares apresentam diferentes desafios de pesquisa em aberto, alguns deles relacionados ao ambiente específico de comunicação dessas redes. As redes veicula-

res possuem nós que podem se mover a alta velocidade, embora em trajetórias limitadas. Consideradas essas características, essas redes devem ser robustas e escaláveis, já que devem operar em cenários com poucos ou com alguns milhares de nós. Em termos de qualidade de serviço e segurança, as redes veiculares possuem requisitos estritos, pois em muitas situações a integridade física de seres humanos pode estar em jogo. Nesta seção, são destacados os principais desafios em aberto na área de redes veiculares.

5.7.1. Endereçamento

A atribuição dos endereços na Internet é feita de forma hierárquica. Assim, ao receber um pacote para encaminhamento, o roteador verifica o endereço de destino e procura uma rota na tabela de roteamento que possua o maior número de bits iniciais em comum. O processo de escolha desses prefixos mais longos se repete a cada roteador até que o pacote alcance seu destino. O objetivo é aumentar a escalabilidade da rede, já que cada roteador não precisa nem armazenar nem anunciar endereços IP individuais. O roteamento na Internet, entretanto, requer que as estações sejam estáticas para que a estrutura hierárquica seja mantida. Quando há nós móveis, os endereços não são mantidos, sendo necessária uma forma automática de atribuição de endereços para que as estações possam se comunicar enquanto se movem. Muitos trabalhos propõem soluções como o uso do IP móvel, do NAT (*Network Address Translation*), do DHCP (*Dynamic Host Configuration Protocol*) etc. para lidar com questões de endereçamento nas redes móveis. Entretanto, nenhuma dessas soluções resolveu definitivamente o problema [Moraes et al. 2008]. Soluções de configuração de endereços já foram propostas para redes ad hoc móveis, mas não consideram a topologia e o padrão de mobilidade das redes veiculares [Weniger 2005]. Portanto, é necessário desenvolver protocolos de atribuição de endereços específicos para essas redes, que podem ter como base os esquemas de autoconfiguração já propostos para as redes ad hoc móveis.

Em redes ad hoc móveis, as soluções de configuração de endereço podem ser classificadas em descentralizadas, melhor esforço e baseadas em líder [Fazio et al. 2007]. As primeiras são realizadas de forma distribuída na qual um nó que necessita de um endereço de rede envia uma mensagem em difusão para requisitar parâmetros de configuração. Essa requisição é respondida por algum nó da rede que, após interagir com os outros nós para verificar a disponibilidade de um endereço, fornece ao nó requisitante os parâmetros necessários. O modo descentralizado pode gerar alto tráfego de controle devido à necessidade de interações entre todos os nós da rede. Já as soluções de melhor esforço consideram desnecessária a preocupação com a duplicidade de endereços antes da ocorrência de um conflito. Nessas soluções, endereços de rede são atribuídos sem a garantia de unicidade. Assim, há a necessidade de mecanismos que reajam às duplicidades, detectando tentativas de comunicação entre nós com o mesmo endereço ou encaminhamento de dados para um nó diferente do desejado. Essa característica reativa tem como problema o atraso gerado na comunicação. Por último, as soluções baseadas em líder são realizadas de forma hierárquica, possuindo como princípio a escolha de alguns nós que mantenham o controle da associação de endereços. Em cenários de alta mobilidade, como no caso das redes veiculares, pode haver quebra de comunicação entre os nós líderes, podendo gerar duplicidade de endereços de rede. As redes ad hoc infraestruturadas podem ainda usufruir de pontos de acesso para gerenciar a associação de endereços.

Fazio et al. apresentam problemas relacionados à atribuição de endereços IP por Unidades de Acostamento (RSUs) espalhadas pela estrada. O DHCP, por exemplo, não é eficiente em redes veiculares se empregado na forma tradicional. Caso RSUs isoladas sejam utilizadas como servidores DHCP, um veículo pode receber um endereço do ponto de acesso em seu alcance, que já está sendo utilizado por outro veículo servido por um segundo ponto de acesso. Portanto, a RSU garantirá unicidade do endereço apenas em sua área de alcance. Devido à característica ad hoc das redes veiculares, esse esquema de endereçamento não é apropriado. Nas redes veiculares, a rede se estende para além do alcance das RSUs, impossibilitando a atribuição de endereço aos nós a mais de um salto dos pontos de acesso. Uma possível solução é utilizar um DHCP adaptado às redes de múltiplos saltos. Entretanto, essa solução pode inserir outros problemas relacionados à descoberta de pontos de acesso, sincronização de informação entre RSUs, distância entre veículos e RSUs, e ainda atrasos na comunicação.

O protocolo VAC (*Vehicular Address Configuration*) considera a necessidade da comunicação em tempo real [Fazio et al. 2007]. Para isso, é utilizada a estratégia baseada em líder, qualquer nó da rede possui acesso direto a pelo menos um nó líder. Os líderes são escolhidos dinamicamente e fornecem serviço de DHCP distribuído, assegurando a unicidade de endereços IP em um determinado escopo. Esse escopo consiste na união das regiões de alcance de um determinado número de líderes que trocam informações entre si, sendo responsáveis por diferentes conjuntos de endereços. A divisão da VANET em regiões reduz o tráfego de controle. Essa abordagem pode ser empregada no suporte às aplicações que necessitam de comunicação entre veículos em apenas uma determinada região como, por exemplo, as aplicações de segurança no trânsito. Aplicações que necessitam de endereçamento global, entretanto, não podem utilizar a divisão de rede proposta. No protocolo VAC há também a necessidade de verificação de duplicidade de endereço quando um nó se move de um escopo para outro. Portanto, a eficiência do protocolo depende, além de outros fatores, da velocidade relativa entre os líderes e os nós pertencentes a um escopo.

O modo infraestruturado também pode ser usado para atribuição de endereços. Para tal, é proposto o uso de um servidor DHCP centralizado para contornar problemas do VAC, como duplicidade de endereços e necessidade de todos os nós possuírem capacidade de serem líderes [Mohandas e Liscano 2008]. Segundo os autores, esse último problema deve ser considerado, pois ao se tornar líder, um nó consome mais recursos computacionais que o normal. A proposta de Mohandas e Liscano utiliza RSUs conectadas a um servidor DHCP central que controla a distribuição de endereços. A desvantagem dessa arquitetura é a necessidade de elementos fixos e a utilização de uma entidade gerenciadora de endereços, como governo ou concessionárias de vias.

O GeoSAC (*Geographically Scoped stateless Address Configuration*) [Baldessari et al. 2008] consiste na adaptação de mecanismos do SLAAC (*Stateless Address Autoconfiguration*) do IPv6 para serem utilizados com endereçamento geográfico. Na arquitetura considerada no trabalho, uma camada abaixo da camada de rede é responsável pelo roteamento geográfico e apresenta para o IPv6 uma topologia planificada. Utilizando essa arquitetura, o enlace visto pelo IPv6 possui nós que não estão diretamente conectados, mas que fazem parte de uma área geográfica relacionada a um ponto de acesso. Com isso, a camada abaixo da camada de rede apresenta um enlace IPv6 multidestinatário que

consiste em um particionamento da rede veicular constituído por todos os nós de uma determinada área geográfica. Esse mecanismo pode ser utilizado para contornar o problema do ponto de acesso só possuir controle de endereçamento dos nós que estão ao seu alcance, como exposto anteriormente. No GeoSAC um ponto de acesso envia mensagem de anúncio de roteador (*Router Advertisement* - RA) para todos os nós de uma determinada área. Devido a um mecanismo de encaminhamento geográfico utilizado pelos nós, a mensagem pode também alcançar os nós que estejam a mais de um salto do ponto de acesso, mas dentro de uma área geográfica limitada. De acordo com o SLAAC, cada nó pode gerar seu endereço anexando o identificador de rede, oriundo de seu endereço MAC, ao prefixo IPv6 recebido no RA. Em seguida, o nó verifica a duplicidade de endereço.

5.7.2. Simulação

A realização de testes de desempenho em redes veiculares pode exigir um grande número de pessoas, custos elevados e ainda necessitar condições climáticas e ambientes favoráveis. Além disso, a repetição de um determinado experimento em um ambiente com muitas variáveis é difícil. Embora a utilização de simulações seja uma alternativa atrativa por ser um ambiente controlado e por consumir menos recursos, a reprodução de condições similares às encontradas em campo é um desafio.

A simulação de redes veiculares é uma tarefa complexa, pois envolve modelar a propagação de sinais, a disputa do acesso ao meio e diversos outros protocolos de redes. Além disso, trata de uma rede móvel, para a qual devem ser desenvolvidos modelos de mobilidade específicos.

Grande parte das soluções propostas utiliza um simulador de redes já consagrado em conjunto com um simulador de mobilidade ou com outro tipo de *software*. Alguns dos simuladores mais utilizados para redes móveis são o ns-2 (*The Network Simulator*) e o GloMoSim (*Global Mobile Information System Simulator*). O ns-2 [Fall e Varadhan 2002] é um simulador de redes de propósito geral, possui código aberto e está em constante desenvolvimento. O ns-2 ainda não implementa o padrão IEEE 802.11p, mas já existem trabalhos que modificam o simulador incluindo alguns recursos desse padrão [Gukhool e Cherkaoui 2008]. O GloMoSim [Bajaj et al. 1999] é um simulador de redes que implementa diversos protocolos e é utilizado apenas para simular o comportamento das redes sem-fio.

Apesar do esforço em tornar as simulações mais realistas, alguns pontos ainda são muito simplificados. Por exemplo, o módulo de propagação sem-fio do ns-2 original tem disponível apenas três modelos. O mais simples deles é o modelo de espaço livre que calcula a atenuação do sinal apenas em função da distância entre os nós. O modelo de dois raios possui o funcionamento semelhante ao modelo de espaço livre, mas considera a reflexão do sinal no solo a partir de uma determinada distância entre o par origem-destino. Essa distância é calculada em função das alturas das antenas em relação ao solo. O terceiro é o modelo de sombreamento que, diferente dos modelos anteriores, não calcula a atenuação de forma determinística. O modelo de sombreamento considera também os efeitos do desvanecimento que são modelados segundo uma distribuição log-normal.

Um modelo de mobilidade que se tornou bastante utilizado nas simulações de redes móveis é o modelo *Random Waypoint*. Nesse modelo os nós movimentam-se sobre

uma sequência de segmentos de reta. Em cada trajeto os nós trafegam com uma velocidade aleatória e pode parar no ponto final do segmento durante um tempo de pausa também aleatório. Quando um nó chega ao destino, ele aguarda o tempo de pausa antes de começar seu movimento para o próximo ponto. O modelo *Random Waypoint* não é realista para redes veiculares, pois os veículos movimentam-se apenas dentro das vias.

Simuladores específicos para redes veiculares estão sendo propostos. Uma das principais características levadas em consideração nesses simuladores é o tráfego de veículos. Os simuladores de movimentação de veículos podem ser classificados em microscópicos ou macroscópicos. O primeiro tipo considera o comportamento de cada veículo durante a simulação. Já o segundo, utiliza parâmetros gerais de tráfego, tais como velocidade média ou quantidade de veículos que trafegam na via.

A ferramenta MOVE (*MObility model generator for VEhicular networks*) automatiza a criação de modelos de mobilidade para redes veiculares [Karnadi et al. 2007]. Essa ferramenta utiliza um editor de mapas de estradas e um editor de movimentação de veículos. Com o editor de mapas, o usuário pode criar mapas manualmente, gerá-los automaticamente ou ainda importar mapas reais. O editor de movimentação de veículos permite que o usuário adicione as rotas de cada veículo para o mapa gerado anteriormente. Na versão mais recente do MOVE, o editor de movimentação de veículos pode ser substituído pelo simulador de tráfego SUMO [Krajzewicz et al. 2002] que gera as rotas dos veículos automaticamente. A partir do mapa e das movimentações geradas, o MOVE gera arquivos de trajetórias que podem ser utilizados por simuladores como o ns-2 e o QualNet [S.N. Technologies 2004]. Esse último é um produto comercial baseado no GloMoSim.

O simulador de movimentação SUMO (*Simulation of Urban Mobility*) é um simulador microscópico de tráfego urbano utilizado em algumas soluções de simulação para redes veiculares. O SUMO simula a movimentação de diferentes tipos de veículos sem a ocorrência de colisões e suporta vias de múltiplas faixas de rolamento. O funcionamento do SUMO é baseado em um modelo de comportamento dos motoristas combinado com os controladores de tráfego presentes nas vias. O simulador possui código aberto.

Gorgorin et al. desenvolveram uma ferramenta para simular a movimentação dos veículos, a transmissão e a recepção dos pacotes de dados, e a recepção de informações de posicionamento do GPS [Gorgorin et al. 2006]. Esse simulador utiliza um sistema de fila de eventos, em que o envio e a recepção de pacotes e a recepção dos dados do GPS são controlados por essa fila. Em intervalos regulares de tempo, um evento de recepção do GPS é disparado e passado para cada veículo, exatamente da mesma forma em que acontece nas aplicações reais para redes veiculares. O evento de envio de pacotes é chamado por um veículo e a recepção desse pacote é agendada levando em consideração a propagação do sinal. O módulo de mobilidade atualiza a posição de cada veículo com base nos parâmetros de seu modelo de mobilidade.

Simuladores de tráfego que enviam informações para o simulador de redes e não recebem retorno são chamados centrados na rede. Para algumas aplicações de redes veiculares, entretanto, é necessário que o motorista obtenha as informações pela rede para tomar decisões de mudança de trajeto. Simuladores de tráfego cujo módulo de tráfego obtém informações do módulo de redes são conhecidos como centrados na aplicação. A

maior parte dos simuladores de tráfego é centrado na rede. O TraNS (*Traffic and Network Simulation Environment*) [Piórkowski et al. 2008], entretanto, pode ser utilizado tanto centrado na rede quanto na aplicação. O TraNS é uma ferramenta de simulação que utiliza o ns-2 e o SUMO. Além disso, com essa ferramenta é possível testar a influência das aplicações para redes veiculares no comportamento do tráfego de veículos. Isso é possível devido ao TraCI (*Traffic Control Interface*), um módulo de interface que faz a ligação entre o simulador de redes e o simulador de tráfego. O TraCI envia comandos de mobilidade para o simulador de tráfego podendo realimentar o simulador de redes com novos modelos de mobilidade. Outra vantagem desse simulador é a presença de um arcabouço para desenvolvimento de aplicações.

Por último, Wang e Lin desenvolveram o simulador de redes NCTUns [Wang e Lin 2008] que já possui módulos de simulação para o protocolo IEEE 802.11p. Esse simulador possui uma interface que permite a criação de nós na rede e trajetos dos veículos. Além disso, permite a edição dos parâmetros dos nós e a simulação do tráfego de pacotes e do movimento dos veículos. O NCTUns utiliza os próprios protocolos do kernel do Linux para realizar a simulação, proporcionando uma simulação mais realista e permitindo a emulação de redes, a criação de trajetórias para os veículos e a utilização de implementações reais de *softwares* para Linux em alguns nós da rede simulada.

5.7.3. Transporte

O desempenho da camada de transporte em redes veiculares ainda é pouco explorado na literatura. Entretanto, já existem diversos trabalhos sobre esse tema em redes ad hoc [Liu e Singh 2001, Chandran et al. 2001]. Esses trabalhos podem servir como um ponto de partida já que essas redes possuem características em comum.

Um dos maiores desafios das redes veiculares e das redes sem-fio em geral é o emprego dos protocolos da camada de transporte desenvolvidos para as redes cabeadas. A adaptação do TCP ao ambiente sem-fio é o principal exemplo. Uma das funções do TCP é prover confiabilidade. Nas redes cabeadas, as taxas de erro binárias (*Bit Error Rate* - BER) são desprezíveis e as perdas de pacotes ocorrem principalmente devido a congestionamentos na rede e posterior descarte em filas. Essas falhas são tratadas pelo TCP por algoritmos de controle de fluxo e de congestionamento baseados no envio pelo destinatário de reconhecimentos positivos (*acknowledgement* - ACKs). Caso não haja o recebimento de ACKs pela fonte, o controle de congestionamento do TCP reduz a taxa de transmissão de pacotes. Esta abordagem não é válida para as redes sem-fio, pois diferente das redes cabeadas, as falhas ocorrem principalmente devido às taxas de erro binárias elevadas, instabilidades do canal e mobilidade dos nós [Tian et al. 2005]. Assim, não diferenciar entre congestionamento e outros tipos de erro, pode levar a uma queda desnecessária de desempenho do TCP. Nas redes veiculares, além do problema do TCP comum às redes sem-fio, há o agravante dos tempos de contato serem curtos. O TCP antes de iniciar a transferência de dados, passa por uma fase de estabelecimento de conexão. Essa fase exige um tempo mínimo que pode ser maior que o tempo de contato entre os veículos. O uso do TCP, portanto, deve levar em conta mais essa característica.

Diversos trabalhos propõem modificações para o TCP ou mesmo novos protocolos para melhorar o desempenho da camada de transporte nas redes sem-fio. Esses protocolos

operam no tradicional modo fim-a-fim ou no modo particionado [Tian et al. 2005]. Esse último considera a heterogeneidade da rede. A conexão pode ser separada em um roteador intermediário, protegendo a rede cabeada das perdas das redes sem-fio [Bakre e Badrinath 1995]. Esse método tem como desvantagem, porém, a violação do argumento fim-a-fim do TCP.

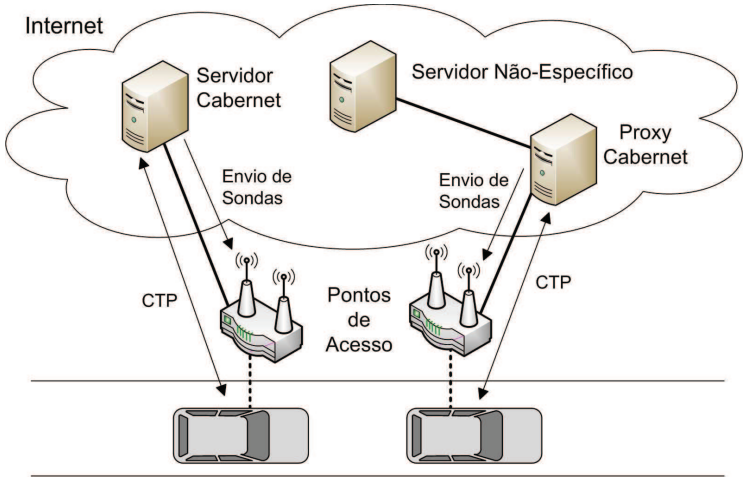


Figura 5.12. Arquitetura da Cabernet [Eriksson et al. 2008].

No caso específico das redes veiculares, uma proposta alternativa para a camada de transporte é a Cabernet. A Cabernet é uma rede provedora de conteúdo que utiliza pontos de acesso IEEE 802.11 não modificados [Eriksson et al. 2008]. Esses pontos de acesso são usados para transferir e receber dados de veículos utilizando servidores específicos, como mostrado na Figura 5.12. A Cabernet propõe um mecanismo de associação de veículos aos pontos de acesso, bem como o protocolo de transporte CTP (*Cabernet Transport Protocol*). Esse protocolo aumenta a taxa de transferência em enlaces sem-fio, diferenciando perdas por erros binários das perdas por congestionamento. O CTP considera que perdas por congestionamento só ocorrem na parte cabeada da rede, como no caminho entre o ponto de acesso e um servidor, reduzindo a taxa de transmissão somente quando detectar falhas nesse caminho. Assumindo ainda que não há terminais escondidos, e portanto as perdas por colisões são negligenciadas, as perdas no meio sem-fio são devidas apenas a erros de transmissão. Para diferenciar falhas na rede cabeada de falhas na rede sem-fio, o emissor CTP envia sondas para o ponto de acesso nessa parte da rede. A fração de perdas das sondas é utilizada como estimativa da fração de perdas por congestionamento. A taxa de transmissão é ajustada de acordo com as perdas por congestionamento na região cabeada. Por outro lado, quando não há o recebimento de ACKs, o CTP apenas efetua a retransmissão dos dados, e não ajusta a taxa de transmissão como faria o TCP. Para prover conexão dos veículos aos servidores que não sejam específicos da Cabernet, esse projeto faz uso de um *proxy*. Esse elemento possui como função esconder de servidores da Internet a mobilidade das redes veiculares e atuar como interface entre o CTP e outros protocolos, como o TCP.

Outra proposta de camada de transporte para redes veiculares é o MCTP (*Mobile Control Transport Protocol*) [Bechler et al. 2005] que, da mesma forma que o CTP, utiliza pontos de acesso e o modo particionado na comunicação entre veículos e a Internet.

O MCTP implementa uma subcamada entre o TCP e a camada de rede, possuindo como ideia básica observar o fluxo de pacotes IP entre fonte e destino e reagir adequadamente. Com base nas informações recebidas e eventos causados pelo TCP, o MCTP é projetado para identificar situações de falhas nos enlaces sem-fio, congestionamentos, particionamentos de rede e desconexões da Internet. Essas situações definem uma máquina de estados que entra em operação após o estabelecimento de uma conexão pelo TCP. De acordo com o estado da comunicação, o MCTP controla os procedimentos de transmissão do TCP, assim como as retransmissões e os limites de tempo para uma conexão.

Como visto, a maioria dos problemas na camada de transporte está relacionada a características do TCP, como controle de congestionamento, de fluxo e estabelecimento de conexão. Por esses motivos, uma possível solução para problemas da camada de transporte em redes veiculares é o uso do UDP. Uma vez que o UDP não estabelece conexão e não faz controle de congestionamento nem de fluxo, o seu uso tem se tornado uma saída a curto prazo para as redes veiculares, sendo também recomendado no padrão IEEE 1609.3 [Alves et al. 2008].

5.7.4. Segurança

Como qualquer grande rede de computadores, as redes veiculares são susceptíveis a ataques por usuários ou nós mal intencionados. Tais ataques podem variar de uma simples escuta, em que um determinado usuário pode obter informações sobre outro usuário, a ataques mais poderosos, como no caso em que um conluio de nós modifica o conteúdo de mensagens sendo enviadas. Por exemplo, em aplicações de controle do tráfego, alguns veículos podem divulgar informações falsas aos outros veículos de modo que eles acabem utilizando um caminho diferente.

Uma das maiores dificuldades para a implantação de redes veiculares é garantir o seu funcionamento mesmo diante de situações adversas e de atacantes mal intencionados. Para abordar esses problemas, várias propostas foram feitas [Sampigethaya et al. 2007, Pathak et al. 2008, Papadimitratos et al. 2008]. A maioria dessas propostas, tal como [Sampigethaya et al. 2007], trata de problemas específicos, como a autenticação e a privacidade dos nós da rede. No entanto, existem algumas propostas nas quais são descritas arquiteturas de segurança mais genéricas [Papadimitratos et al. 2008].

Em termos de segurança, as redes veiculares possuem desafios específicos. Entre os principais problemas, deve ser levado em conta que, em determinadas aplicações, a segurança da informação é mais crítica que na Internet, pois pode envolver a segurança de vidas humanas, por exemplo, em aplicações de sinalização de acidentes. Em outras aplicações, a informação de trajetória pode ser utilizada para algum tipo de otimização. Por exemplo, para prever contatos com outros veículos [Cavalcanti et al. 2008], o anonimato é fundamental [Papadimitratos et al. 2008]. É indesejável que um atacante tenha acesso à informação sobre a trajetória de um indivíduo, pois essa informação pode ferir a privacidade da vítima ou mesmo, ser utilizada para ataques pessoais.

Antes de compreender os diversos ataques que podem ocorrer em redes veiculares, é útil classificar os adversários de acordo com as suas capacidades e métodos. Para este efeito, é utilizada a classificação apresentada em [Raya e Hubaux 2005], que considera três dimensões diferentes para os adversários de acordo com o seu estado de adesão, a sua

motivação e o seu método de ataque. O estado de adesão de um adversário define se ele é interno ou intruso. Um adversário interno é um membro legítimo da rede capaz de se comunicar com qualquer outro membro da rede de forma autenticada. Já um adversário do tipo intruso não é um membro legítimo da rede e, portanto, é mais limitado. Já a motivação de um atacante pode ser classificada como maliciosa ou racional. Um atacante malicioso é um adversário cuja principal motivação é perturbar o serviço de rede. Um atacante racional, por outro lado, visa benefícios pessoais e é, portanto, mais previsível. Por fim, o método usado para ataque pode ser dito ativo ou passivo. Enquanto um adversário ativo pode criar novas mensagens e modificar ou apagar mensagens que estão em trânsito, um adversário passivo é limitado às escutas.

Definidos os tipos de adversários possíveis em redes veiculares, é possível destacar três tipos de ataques: os ataques por desinformação, ataques por rastreamento e negação de serviço. Os ataques por desinformação são ataques ativos em que adversários internos divulgam informações falsas pela rede, seja com a intenção de perturbar o funcionamento da mesma ou para obter ganhos pessoais [Parno e Perrig 2005, Raya e Hubaux 2005]. Um exemplo desse ataque é a formação de um conluio de veículos para transmitir informações falsas sobre as condições de tráfego, e assim, desviar o tráfego de uma determinada via. Outro exemplo de ataque por desinformação é aquele em que um determinado nó da rede mente sobre a sua identidade e se faz passar por outro nó. Por último, também se enquadram nessa categoria ataques nos quais o adversário suprime seletivamente mensagens em trânsito com o intuito de perturbar o tráfego da rede. O segundo tipo de ataque mencionado corresponde aos ataques por rastreamento. Os ataques dessa categoria são ataques passivos em que o objetivo do adversário é monitorar a localização de um determinado veículo ou grupo de veículos e utilizar essa informação para fins diversos, variando desde uma simples geração de estatísticas de tráfego até assuntos de natureza jurídica, tais como decidir quem é o responsável por um determinado acidente [Raya e Hubaux 2005]. O último tipo de ataque é a negação de serviço que é comumente encontrado nas redes cabeadas. Esse é um ataque ativo no qual o adversário tenta perturbar o funcionamento da rede ou até mesmo derrubá-la, através da sobrecarga dos seus recursos. Alguns exemplos incluem a injeção de um grande número de mensagens na rede ou a geração de interferência no canal de comunicação [Parno e Perrig 2005, Raya e Hubaux 2005].

Como visto, as redes veiculares podem estar sujeitas a diversas formas de ataque. Dessa forma, torna-se importante identificar os requisitos de segurança necessários para proteger as redes veiculares dos ataques e garantir o funcionamento correto dessas redes. Alguns desses requisitos, como a garantia da integridade dos dados e autenticação dos nós da rede, são também comuns a outras redes, tais como redes ad hoc sem-fio. Outros, como a garantia da privacidade dos nós, são mais importantes para redes veiculares, já que essas redes podem revelar detalhes importantes sobre o deslocamento de um veículo.

Dentre os requisitos de segurança, os mais importantes no contexto de redes veiculares são autenticação dos nós, integridade e confidencialidade dos dados, anonimato, privacidade e controle de acesso. A autenticação dos nós é importante para evitar erros de identificação e tornar possível a distinção entre nós legítimos e intrusos. Isso é extremamente importante para verificar a identidade do remetente de cada mensagem recebida. A integridade dos dados é necessária para evitar que um atacante seja capaz de alterar

ou reutilizar mensagens legítimas. Além da integridade, a confidencialidade dos dados também é importante. Algumas aplicações em redes veiculares podem necessitar que o conteúdo da comunicação permaneça confidencial para evitar que alguns nós tenham acesso a dados aos quais eles não estão autorizados. Já o anonimato e a privacidade dos nós são necessários para evitar ataques por rastreamento e impedir que entidades não autorizadas sejam capazes de localizar ou rastrear a trajetória de um veículo ou grupo de veículos. Em especial, uma entidade não autorizada não deve ser capaz de saber se duas mensagens diferentes foram criadas pelo mesmo nó. O último requisito é o controle de acesso. A fim de garantir que cada nó só realize funções a que eles estejam autorizados, é necessário implementar uma política global para o controle de acesso.

Atualmente, muitas ferramentas para impedir os ataques descritos nesta seção vêm sendo propostas na literatura. Cada uma delas tem em vista pelo menos o cumprimento de um dos requisitos de segurança mencionados para as redes veiculares.

As assinaturas digitais e os códigos de autenticação de mensagem (MACs) podem ser utilizados a fim de garantir a autenticação de nós e a integridade dos dados. O uso de assinaturas digitais requer a criação de uma ou mais infraestruturas de chaves públicas (PKIs), cada uma gerida por uma autoridade certificadora (CA). O objetivo de uma CA é gerenciar as identidades e as credenciais de todos os nós nela registrados. O uso de códigos de autenticação de mensagens necessita que cada nó da rede pré-estabeleça uma chave secreta com qualquer um dos nós com os quais ele possa se comunicar. Uma das principais vantagens da utilização de assinaturas digitais é que elas gozam da propriedade de não repúdio, além de garantir a autenticação dos nós. Elas também não exigem que nós da rede estabeleçam previamente segredos em comum. Infelizmente, os algoritmos de geração e verificação de assinaturas não são tão eficientes como no caso do MAC. Além disso, o tamanho da assinatura também tende a ser maior do que a etiqueta de verificação gerada por um MAC. Uma vez que os nós em redes veiculares não são tão computacionalmente limitados em comparação com os nós de outras redes ad hoc, tais como redes de sensores, a maioria das soluções propostas até agora, tal como [Papadimitratos et al. 2008], se baseia na utilização de assinaturas. No entanto, existem algumas propostas que recomendam o uso de soluções híbridas envolvendo tanto assinaturas digitais como MACs, a fim de melhorar a eficiência global do sistema [Zhang et al. 2008].

Para atender ao requisito de privacidade dos nós nas redes veiculares, dois tipos de soluções têm sido propostas na literatura, baseadas em pseudônimos e baseadas em assinaturas de grupo. Na solução baseada em pseudônimos, cada nó possui um conjunto de pseudônimos associado a ele. Um pseudônimo é uma chave pública, cujo certificado não contém qualquer informação que possa identificar o nó. Para assinar as mensagens usando um pseudônimo, o nó simplesmente usa a chave secreta correspondente. Como não é difícil determinar se duas assinaturas diferentes foram geradas com o mesmo pseudônimo, cada pseudônimo deve ser utilizado por apenas um curto espaço de tempo. Eles devem ser descartados logo em seguida para evitar que atacantes possam rastrear a localização de um nó. Para poder revogar o anonimato de um nó, a CA deve manter uma lista de todas as identidades e pseudônimos para as quais tenha emitido um certificado.

Em uma solução baseada em assinaturas de grupo, os nós de rede são divididos em grupos e a cada grupo uma única chave pública é associada. Apesar da chave pública

ser única, a cada usuário do grupo é dada uma chave secreta diferente para gerar assinaturas. Uma das principais características de assinaturas de grupo é que, apesar de qualquer membro do grupo ser capaz de assinar mensagens em nome do grupo, é impossível saber se duas assinaturas diferentes foram geradas pelo mesmo membro do grupo.

A principal vantagem de utilizar uma solução baseada em pseudônimos é que os algoritmos de assinatura e de verificação são mais eficientes do que os utilizados em assinaturas de grupo. Por essa razão, a maioria das soluções até agora propostas se baseiam na utilização de pseudônimos. No entanto, como salientado acima, soluções baseadas em pseudônimos não fornecem o mesmo nível de anonimato que aquelas baseadas em assinaturas de grupo, pois não é difícil determinar se duas assinaturas diferentes foram geradas com o mesmo pseudônimo. Como resultado, algumas propostas [Raya e Hubaux 2005] recomendam a utilização de soluções híbridas envolvendo pseudônimos e assinaturas de grupos, visando uma solução global mais eficaz.

Embora a maioria das aplicações vislumbradas para redes veiculares não necessitem que seus dados permaneçam confidenciais, pode haver alguns casos em que o canal de comunicação deve permanecer privado. Nesses casos, tanto um algoritmo de encriptação com chaves públicas, se uma PKI já estiver disponível, como um algoritmo de encriptação com chaves privadas podem ser usados.

Finalmente, para evitar que a chave secreta de nós honestos caia nas mãos dos adversários, é extremamente importante mantê-las armazenadas em um local seguro. Por esta razão, a maioria das soluções encontradas na literatura recomenda o uso de memórias protegidas e a prova de falsificação e alteração.

5.7.5. Massa Crítica

A importância da arquitetura ad hoc nas redes veiculares pode ser vista pelo número de aplicações que assumem essa arquitetura. Entretanto, um dos desafios das aplicações que utilizam a comunicação V2V é a fase inicial de operação da rede, quando o número de usuários é pequeno. Redes veiculares puramente ad hoc sofrem diretamente o "efeito de rede", no qual o valor agregado da tecnologia para um usuário depende do número de usuários que possuem veículos equipados com a mesma tecnologia. Isso ocorre porque, para o funcionamento de diversas aplicações, é necessária uma conectividade mínima, que só é alcançada por um número mínimo de veículos equipados com a tecnologia [Panichpapiboon e Pattara-atikom 2008, Yousefi et al. 2008].

Duas alternativas básicas para promover a introdução de uma tecnologia no mercado são o aumento de seu valor agregado e a adoção de leis que tornem obrigatório o seu uso. Essa última não se aplica às redes veiculares, pois é necessário provar a efetividade da lei antes dessa ser sancionada. A prova consiste em demonstrar os benefícios da tecnologia, o que demanda certo grau de conectividade da rede. Logo, o auxílio do poder legislativo não constitui uma alternativa viável para dar início ao uso das redes veiculares, mas pode ser uma alternativa para difundir a utilização dessas redes em uma segunda fase de implantação. O aumento do valor agregado é, então, a alternativa mais adequada. Nesse caso, porém, diversas implicações ocorrem principalmente devido ao efeito de rede observado. Os consumidores só irão equipar seus veículos com a tecnologia de rede veicular quando puderem usufruir dela. Por sua vez, esse usufruto só irá acontecer após a

adesão de certo número de consumidores à tecnologia, constituindo um ciclo vicioso que pode adiar a penetração da tecnologia no mercado [Matheus et al. 2004].

Apesar das implicações citadas, o valor agregado pode crescer com o surgimento de aplicações que não necessitem da comunicação direta entre veículos. Essas aplicações podem utilizar as RSUs para oferecer serviços a diferentes grupos de interesse, incentivando consumidores a equiparem seus veículos com a tecnologia de rede veicular. A implantação de redes veiculares infraestruturadas envolve, porém, custos que podem ser elevados. Existe ainda uma questão em aberto sobre que entidades devem financiar tal infraestrutura, dentre elas estão as concessionárias de vias, o governo e os usuários. Outra alternativa para o aumento de usuários de redes veiculares é a utilização de equipamentos comuns, como computadores portáteis e PDAs, no interior dos veículos [Alves et al. 2008]. Nessa abordagem não há necessidade de investimento financeiro adicional pelo usuário, devido à larga utilização desses dispositivos, o que configura um incentivo a novos usuários. Além das citadas, são propostas alternativas como incentivar a implantação de unidades básicas, que apenas encaminham pacotes, em todos os veículos e conceder bônus, como redução de impostos, aos consumidores que optarem por equipar seus veículos com a tecnologia de redes veiculares [Matheus et al. 2004].

Um estudo realizado na Alemanha [Matheus et al. 2004] mostra a dificuldade de penetração das redes veiculares no mercado. Nesse estudo é citado que, no exemplo de aplicações de segurança no trânsito, pelo menos 10% dos veículos do país necessitam estar equipados com a tecnologia de redes veiculares. Segundo esse mesmo estudo, se todos os veículos novos na Alemanha saíssem de fábrica com a tecnologia, a porcentagem necessária seria atingida em um ano e meio. Se apenas 50% dos novos veículos fossem equipados com a tecnologia, o período seria de três anos. O trabalho também aponta que veículos corporativos são revendidos em média após dois anos e meio a partir de sua data da compra. Isso significa que proprietários poderiam revender seus veículos com uma tecnologia que eles não utilizaram. É importante, então, incentivar indústrias automobilísticas a integrarem a tecnologia de rede veicular em seus automóveis. Mesmo assim, alguns desafios podem surgir como o fato de uma indústria não encontrar benefícios se implementar sozinha a tecnologia de redes veiculares em seus automóveis.

5.8. Experimentos de Campo

Atualmente, muitos esforços em redes veiculares estão voltados para experimentos de campo. Com base em resultados práticos, é possível verificar que aplicações atuais se adaptam às condições dessas redes e quais as modificações necessárias para que outras aplicações possam também ser utilizadas. Em geral, as características que mais influenciam o desempenho das aplicações nas redes veiculares são o tempo de contato entre veículos, as condições de transmissão sem-fio, o tempo de adaptação ou reação dos algoritmos e protocolos envolvidos e o uso de protocolos e soluções legados das redes cabeadas.

Nos experimentos deste trabalho, define-se tempo de contato como o intervalo entre o primeiro e o último pacotes de dados recebidos. Esse tempo pode ser muito curto, já que as velocidades dos nós das redes veiculares podem ser elevadas. Além disso, não somente o módulo da velocidade deve ser considerado, mas também a direção e o sentido

do deslocamento.

O aumento da capacidade das redes veiculares é alcançado através da maximização da quantidade de dados transferidos durante um contato. Uma forma trivial é aumentar o tempo de contato entre os nós. Para isso, pode-se aumentar o alcance de transmissão com antenas direcionais ou maior potência de transmissão. Pode-se também projetar soluções para aproveitar de forma mais eficiente o tempo de contato disponível, mesmo que esse seja curto. Para isso, é preciso lidar com os problemas relacionados com a transmissão no meio sem-fio para aprimorar a robustez e a eficiência das transmissões. Técnicas de processamento de sinais podem ser utilizadas com esse propósito. Dentre essas técnicas estão o uso de antenas MIMO (*Multiple Input Multiple Output*) que podem aprimorar o desempenho das redes sem-fio em geral, mas a avaliação delas não é abordada neste trabalho. Outra maneira de aumentar a capacidade das redes veiculares ocorre através da redução do tempo de adaptação dos algoritmos e protocolos envolvidos. Uma vez que eles consigam reagir de forma mais rápida, a quantidade de dados transferidos é maior, pois a configuração corrente torna-se mais próxima à ideal. Muitos dos protocolos utilizados, entretanto, ainda são os mesmos das redes cabeadas, nas quais a variação das condições ocorre de forma mais lenta. O IEEE 802.11p é uma iniciativa que está em fase de padronização (Seção 5.3.1.5). Entretanto, além desse novo padrão, são também necessários novos protocolos de camadas superiores, como novos protocolos de roteamento e transporte. Considerando o estado atual, uma maneira de testar o desempenho das redes veiculares é utilizar os equipamentos de prateleira disponíveis.

A aplicação escolhida para os primeiros testes foi a transferência de arquivos entre veículos [Alves et al. 2008]. O objetivo é avaliar a viabilidade das redes veiculares para aplicações comuns. Dados os conhecidos problemas do TCP em redes sem-fio, o primeiro teste com protocolos da Internet foi com o UDP. Além disso, analisa-se o desempenho das extensões do padrão IEEE 802.11 e de parâmetros como a velocidade dos veículos e o tamanho dos pacotes de dados transferidos. A plataforma de testes é composta por computadores portáteis IBM T42, equipados com interfaces sem-fio Linksys WPC54G (IEEE 802.11 a/b/g) baseadas em chipset Atheros. Os computadores são levados ao colo do passageiro e antenas externas não são utilizadas. Como sistema operacional, é utilzado o Linux com kernel versão 2.6.22-22-686 e *driver* Madwifi versão 0.9.3.3. Alguns parâmetros do algoritmo de seleção de taxa de bits chamado `SampleRate` padrão são ajustados. Esses ajustes foram realizados conforme sugerido em [Hadaller et al. 2007] para aumentar a reação do algoritmo em período de rápidas mudanças. Para o envio de dados e medição da qualidade do enlace, foi utilizada a ferramenta de geração de tráfego `Iperf` em sua versão 2.0.2.

Alguns parâmetros foram ajustados antecipadamente, para evitar atrasos extras devido à configuração e aumentar o tempo de contato. Os endereços IP dos portáteis foram fixados e os endereços MAC dos portáteis foram adicionados a um arquivo de configuração do ARP (*Address Resolution Protocol*). Assim, evita-se que haja requisições a endereços MAC. Foram também fixados o identificador da rede (*Extended Service Set ID* - ESSID) e o canal de operação do IEEE 802.11.

Os testes foram realizados em uma rua reta de 400 metros de extensão no *campus* da UFRJ (Universidade Federal do Rio de Janeiro) sob tráfego de carros leve. As posições

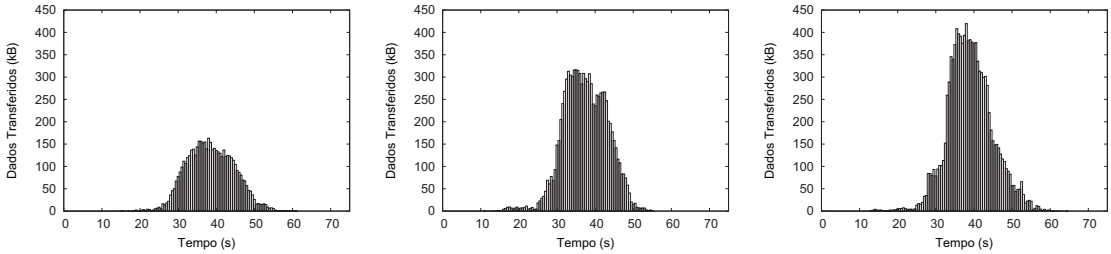
iniciais dos carros são distantes o suficiente para que cada nó esteja fora da área de cobertura do outro. Nenhuma outra rede IEEE 802.11 que pudesse interferir nos resultados foi encontrada em operação nessa área, exceto alguns sinais fracos em outros canais detectados fora da região em que os dados são transferidos. A velocidade de ambos os carros foi variada entre 20 e 60 km/h, alterando, assim, a velocidade relativa entre 40 e 120 km/h. Um dos carros utiliza o `Iperf` como servidor e o outro como cliente. Em ambos os casos o cliente envia dados e o servidor conta a quantidade recebida a cada 500 ms.

Os computadores portáteis foram sincronizados, antecipadamente, utilizando o protocolo NTP (*Network Time Protocol*). Os carros partiam no mesmo instante e tanto o cliente quanto o servidor eram lançados imediatamente. Ambos os carros movem-se pela margem direita da rua à mesma velocidade e cruzam-se aproximadamente no meio da rua. Todos os resultados utilizaram como instante de referência o momento $t = 0$, no qual os carros começam a se movimentar.

5.8.1. Medidas de Capacidade da Rede

Por economia de espaço, apenas os resultados com o IEEE 802.11g são apresentados, já que o uso do IEEE 802.11a apresentou pior desempenho nesse cenário. O IEEE 802.11a opera em uma faixa de frequência mais alta e por isso está mais sujeito a atenuação.

Cada configuração (padrão IEEE 802.11, velocidade do veículo e tamanho de pacote) foi testada 10 vezes. Os resultados mostram o valor médio das 10 rodadas. A métrica avaliada foi a quantidade de dados recebida durante o contato dos dois veículos.



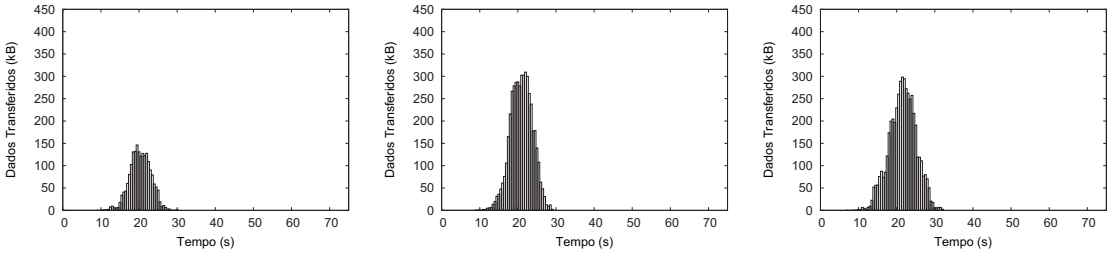
(a) Pacotes de 150 bytes. (b) Pacotes de 500 bytes. (c) Pacotes de 1460 bytes.

Figura 5.13. Média de dados transferidos sobre UDP utilizando IEEE 802.11g a 20 km/h.

A Figura 5.13 mostra a quantidade média de dados recebidos pelo carro que executa o servidor `Iperf`, quando ambos os carros estão em movimento a 20 km/h. Como mostra a Tabela 5.4, o tempo médio de contato é de aproximadamente 35 segundos. Note que esse valor de tempo não pode ser medido diretamente da figura, devido aos inícios dos contatos das 10 rodadas não começarem ao mesmo tempo, e porque caixas menores que 1 kbyte não são visíveis. Observa-se que o pico de vazão é de 6,4 Mbps obtido com pacotes de 1460 bytes. É importante recordar que cada ponto da curva mostra dados acumulados, em kbytes, em um período de 500 ms.

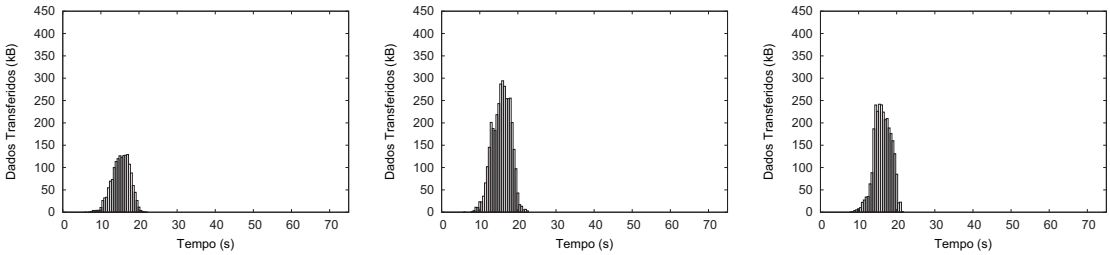
Ao aumentar a velocidade dos carros para 40 km/h, a utilização de pacotes de 1460 bytes ainda permite transferir mais dados durante o cruzamento. Todavia, como visto na Figura 5.14, a diferença é menor do que com 20 km/h. Nesse último caso, o tempo de contato é de aproximadamente metade do encontrado no caso anterior. Já a

vazão máxima, ilustrada nas Figuras 5.14(b) e 5.14(c), é de aproximadamente 4,8 Mbps. Experimentos com carros movimentando-se a 60 km/h também foram realizados. Os resultados são mostrados na Figura 5.15.



(a) Pacotes de 150 bytes. (b) Pacotes de 500 bytes. (c) Pacotes de 1460 bytes.

Figura 5.14. Média de dados transferidos sobre UDP utilizando IEEE 802.11g a 40 km/h.



(a) Pacotes de 150 bytes. (b) Pacotes de 500 bytes. (c) Pacotes de 1460 bytes.

Figura 5.15. Média de dados transferidos sobre UDP utilizando IEEE 802.11g a 60 km/h.

A Tabela 5.4 mostra o total de dados transferidos entre os dois veículos. Observa-se que quanto maior a velocidade, menor o impacto do tamanho do pacote no total de dados transferidos. No caso em que os carros se movimentam a 60 km/h, podemos observar ainda uma leve diminuição nesse valor: 3,5 Mbytes de dados foram transferidos utilizando pacotes de 500 bytes, enquanto que somente 2,8 Mbytes de dados foram transferidos utilizando pacotes de 1460 bytes. Essas medidas indicam um compromisso entre o tamanho do pacote e a velocidade. A vazão apresentada na tabela é a média das vazões medidas em cada rodada pelo `Iperf`. Essa média foi calculada para cada intervalo de 500 ms. Conforme a Tabela 5.4, o valor da vazão média (calculado sobre as 10 rodadas) é aproximadamente o mesmo quando a velocidade varia e o tamanho do pacote é mantido. Entretanto, considerando valores de desvio padrão (denotado por σ), as variações em vazão não são significativas. Logo, a redução da quantidade de dados recebidos quando a velocidade aumenta é devida principalmente a um tempo de contato mais curto.

5.9. Considerações Finais

As redes veiculares possibilitam uma série de aplicações que podem tornar a experiência de dirigir mais segura, já que evitam colisões; mais eficiente, já que reduzem o tempo de viagem, evitam congestionamentos e aumentam a capacidade das vias; e mais agradável, já que proporcionam novas aplicações de entretenimento. Entretanto, as características dessas redes impõem desafios ao seu desenvolvimento. Além dos problemas inerentes ao meio de transmissão sem-fio, nas redes veiculares, há ainda a alta mobilidade

Tabela 5.4. Média de dados transferidos, tempo de contato e vazão.

Velocidade (km/h)	Tamanho do Pacote (bytes)	Dados Transferidos (Mbytes)	Tempo de Contato (segundos)	Vazão (Mbps)
20	150	4,9 (σ=0,89)	35,95 (σ=6,12)	0,73 (σ=0,12)
	500	9,2 (σ=1,23)	33,95 (σ=5,42)	1,42 (σ=0,18)
	1460	10,8 (σ=3,36)	37,40 (σ=4,99)	1,60 (σ=0,49)
40	150	1,9 (σ=0,38)	15,60 (σ=3,24)	0,58 (σ=0,10)
	500	4,6 (σ=0,51)	17,05 (σ=2,91)	1,33 (σ=0,16)
	1460	4,8 (σ=1,64)	16,65 (σ=2,79)	1,39 (σ=0,53)
60	150	1,6 (σ=0,41)	11,70 (σ=1,70)	0,64 (σ=0,18)
	500	3,5 (σ=1,15)	11,95 (σ=2,48)	1,37 (σ=0,48)
	1460	2,8 (σ=1,66)	10,50 (σ=1,74)	1,12 (σ=0,61)

dos nós. Essa última característica pode tornar as redes veiculares altamente instáveis, já que o número de quebras de enlaces tende a ser maior. Esse cenário demonstra a necessidade de novos protocolos e mecanismos que levem em conta já em um primeiro momento as limitações dessas redes. Caso contrário, o desempenho obtido poderá ser aquém do exigido pelas novas aplicações.

Como visto neste capítulo, não obstante o crescente número de trabalhos na área, há ainda um enorme caminho a ser trilhado em pesquisa até que as redes veiculares possam atender de forma satisfatória os requisitos das aplicações. Entretanto, o sucesso das redes sem-fio e o rápido aprimoramento que as tecnologias relacionadas vêm conquistando indicam que esse caminho é viável.

Agradecimentos

Trabalho realizado com recursos da CAPES, CNPq, FAPERJ, FUJB e FINEP.

Referências

[Ahmed e Kanere 2006] Ahmed, S. e Kanere, S. S. (2006). SKVR: scalable knowledge-based routing architecture for public transport networks. Em *ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, páginas 92–93.

[Alves et al. 2008] Alves, R. S., Abdesslem, F. B., Cavalcanti, S. R., Campista, M. E. M., Costa, L. H. M. K., Rubinstein, M. G., Amorim, M. D. e Duarte, O. C. M. B. (2008). Uma análise experimental da capacidade de redes ad hoc veiculares. Em *Simpósio Brasileiro de Telecomunicações (SBrT)*.

[Bajaj et al. 1999] Bajaj, L., Takai, M., Ahuja, R., Tang, K., Bagrodia, R. e Gerla, M. (1999). GloMoSim: A scalable network simulation environment. Relatório Técnico 990027, UCLA Computer Science Department.

[Bakre e Badrinath 1995] Bakre, A. e Badrinath, B. (1995). I-TCP: indirect TCP for mobile hosts. Em *International Conference on Distributed Computing Systems*, páginas 136–143.

[Baldessari et al. 2008] Baldessari, R., Bernardos, C. e Calderon, M. (2008). GeoSAC-scalable address autoconfiguration for VANET using geographic networking concepts. Em *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, páginas 1–7.

[Bechler et al. 2005] Bechler, M., Jaap, S. e Wolf, L. (2005). An optimized TCP for internet access of vehicular ad hoc networks. Em *NETWORKING 2005*, volume 3462/2005 de *Lecture Notes in Computer Science*, páginas 869–880. Springer Berlin / Heidelberg.

[Biswas et al. 2006] Biswas, S., Tatchikou, R. e Dion, F. (2006). Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. *IEEE Communications Magazine*, 44(1):74–82.

[Borgonovo et al. 2004] Borgonovo, F., Capone, A., Cesana, M. e Fratta, L. (2004). ADHOC MAC: new MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services. *Wireless Networks*, 10(4):359–366.

[Burgess et al. 2006] Burgess, J., Gallagher, B., Jensen, D. e Levine, B. N. (2006). MaxProp: Routing for vehicle-based disruption-tolerant networks. Em *IEEE Conference on Computer Communications (INFOCOM)*, páginas 1–11.

[Caliskan et al. 2006] Caliskan, M., Graupner, D. e Mauve, M. (2006). Decentralized discovery of free parking places. Em *ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, páginas 30–39.

[Camp 2005] Camp, T. (2005). Location information services in mobile ad hoc networks. Em *Handbook of Algorithms for Mobile and Wireless Networking and Computing*, Information Science Series, capítulo 14, páginas 317–339. Chapman & Hall/CRC.

[Cavalcanti et al. 2008] Cavalcanti, S. R., Campista, M. E. M., Abdesslem, F. B., Costa, L. H. M. K. e Amorim, M. D. (2008). VEER: Um algoritmo de seleção de pares em redes ad hoc veiculares. Em *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, páginas 315–328.

[Chandran et al. 2001] Chandran, K., Raghunathan, S., Venkatesan, S. e Prakash, R. (2001). A feedback-based scheme for improving TCP performance in ad hoc wireless networks. *IEEE Personal Communications*, 8(1):34–39.

[Chen e Cai 2005] Chen, W. e Cai, S. (2005). Ad hoc peer-to-peer network architecture for vehicle safety communications. *IEEE Communications Magazine*, 43(4):100–107.

[Cohen 2008] Cohen, B. (2008). The BitTorrent protocol specification. http://www.bittorrent.org/beps/bep_0003.html. Acessado em 20 de março de 2009.

[COMeSafety 2009] COMeSafety (2009). COMeSafety: A EU specific support activity. http://www.comesafety.org/index.php?id=100. Acessado em 13 de março de 2009.

[Deering e Hinden 1998] Deering, S. e Hinden, R. (1998). Internet protocol, version 6 (IPv6) specification. RFC 2460. http://www.ietf.org/rfc/rfc2460.txt.

[Dobias e Grabow 1994] Dobias, F. e Grabow, W. (1994). Adaptive array antennas for 5.8 GHz vehicle to roadside communication. Em *IEEE Vehicular Technology Conference (VTC)*, páginas 1512–1516.

[Eriksson et al. 2008] Eriksson, J., Balakrishnan, H. e Madden, S. (2008). Cabernet: vehicular content delivery using WiFi. Em *ACM International Conference on Mobile Computing and Networking (MobiCom)*, páginas 199–210.

[Fall e Varadhan 2002] Fall, K. e Varadhan, K. (2002). *The ns Manual (formerly ns Notes and Documentation)*. The VINT Project.

[Fazio et al. 2007] Fazio, M., Palazzi, C., Das, S. e Gerla, M. (2007). Facilitating real-time applications in VANETs through fast address auto-configuration. Em *IEEE Consumer Communications and Networking Conference (CCNC)*, páginas 981–985.

[Festag et al. 2008] Festag, A., Noecker, G., Strassberger, M., Lübke, A., Bochow, B., Torrent-Moreno, M., Schnaufer, S., Eigner, R., Catrinescu, C. e Kunisch, J. (2008). NoW - Network on Wheels: Project objectives, technology and achievements. Em *International Workshop on Intelligent Transportation (WIT)*.

[Franz et al. 2005] Franz, W., Hartenstein, H. e Mauve, M. (2005). *Inter-Vehicle-Communications Based on Ad Hoc Networking Principles - The FleetNet Project*. Universitätsverlag Karlsruhe, 1 edição.

[Gorgorin et al. 2006] Gorgorin, C., Gradinescu, V., Diaconescu, R., Cristea, V. e Iftode, L. (2006). An integrated vehicular and network simulator for vehicular ad-hoc networks. Em *European Simulation and Modelling Conference (ESM)*.

[Green 2000] Green, M. (2000). "How long does it take to stop?" Methodological analysis of driver perception-brake times. *Transportation Human Factors*, 2(3):195–216.

[Gukhool e Cherkaoui 2008] Gukhool, B. e Cherkaoui, S. (2008). IEEE 802.11 p modeling in ns-2. Em *IEEE Conference on Local Computer Networks (LCN)*, páginas 622–626.

[Guo et al. 2005] Guo, M., Ammar, M. H. e Zegura, E. W. (2005). V3: a vehicle-to-vehicle live video streaming architecture. Em *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, páginas 171–180.

[Hadaller et al. 2007] Hadaller, D., Keshav, S., Brecht, T. e Agarwal, S. (2007). Vehicular opportunistic communication under the microscope. Em *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, páginas 206–219.

[Hartenstein e Laberteaux 2008] Hartenstein, H. e Laberteaux, K. P. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, 46(6):164–171.

[Hein et al. 2002] Hein, G. W., Godet, J., Issler, J.-L., Martin, J.-C., Erhard, P., Lucas-Rodriguez, R. e Pratt, T. (2002). Status of galileo frequency and signal design. Em *International Technical Meeting of the Satellite Division of the Institute of Navigation ION GPS*, páginas 266–277.

[Hofmann-Wellenhof et al. 2008] Hofmann-Wellenhof, B., Lichtenegger, H. e Collins, J. (2008). *Global Positioning System (GPS): Theory and Practice*. Springer.

[IEEE Std 1609.1 2006] IEEE Std 1609.1 (2006). *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) – Resource Manager*. IEEE Vehicular Technology Society.

[IEEE Std 1609.2 2006] IEEE Std 1609.2 (2006). *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages*. Intelligent Transportation Systems Committee.

[IEEE Std 1609.3 2007] IEEE Std 1609.3 (2007). *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services*. Intelligent Transportation Systems Committee.

[IEEE Std 1609.4 2006] IEEE Std 1609.4 (2006). *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-channel Operation*. IEEE Vehicular Technology Society.

[Jaromczyk e Toussaint 1992] Jaromczyk, J. e Toussaint, G. (1992). Relative neighborhood graphs and their relatives. *Proceedings of the IEEE*, 80(9):1502–1517.

[Jiang e Delgrossi 2008] Jiang, D. e Delgrossi, L. (2008). IEEE 802.11p: Towards an international standard for wireless access in vehicular environments. Em *IEEE Vehicular Technology Conference (VTC-Spring)*, páginas 2036–2040.

[Karnadi et al. 2007] Karnadi, F. K., Mo, Z. H. e Lan, K.-C. (2007). Rapid generation of realistic mobility models for VANET. Em *IEEE Wireless Communications and Networking Conference (WCNC)*, páginas 2506–2511.

[Karp e Kung 2000] Karp, B. e Kung, H. (2000). GPSR: Greedy perimeter stateless routing for wireless networks. Em *ACM International Conference on Mobile Computing and Networking (MobiCom)*, páginas 243–254.

[Kasemann et al. 2002] Kasemann, M., Füβler, H., Hartenstein, H. e Mauve, M. (2002). A reactive location service for mobile ad hoc networks. Relatório Técnico TR-2002-014, Department of Computer Science, University of Mannheim.

[Korkmaz et al. 2004] Korkmaz, G., Ekici, E., Özgüner, F. e Ümit Özgüner Ekici (2004). Urban multi-hop broadcast protocol for inter-vehicle communication systems. Em *ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, páginas 76–85.

[Krajzewicz et al. 2002] Krajzewicz, D., Hertkorn, G., Rössel, C. e Wagner, P. (2002). SUMO (Simulation of Urban MObility) an open-source traffic simulation. Em *Middle East Symposium on Simulation and Modelling (MESM)*, páginas 183–187.

[LeBrun et al. 2005] LeBrun, J., Chuah, C.-N., Ghosal, D. e Zhang, M. (2005). Knowledge-based opportunistic forwarding in vehicular wireless ad hoc networks. Em *IEEE Vehicular Technology Conference (VTC-Spring)*, volume 4, páginas 2289–2293.

[Lee et al. 2007] Lee, K., Lee, S.-H., Cheung, R., Lee, U. e Gerla, M. (2007). First experience with CarTorrent in a real vehicular ad hoc network testbed. Em *Mobile Networking for Vehicular Environments (MOVE)*, páginas 109–114.

[Lee et al. 2008] Lee, K. C., Le, M., Harri, J. e Gerla, M. (2008). LOUVRE: Landmark overlays for urban vehicular routing environments. Em *IEEE Vehicular Technology Conference (VTC-Fall)*, páginas 1–5.

[Lee et al. 2006] Lee, U., Park, J.-S., Yeh, J., Pau, G. e Gerla, M. (2006). CodeTorrent: content distribution using network coding in VANET. Em *International Workshop on Decentralized Resource Sharing in Mobile Computing and Networking (MobiShare)*, páginas 1–5.

[Li e Wang 2007] Li, F. e Wang, Y. (2007). Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular Technology Magazine*, 2(2):12–22.

[Liu e Singh 2001] Liu, J. e Singh, S. (2001). ATCP: TCP for mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 9(7):1300–1315.

[Lochert et al. 2003] Lochert, C., Hartenstein, H., Tian, J., Füβler, H., Hermann, D. e Mauve, M. (2003). A routing strategy for vehicular ad hoc networks in city environments. Em *IEEE Intelligent Vehicles Symposium (IV)*, páginas 156–161.

[Lochert et al. 2005] Lochert, C., Mauve, M., Füβler, H. e Hartenstein, H. (2005). Geographic routing in city scenarios. *ACM SIGMOBILE Mobile Computing and Communications Review*, 9(1):69–72.

[Maihofer e Eberhardt 2004] Maihofer, C. e Eberhardt, R. (2004). Geocast in vehicular environments: caching and transmission range control for improved efficiency. Em *IEEE Intelligent Vehicles Symposium (IV)*, páginas 951–956.

[Maihofer et al. 2005] Maihofer, C., Leinmuller, T. e Schoch, E. (2005). Abinding geocast: Time-stable geocast for ad hoc networks. Em *ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, páginas 20–29.

[Mak et al. 2005] Mak, T. K., Laberteaux, K. P. e Sengupta, R. (2005). A multi-channel VANET providing concurrent safety and commercial services. Em *ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, páginas 1–9.

[Matheus et al. 2004] Matheus, K., Morich, R. e Lübke, A. (2004). Economic background of car-to-car communication. Em *Informationssysteme für mobile Anwendungen (IMA)*.

[Menouar et al. 2006] Menouar, H., Filali, F. e Lenardi, M. (2006). A survey and qualitative analysis of MAC protocols for vehicular ad hoc networks. *IEEE Wireless Communications Magazine*, 13(5):30–35.

[Mohandas e Liscano 2008] Mohandas, B. e Liscano, R. (2008). IP address configuration in VANET using centralized DHCP. Em *IEEE Conference on Local Computer Networks (LCN)*, páginas 608–613.

[Moraes et al. 2008] Moraes, I., Campista, M., Duarte, J., Passos, D., Costa, L., Rubinstein, M., de Albuquerque, C. e Duarte, O. (2008). On the impact of user mobility on peer-to-peer video streaming. *IEEE Wireless Communications Magazine*, 15(6):54–62.

[Nadeem et al. 2004] Nadeem, T., Dashtinezhad, S., Liao, C. e Iftode, L. (2004). TrafficView: traffic data dissemination using car-to-car communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 8(3):6–19.

[Namboodiri e Gao 2007] Namboodiri, V. e Gao, L. (2007). Prediction-based routing for vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 56(4):2332–2345.

[Nandan et al. 2005] Nandan, A., Das, S., Pau, G., Gerla, M. e Sanadidi, M. Y. (2005). Co-operative downloading in vehicular ad-hoc wireless networks. Em *IEEE Wireless On demand Network Systems and Services (WONS)*, páginas 32– 41.

[Naumov et al. 2006] Naumov, V., Baumann, R. e Gross, T. (2006). An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces. Em *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, páginas 108–119.

[Naumov e Gross 2007] Naumov, V. e Gross, T. R. (2007). Connectivity-aware routing (CAR) in vehicular ad-hoc networks. Em *IEEE Conference on Computer Communications (INFOCOM)*, páginas 1919–1927.

[Navda et al. 2007] Navda, V., Subramanian, A. P., Dhanasekaran, K., Timm-Giel, A. e Das, S. (2007). MobiSteer: Using steerable beam directional antenna for vehicular network access. Em *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, páginas 192–205.

[Oliveira et al. 2007] Oliveira, C. T., Moreira, M. D. D., Rubinstein, M. G., Costa, L. H. M. K. e Duarte, O. C. M. B. (2007). Redes tolerantes a atrasos e desconexões. Em *Minicursos do Simpósio Brasileiro de Redes de Computadores (SBRC)*, capítulo 5, páginas 203–256. Sociedade Brasileira de Computação.

[Ott e Kutscher 2004] Ott, J. e Kutscher, D. (2004). Drive-thru internet: IEEE 802.11b for “automobile” users. Em *IEEE Conference on Computer Communications (INFOCOM)*.

[Panayappan et al. 2007] Panayappan, R., Trivedi, J., Studer, A. e Perrig, A. (2007). VANET-based approach for parking space availability. Em *ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, páginas 75–76.

[Panichpapiboon e Pattara-atikom 2008] Panichpapiboon, S. e Pattara-atikom, W. (2008). Connectivity requirements for self-organizing traffic information systems. *IEEE Transactions on Vehicular Technology*, 57(6):3333–3340.

[Papadimitratos et al. 2008] Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A. e Hubaux, J.-P. (2008). Secure

vehicular communication systems: design and architecture. *IEEE Wireless Communications Magazine*, 46(11):100–109.

[Parno e Perrig 2005] Parno, B. e Perrig, A. (2005). Challenges in securing vehicular networks. Em *Workshop on Hot Topics in Networks (HotNets)*.

[Pathak et al. 2008] Pathak, V., Yao, D. e Iftode, L. (2008). Securing location aware services over VANET using geographical secure path routing. Em *IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, páginas 346–353.

[Peng e Cheng 2007] Peng, J. e Cheng, L. (2007). A distributed MAC scheme for emergency message dissemination in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 56(6):3300–3308.

[Perkins et al. 2003] Perkins, C., Belding-Royer, E. e Das, S. (2003). Ad hoc on-demand distance vector (AODV) routing. RFC 3561. http://www.ietf.org/rfc/rfc3561.txt.

[Piórkowski et al. 2008] Piórkowski, M., Raya, M., Lugo, A. L., Papadimitratos, P., Grossglauser, M. e Hubaux, J.-P. (2008). TraNS: realistic joint traffic and network simulator for VANETs. *ACM SIGMOBILE Mobile Computing and Communications Review*, 12(1):31–33.

[Prinz et al. 2008] Prinz, V., Brocco, M. e Woerndl, W. (2008). Peer-to-peer algorithms for C2C communication systems. Em *International Conference on Advances in Mobile Computing and Multimedia - MoMM*, páginas 376–381.

[Ramsey 2009] Ramsey, M. (2009). Chrysler redefines “radio” and brings Internet to the car. http://www.hear2.com/2008/03/chrysler-redefi.html. Acessado em 18 de fevereiro de 2009.

[Raya e Hubaux 2005] Raya, M. e Hubaux, J.-P. (2005). The security of vehicular ad hoc networks. Em *ACM workshop on Security of ad hoc and sensor networks (SASN)*, páginas 11–21.

[Reichardt et al. 2002] Reichardt, D., Miglietta, M., Moretti, L., Morsink, P. e Schulz, W. (2002). CarTALK 2000: safe and comfortable driving based upon inter-vehicle-communication. Em *IEEE Intelligent Vehicles Symposium (IV)*, páginas 545–550.

[Rizvi et al. 2007] Rizvi, S., Olariu, S., Weigle, M. e Rizvi, M. (2007). A novel approach to reduce traffic chaos in emergency and evacuation scenarios. Em *IEEE Vehicular Technology Conference (VTC-Fall)*, páginas 1937–1941.

[Sampigethaya et al. 2007] Sampigethaya, K., Li, M., Huang, L. e Poovendran, R. (2007). AMOEBA: Robust location privacy scheme for VANET. *IEEE Journal on Selected Areas in Communications*, 25(8):1569–1589.

[Schulze et al. 2005] Schulze, M., Noecker, G. e Boehm, K. (2005). PReVENT: A european program to improve active safety. Em *International Conference on Intelligent Transportation Systems Telecommunications*.

[Seet et al. 2004] Seet, B.-C., Liu, G., Lee, B.-S., Foh, C.-H., Wong, K.-J. e Lee, K.-K. (2004). A-STAR: A mobile ad hoc routing strategy for metropolis vehicular communications. Em *NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications*, volume 3042/2004 de *Lecture Notes in Computer Science*, páginas 989–999. Springer Berlin / Heidelberg.

[Shankar e Yedla 2007] Shankar, S. e Yedla, A. (2007). MAC layer extensions for improved QoS in 802.11 based vehicular ad hoc networks. Em *IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, páginas 1–6.

[Shladover et al. 1991] Shladover, S., Desoer, C., Hedrick, J., Tomizuka, M., Walrand, J., Zhang, W.-B., McMahon, D., Peng, H., Sheikholeslam, S. e McKeown, N. (1991). Automated vehicle control developments in the PATH program. *IEEE Transactions on Vehicular Technology*, 40(1):114–130.

[S.N. Technologies 2004] S.N. Technologies (2004). Introduction to QualNet. Qualnet User's Manual.

[Subramanian et al. 2008] Subramanian, A. P., Navda, V., Deshpande, P. e Das, S. R. (2008). A measurement study of inter-vehicular communication using steerable beam directional antenna. Em *ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, páginas 7–16.

[Taleb et al. 2007] Taleb, T., Sakhaee, E., Jamalipour, A., Hashimoto, K., Kato, N. e Nemoto, Y. (2007). A stable routing protocol to support ITS services in VANET networks. *IEEE Transactions on Vehicular Technology*, 56(6):3337–3347.

[Tank e Linnartz 1997] Tank, T. e Linnartz, J. (1997). Vehicle-to-vehicle communications for AVCS platooning. *IEEE Transactions on Vehicular Technology*, 46(2):528–536.

[Thomson et al. 2007] Thomson, S., Narten, T. e Jinmei, T. (2007). IPv6 stateless address autoconfiguration. RFC 4862. http://www.ietf.org/rfc/rfc4862.txt.

[Tian et al. 2003] Tian, J., Han, L. e Rothermel, K. (2003). Spatially aware packet routing for mobile ad hoc inter-vehicle radio networks. Em *IEEE International Conference on Intelligent Transportation Systems (ITSC)*, volume 2, páginas 1546–1551.

[Tian et al. 2005] Tian, Y., Xu, K. e Ansari, N. (2005). TCP in wireless environments: problems and solutions. *IEEE Communications Magazine*, 43(3):S27–S32.

[Vivo et al. 2007] Vivo, G., Dalmasso, P. e Vernacchia, F. (2007). The european integrated project "SAFESPOT" – how ADAS applications co-operate for the driving safety. Em *IEEE International Conference on Intelligent Transportation Systems (ITSC)*, páginas 624–629.

[VSCC 2005] VSCC (2005). Vehicle safety communications project task 3 final report: Identify intelligent vehicle safety applications enabled by DSRC. Relatório Técnico DOT HS 809 859, National Highway Traffic Safety Administration.

[Wang e Lin 2008] Wang, S. e Lin, C. (2008). NCTUns 5.0: A network simulator for IEEE 802.11 (p) and 1609 wireless vehicular network researches. Em *IEEE Vehicular Technology Conference (VTC-Fall)*, páginas 1–2.

[Weniger 2005] Weniger, K. (2005). PACMAN: passive autoconfiguration for mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 23(3):507–519.

[Wischhof et al. 2005] Wischhof, L., Ebner, A. e Rohling, H. (2005). Information dissemination in self-organizing intervehicle networks. *IEEE Transactions on Intelligent Transportation Systems*, 6(1):90–101.

[Wischhof et al. 2003] Wischhof, L., Ebner, A., Rohling, H., Lott, M. e Halfmann, R. (2003). SOTIS: A self-organizing traffic information system. Em *IEEE Vehicular Technology Conference (VTC-Spring)*, volume 4, páginas 2442–2446.

[Wisitpongphan et al. 2007] Wisitpongphan, N., Bai, F., Mudalige, P., Sadekar, V. e Tonguz, O. (2007). Routing in sparse vehicular ad hoc wireless networks. *IEEE Journal on Selected Areas in Communications*, 25(8):1538–1556.

[Xie et al. 1993] Xie, M., Trassoudaine, L., Alizon, J., Thonnat, M., Gallice, J. e Sophia-Antipolis, I. (1993). Active and intelligent sensing of road obstacles: Application to the european eureka-PROMETHEUS project. Em *International Conference on Computer Vision (ICCV)*, páginas 616–623.

[Xu et al. 2004] Xu, Q., Mak, T., Ko, J. e Sengupta, R. (2004). Vehicle-to-vehicle safety messaging in DSRC. Em *ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, páginas 19–28.

[Yousefi et al. 2008] Yousefi, S., Altman, E., El-Azouzi, R. e Fathy, M. (2008). Analytical model for connectivity in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 57(6):3341–3356.

[Zang et al. 2007] Zang, Y., Stibor, L., Walke, B., Reumerman, H.-J. e Barroso, A. (2007). A novel MAC protocol for throughput sensitive applications in vehicular environments. Em *IEEE Vehicular Technology Conference (VTC-Spring)*, páginas 2580–2584.

[Zhang et al. 2008] Zhang, C., Lin, X., Lu, R., Ho, P.-H. e Shen, X. (2008). An efficient message authentication scheme for vehicular communications. *IEEE Transactions on Vehicular Technology*, 57(6):3357–3368.

[Zhang et al. 2006] Zhang, X., Su, H. e Chen, H.-H. (2006). Cluster-based multi-channel communications protocols in vehicle ad hoc networks. *IEEE Wireless Communications Magazine*, 13(5):44–51.

[Zhao e Cao 2008] Zhao, J. e Cao, G. (2008). VADD: Vehicle-assisted data delivery in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 57(3):1910–1922.