UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE AUTOMAÇÃO E SISTEMAS

Renê R. Oliveira

PROTOCOLO ADAPTATIVO DE DISSEMINAÇÃO DE DADOS PARA APLICAÇÕES DE SEGURANÇA NO TRÂNSITO EM RODOVIAS.

Florianópolis(SC)

2013

Renê R. Oliveira

PROTOCOLO ADAPTATIVO DE DISSEMINAÇÃO DE DADOS PARA APLICAÇÕES DE SEGURANÇA NO TRÂNSITO EM RODOVIAS.

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

Florianópolis(SC)

2013

Aos meus pais e Saskya Bodenmüller

AGRADECIMENTOS

Primeiramente agradeço a minha mãe, Seule Figueredo da Rosa Oliveira, por ser forte, por lutar, por me apoiar em todos os momentos da minha vida e por ter sido muitas vezes meu porto seguro. Agradeço ao meu pai, Paulo da Silva Oliveira, por ter sido um grande pai, por ter me ensinado valores que levarei para o resto de minha vida. Além de ter trabalhado e lutado juntamente com minha mãe para que eu tivesse oportunidade de me instruir.

Agradeço a Saskya, por estar sempre ao meu lado, por sempre me incentivar, me valorizar e se preocupar comigo.

Agradeço ao meu orientador Carlos Barros Montez e minha coorientadora Michelle Silva Wangham por terem acreditado neste trabalho e por me ajudarem durante todo o desenvolvimento. Por fim, agradeço a todos os meus amigos e pessoas que de alguma maneira contribuíram para que este trabalho fosse concluído.

Desistir é algo que Lauda não faz.

Andreas Nikolaus Lauda

RESUMO

As *VANETs (Vehicular Ad hoc Networks)* são formadas por sistemas de comunicação entre veículos que fazem parte de um ambiente de trânsito e têm seus nós compostos por veículos e por equipamentos fixos que estão presentes ao longo das vias. Estas redes objetivam proporcionar conforto e segurança aos passageiros, por meio de informações sobre acidentes na pista, condição da estrada e aplicações de entretenimento. A disponibilidade e o tempo em que as mensagens trafegam nesta rede são essenciais para tais aplicações. Por isso, as VANETs requerem métodos eficientes e confiáveis para a comunicação de dados. Para prover confiabilidade à difusão de dados em redes veiculares deve-se transpassar alguns problemas como, por exemplo, *broadcast storm*, nós ocultos, alta colisões de pacotes, redundância de informação, entre outros. Muitos destes problemas persistem em estudos realizados anteriormente. Este trabalho tem por objetivo prover confiabilidade na disseminação de mensagens em aplicações voltadas a segurança no trânsito por meio de um protocolo adaptativo e eficiente. O protocolo proposto é adaptativo pois adapta o período entre transmissões de mensagens de controle de acordo com a densidade da rodovia, a fim de diminuir o número de mensagens geradas na rede. Também visa ser eficiente pois diminui a quantidade de colisões frente a quantidade de pacotes gerados na rede, oferece menor atraso no envio das mensagens e diminui a quantidade de retransmissões em cenários com mais de um alerta na rede. O trabalho envolveu (I) a definição do protocolo proposto, a integração e o uso deste pela aplicação, (II) a implementação de uma aplicação para rodovias com simuladores de redes e de tráfego bidirecionalmente acoplados, (III) avaliação da confiabilidade do protocolo proposto e dos impactos decorrentes do uso do protocolo na aplicação de disseminação de alertas por meio de simulações realizadas em diferentes cenários de densidade de veículos, e (IV) as análises dos resultados experimentais obtidos. Os resultados dos experimentos comprovam que o protocolo proposto, para os cenários simulados é 100 % confiável e que os impactos decorrentes do seu uso não prejudicam as funcionalidades da aplicação, comprovando a eficiência do protocolo.

Palavras-chave: Redes veiculares. Protocolo confiável. Comunicação móvel. Segurança Rodoviária.

ABSTRACT

The VANETs (Vehicular Ad hoc Networks) are formed by communication systems among vehicles which are part of the same traffic environment. Their nodes are composed of vehicles and fixed equipment present along the traffic ways. The aim of these networks is to provide comfort and safety to passengers through information about accidents on the road, road conditions and entertainment applications. The availability and the time span in which these messages move through the network are essential for these applications. Consequently, the VANETs require efficient and reliable methods for data communication. To ensure that data transmission in vehicular networks is reliable certain problems must be overcome, such as broadcast storm, hidden nodes, high collision of packages, information redundancy, among others. Many of these problems persist in previous studies. Thus, this work aims at providing, through an adaptive and efficient protocol, reliability to message transmission in applications targeted at traffic safety. The proposed protocol is adaptive as it adapts the time span between the transmissions of messages according to the road density, in order to decrease the number of messages generated in the network. It also aims at efficiency as it decreases the amount of collisions due to the number of packages generated in the network, presents less delay in message transmission and decreases the amount of retransmissions in scenarios with more than one alert in the network. This research involved (I) the definition of the proposed protocol, its integration and use by the application, (II) the implementation of an application for motorways with network and traffic simulators directionally attached, (III) evaluation of the reliability of the proposed protocol and of the impacts resulting from the use of the protocol in the application of spread of alerts through simulations carried out in diverse scenarios of vehicle density, (IV) the analyses of the experimental results. These results prove that the proposed protocol is 100 % reliable for simulated scenarios and that the impacts produced by its use do not harm the functionalities of the application, proving the efficiency of the protocol.

Keywords: Vehicular networks. Reliable protocol. Mobile communication. Road safety.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

LIST OF ALGORITHMS

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO

De acordo com uma pesquisa feita pelo IPEA (Instituto de Pesquisa Econômica Aplicada) sobre os acidentes de trânsito, somente nas rodovias brasileiras, os custos para os cofres públicos foram de 30 bilhões de reais entre o período de janeiro de 2011 a julho de 2012. O levantamento considerou desde os danos materiais até os gastos com atendimento e os prejuízos por interrupção do trabalho (IPEA, 2012). A pesquisa encomendada pelo Departamento Nacional de Trânsito (DENATRAN), constatou que as rodovias nacionais contabilizam, em média, trezentos acidentes por dia, o que corresponde a um acidente a cada quatro minutos e meio. Entre estes, acontece um atropelamento a cada duas horas, resultando na morte de mais de um mil pedestres por ano. O número de mortes no grupo dos motociclistas é próximo de um mil a cada ano (IPEA, 2008).

O automóvel, exige que o ser humano esteja qualificado técnica e mentalmente para operá-lo de forma segura. Para que responda de forma adequada a determinado estímulo, é necessário que este esteja alerta, caso contrário, o condutor poderá se colocar em uma situação de perigo. Este estado de alerta é afetado por muitos fatores, fazendo com que as pessoas respondam com maior ou menor rapidez em situações de emergências (EVANS, 1991).

Diante deste contexto, no sentido de desenvolver sistemas automatizados que auxiliem o ser humano na prevenção e solução de problemas de trânsito, as redes *ad hoc* móveis (*Mobile Ad Hoc Networks* - MANETs) têm sido foco de muitos estudos. A necessidade de se comunicar a qualquer hora e lugar, além da necessidade de conectar dispositivos, tais como notebooks, smartphones, etc, contribuíram para que essa tecnologia se proliferasse em diversas áreas de aplicação. Com a consolidação desta tecnologia, as redes *ad hoc* veiculares (*Vehicular Ad Hoc Networks* - VANETs) surgiram (BERNSEN; MANIVANNAN, 2009). Estas redes são um dos tipos de redes MANETs mais estudados, devido aos seus desafios e as suas inúmeras aplicações, como por exemplo, a troca de mensagens informando condições de tráfego ou outras situações de risco existentes na via (BECHLER et al., 2003).

Segundo Bernsen e Manivannan (2009), a grande diferença entre MANETs e VANETs está relacionada ao padrão de mobilidade dos nós que compõem estas redes. Nas MANETs, os nós permanecem está-

veis durante um período relativamente longo, enquanto nas VANETs, a velocidade que os nós movimentam-se é elevada e as ligações entre estes permanecem ativas por um curto período de tempo. Devido a estas características, não é possível assegurar a transferência contínua de mensagens, sendo este um dos problemas mais críticos deste ambiente com um forte impacto nas aplicações de segurança de tráfego (BERNSEN; MANIVANNAN, 2009).

As VANETs podem ser compostas somente por veículos ou também por estações fixas ao logo da via, sendo necessário que cada nó da rede esteja equipado com algum dispositivo sem fio capaz de comunicar-se com os outros dispositivos presentes na rede, assim, todos os nós pertencentes a rede veicular têm um papel colaborativo. Esta postura é fundamental no que diz respeito ao funcionamento da rede (KOSCH, 2004). Segundo Taha e Hasan (2007), a utilização de tecnologias de sistemas de comunicação em veículos permitem altos níveis de interação, possibilitando a comunicação entre usuários móveis. Há esforços contínuos em desenvolver e melhorar estas tecnologias com o intuito de torná-los mais inteligentes e, especialmente, mais seguros (TAHA; HASAN, 2007).

Diante do contexto apresentado em Biswas, Tatchikou e Dion (2006) e Panayappan et al. (2007), é possível afirmar que as redes veiculares têm a capacidade de solucionar problemas de segurança no trânsito como os que ocorrem de forma recorrente em rodovias e satisfazer de forma adequada os anseios dos condutores.

Neste contexto, um problema descrito em trabalhos sobre aplicações voltadas a segurança no trânsito que utilizam redes veiculares (BERNSEN; MANIVANNAN, 2009) e (NAUMOV; GROSS, 2007) é a falta de garantias da entrega de mensagens de uma única fonte para cada nó em sua faixa de transmissão com maior confiabilidade possível e com atraso mínima. Segundo Nakorn e Rojviboonchai (2010), alguns protocolos confiáveis oferecem um serviço de entrega de mensagens garantida, por meio de implementações de mecanismos de controle para que seu comportamento possa dinamicamente adaptar-se às condições observadas na rede.

Para prover confiabilidade a entrega de mensagens de dados na rede, deve-se mitigar problemas encontrados em abordagens que buscaram gerar confiabilidade, como por exemplo, nó oculto, *broadcast storm*, alta latência e adaptabilidade diante de inúmeros cenários com densidade de veículos variada, a fim de proporcionar uma melhora no desempenho para as aplicações que têm como requisito crítico a entrega das mensagens em um cenário veicular.

Dentro deste contexto, este trabalho procura trazer uma contribuição para a área de disseminação confiável de dados em redes veiculares.

1.2 PROBLEMA DE PESQUISA

Trabalhos como Xu et al. (2004) e Alshaer e Horlait (2005) passaram a tratar o tempo e a confiabilidade como requisitos críticos para aplicações de segurança no trânsito, pois para os autores a entrega de mensagens aos nós da rede pode evitar acidentes.

Alshaer e Horlait (2005) expõem que o maior desafio encontrado em estudos voltados à disseminação de informações em redes é prover confiabilidade ao entregar mensagens de uma única fonte para cada nó em sua faixa de transmissão com maior confiabilidade possível. Segundo Koubek, Rea e Pesch (2010), caracteriza-se uma difusão como confiável quando a mensagem difundida ou é recebida por todos os membros do grupo ou não é recebida por nenhum deles. Neste contexto, mostra-se necessário mitigar problemas que dificultam a confiabilidade na entrega de mensagens, problemas estes que são citados por Bernsen e Manivannan (2009) e Naumov e Gross (2007). Segundo Xu et al. (2004), existem mecanismos que podem prover um melhor desempenho à difusão de alertas em redes veiculares, tais como, reenvio de mensagens e reconhecimento seletivo.

Alguns trabalhos como (NEKOVEE; BOGASON, 2007), (CHUAN; JIAN, 2012) e (KAMOLTHAM; NAKORN; ROJVIBOONCHAI, 2011), buscaram prover confiabilidade à difusão de dados em redes veiculares e encontraram problemas como, *broadcast storm*, nós ocultos e colisões de pacotes. O *broadcast storm* dificulta a obtenção da confiabilidade na entrega de mensagens. Este problema gera uma condição de sobrecarga na rede ocasionada por um *broadcast* de um pacote incorreto, fazendo que vários nós respondam aos demais, replicando o pacote incorreto, o que faz o problema crescer exponencialmente, tornando-o crítico (NEKOVEE; BOGASON, 2007).

Kamoltham, Nakorn e Rojviboonchai (2011) encontraram dificuldades em mitigar o problema do nó oculto, este problema ocorre quando pelo menos um dos nós da rede é incapaz de detectar a presença de um ou mais nós conectadas a mesma rede. O nó acaba por não receber as mensagens difundidas na rede devido a algum obstáculo ou grande distância entre os nós. Isso causa problemas no acesso compartilhado ao meio causando colisões de pacotes. Estas colisões podem

resultar na degradação da rede.

Embora existam vários trabalhos sobre entrega confiável por meio de difusão, alguns destes não tratam os problemas descritos anteriormente e não se adaptam de acordo com a densidade do cenário. Logo, devem ser desenvolvidas soluções que busquem prover confiabilidade na entrega de mensagens sem impactar no desempenho das aplicações voltadas a segurança no trânsito.

Neste contexto, este trabalho busca tratar problemas que dificultam a tarefa de prover confiabilidade em transmissões de dados em redes veiculares. Em especial, busca-se responder os seguintes questionamentos:

1. É possível prover maior eficiência e eficácia na entrega dos dados por meio da concepção de um protocolo de difusão confiável e adaptativo para redes veiculares?

2. Qual o impacto do uso do protocolo em aplicações voltadas a segurança no trânsito em rodovias?

3. Qual a taxa de entrega com sucesso (confiabilidade) é obtida com o uso do protocolo proposto?

1.2.1 Solução Proposta

A solução proposta consiste, com base nos mecanismos descritos na literatura, conceber um protocolo adaptativo e eficiente que ofereça confiabilidade na entrega de mensagens em redes veiculares.

Para prover confiabilidade à transmissão de mensagens de dados, o protocolo proposto define que o nó transmissor deve armazenar informações sobre seus nós vizinhos a um salto de distância. Por meio de listas, o nó transmissor seleciona um único nó para fazer o reenvio da mensagem e por utilizar este mecanismos o protocolo diminui a quantidade de mensagens reenviadas na rede. A seleção do nó de reenvio é feita de acordo com o ganho calculado de cada vizinho. O nó que possuir maior ganho será o escolhido.

As informações que são armazenadas pela lista de vizinhos são obtidas por meio de trocas de pacotes aperiódicos denominados *beacons*, mensagens de controle consideravelmente menores que as mensagens (alertas) disseminadas na rede. Neste trabalho, são utilizados três tipos de mensagens de controle, que são: (1) requisitar informações da vizinhança, (2) transportar informações dos nós e (3) revogar um alerta na rede. A troca de informações é feita de forma aperiódica e

adaptativa, visando diminuir o tráfego de mensagens de controle em cenários com alta densidade de veículos, tais como, congestionamentos. O protocolo adaptativo analisa o cenário e determina o intervalo entre os envios dos *beacons*, desta forma, em cenários que não ocorrem mudança da vizinhança, a troca de informações entre os nós é feita com menos frequência, o que diminui o tráfego na rede.

Para mitigar o problema de nó oculto, a proposta utiliza dois tipos de nós, nós móveis (veículos) e os nós fixos. Estes nós fixos têm o papel de armazenar as mensagens disseminadas na rede, criando assim uma lista de mensagens. Desta maneira, quando um veículo que não recebeu determinada mensagem passar por um destes pontos fixos, poderá informar qual foi sua última mensagem recebida, caso esta mensagem não seja a última mensagem vigente na rede, o nó fixo a envia ao veículo. Este processo também ocorre com os nós móveis que possuem alguma mensagem que seu vizinho não tem. Desta forma, veículos não atendidos pela disseminação do transmissor ou dos nós de reenvio podem ser atendidos.

O protocolo desenvolvido também tem a preocupação de impedir reenvios desnecessários. Ao receber uma mensagem, o nó selecionado verifica se já recebeu ou não a mensagem, caso tenha recebido, a mensagem é descartada. Em situações, nas quais existem mais de uma mensagem de dados que representa um alerta, o protocolo pode fazer uso da codificação de rede, que realiza uma operação lógica XOR entre as mensagens existentes, com o objetivo diminuir a quantidade de retransmissões realizadas.

A eficiência do protocolo proposto é mensurada por meio da taxa de colisões frente a quantidade de pacotes geradas, do atraso no envio das mensagens, quantidade de pacotes geradas nos cenários e a quantidade de retransmissões necessárias para disseminar uma mensagem na rede.

De forma a avaliar a eficiência e os possíveis impactos do uso do protocolo na disseminação de mensagens de dados realizada por uma aplicação voltada a segurança no trânsito rodoviário, foram realizados experimentos com simuladores de rede e de tráfego bidirecionalmente acoplados. O uso de simulação mostrou-se atraente por permitir o controle sobre o ambiente e por consumir menos recursos. Por meio dos experimentos, foram definidas as seguintes métricas: a confiabilidade referente à taxa de sucesso na entrega dos alertas, o atraso na entrega dos dados, a quantidade de pacotes gerados e o número de colisões de pacotes. Desta forma foi possível definir o impacto do uso deste protocolo na aplicação.

Como hipótese, têm-se as seguintes afirmações:

1. O protocolo prove confiabilidade na entrega das mensagens, mas aumenta o tempo de processamento das mensagens e por fim, aumenta o atraso na entrega das mensagens;
2. O protocolo proposto aumenta a quantidade de mensagens e com isso aumenta a quantidade de colisões de pacotes.

1.2.2 Delimitação do Escopo

Neste trabalho, foi definido um protocolo e uma aplicação para prover confiabilidade na entrega de mensagens de aplicações veiculares voltadas a segurança em rodovias. Esta aplicação, voltada para segurança, visa divulgar informações sobre acidentes, ocorrências no trânsito e condições adversas nas rodovias. Tanto a aplicação, quanto o protocolo foram implementados em simuladores de rede e de tráfego, visto que o desenvolvimento de um protótipo real possui um custo muito elevado.

1.2.3 Justificativa

Segundo Heron et al. (2008), a principal causa de acidentes em rodovias é a falha humana. Com a incorporação de avanços tecnológicos no âmbito automotivo, torna-se possível alertar os condutores que trafegam nas rodovias, sobre situações adversas, como acidentes, pedágios, congestionamentos, entre outros, por meio de uma aplicação distribuída que utiliza as redes interveiculares como sistema de comunicação.

Alshaer e Horlait (2005) afirmam que o desenvolvimento de aplicações voltadas a segurança no trânsito em rodovias tem grandes desafios, tais como, garantir a confiabilidade na entrega de mensagens de dados. Esta confiabilidade surge por meio de implementações de mecanismos e protocolos voltados ao gerenciamento das informações provenientes do cenário veicular e que procuram garantir a entrega de mensagens a todos os nós da rede. Diante deste fato citado por Alshaer e Horlait (2005), faz-se necessário o desenvolvimento de um protocolo confiável para disseminação de informação em redes veiculares, protocolo este, que deve procurar preencher as lacunas deixadas por outras propostas anteriores, como por exemplo, (NEKOVEE; BOGASON, 2007), (NAKORN; ROJVIBOONCHAI, 2010), (KAMOLTHAM; NAKORN; ROJVIBOONCHAI, 2011) e (CHUAN; JIAN, 2012).

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Prover confiabilidade na disseminação de mensagens em aplicações voltadas a segurança no trânsito por meio de um protocolo adaptativo e eficiente.

1.3.2 Objetivos Específicos

De forma a alcançar o objetivo geral definido, os seguintes objetivos específicos foram definidos:

- Analisar mecanismos e outros protocolos existentes que provêm confiabilidade a disseminação de dados;
- Conceber um protocolo adaptativo para redes veiculares que prove confiabilidade na entrega de mensagens;
- Analisar a confiabilidade do protocolo desenvolvido perante outras abordagens; e
- Analisar o impacto do protocolo no desempenho da aplicação.

1.4 METODOLOGIA

Nesta seção, apresenta-se uma classificação da metodologia utilizada nesta pesquisa, bem como os procedimentos metodológicos.

1.4.1 Metodologia da Pesquisa

Neste trabalho, é utilizado o método hipotético-dedutivo, já que o trabalho parte de um problema e segue para a obtenção da sua solução por meio da verificação de hipóteses (LAKATOS; MARCONI, 2000). Segundo Gil (2002), a pesquisa é de natureza aplicada, pois tem como objetivo investigar, comprovar ou rejeitar as hipóteses apresentadas na solução proposta. Com relação ao ponto de vista da forma de abordagem do problema, este trabalho enquadra-se como uma pesquisa quantitativa e qualitativa (LAKATOS; MARCONI, 2000). Quantitativa pelo

fato de que os resultados obtidos por meio dos experimentos foram classificados e analisados por técnicas estatísticas. Já a classificação qualitativa se deve ao fato de que será feita uma análise descritiva sobre garantia da propriedade de disponibilidade implementada.

No ponto de vista de seus objetivos, esse trabalho se enquadra em uma pesquisa exploratória (LAKATOS; MARCONI, 2000), pois visa investigar mecanismos que podem prover confiabilidade ao protocolo desenvolvido por meio de levantamentos bibliográficos e de trabalhos correlacionados.

1.4.2 Procedimentos Metodológicos

Para o cumprimento dos objetivos específicos, referentes à dissertação, foram utilizados os seguintes métodos de pesquisa:

1. **revisão bibliográfica:** o estudo teve por objetivo prover conhecimento e suporte teórico para o desenvolvimento da solução proposta. Também foi realizado um levantamento bibliográfico sobre as redes veiculares, aplicações que utilizam estas redes e conceitos que auxiliaram para o desenvolvimento da aplicação e do protocolo, os quais forneceram mecanismos para o aumento da confiabilidade na disseminação de informações na rede. Neste estudo, foram utilizados materiais bibliográficos publicados em livros, artigos acadêmicos, artigos publicados em periódicos e materiais disponibilizados na internet;

2. **análise de trabalhos relacionados:** foi realizada uma análise dos trabalhos correlatos encontrados na literatura, referenciados por diversos autores, que empregam métodos para melhoria e aumento da confiabilidade na difusão de mensagens em redes veiculares. Estes trabalhos serviram de base para a construção do protocolo proposto e da sua integração a uma aplicação embarcada nos veículos. Esses trabalhos foram selecionados e analisados por meios de critérios definidos na revisão sistemática, cujo protocolo de busca é apresentado no Apêndice A.

3. **definição do protocolo proposto:** após o levantamento bibliográfico e análise de trabalhos correlatos, foi definida a estrutura do protocolo e os mecanismos implementados para prover confiabilidade à transmissão de informações na rede.

4. **implementação da aplicação e do protocolo propostos:**

com base na modelagem realizada, a aplicação e protocolo foram implementados em um simulador de rede bidirecionalmente acoplado;

5. **realização de simulações e testes:** testes funcionais da aplicação foram realizados em um ambiente de simulação. Estes testes foram baseados em planos de teste que foram definidos visando verificar o atendimento aos requisitos, aferir alguns parâmetros para a configuração da rede e da aplicação; e

6. **avaliação do protocolo:** visando avaliar o protocolo desenvolvido neste trabalho foram realizadas simulações de cenários (rodovia fictícia) com densidades diferentes de veículos. Foram analisadas as seguintes métricas: a confiabilidade referente à taxa de sucesso da entrega dos alertas, o atraso máximo na entrega dos alertas, à quantidade de colisões de pacotes e a quantidade de pacotes gerados na rede.

1.5 ESTRUTURA DA DISSERTAÇÃO

Este documento está estruturado em seis capítulos. O Capítulo 1, Introdução, apresentou uma visão geral do trabalho, destacando a motivação, a problematização do trabalho, a solução proposta, os objetivos a serem alcançados ao longo do trabalho e os métodos de pesquisa empregados no desenvolvimento do trabalho.

No Capítulo 2 é apresentada uma revisão bibliográfica sobre redes *ad hoc* veiculares, suas características, vantagens e desvantagens, padrões de comunicação e comunicação em VANETs. Também são apresentadas algumas aplicações para redes *ad hoc* veiculares, aspectos que envolvem a simulação de redes veiculares e simuladores de redes móveis discutidos na literatura. Por fim, são apresentados os conceitos de transporte de informação, aspectos referentes a disseminação de dados em redes veiculares, categorias de protocolos e suas características, além do conceito de codificação de redes.

Já no Capítulo 3 são analisados os principais trabalhos relacionados, explicitando suas características, vantagens e desavantagens, além de suas formas de funcionamento.

O Capítulo 4, apresenta o detalhamento do protocolo, que inclui a modelagem, tecnologias escolhidas para o desenvolvimento da aplicação e simulações realizadas utilizando o protocolo em dez cenários de uso.

No Capítulo 5 são apresentados os resultados obtidos nas simulações e suas análises. Por fim, no Capítulo 6, é apresentada a conclusão, destacando as contribuições deste trabalho, as dificuldades encontradas e as sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, são apresentados os conceitos de redes veiculares, as arquiteturas existentes em redes veiculares, suas características, bem como os protocolos utilizados para disseminação de dados em redes veiculares. Também são apresentados os padrões de comunicação sem fio utilizados em redes móveis. Ainda neste capítulo, são apresentadas algumas aplicações descritas na literatura para redes veiculares voltadas a segurança no trânsito, aspectos de simulação de redes móveis e modelos de mobilidade. Por fim, são apresentados os conceitos de disseminação de dados e codificação de redes.

2.1 REDES VEICULARES

Segundo Zhao e Cao (2008), as redes veiculares estão cada vez mais presentes nas rodovias e aplicações que a utilizam estão se tornando um meio importante para prover mais segurança nas estradas. Estas aplicações caracterizam um Sistema Inteligente de Transporte (*Intelligent Transportation System* - ITS). Exemplos destas aplicações incluem a monitoração cooperativa do tráfego ou prevenção de colisões (LI; WANG, 2007).

As redes veiculares têm seus nós compostos por veículos e por equipamentos fixos que estão presentes ao longo das vias. Todos estes nós possuem interface de comunicação sem fio e apresentam alta mobilidade e trajetórias que acompanham as extensões das vias de trânsito (KOSCH, 2004).

Estas redes, incorporadas a um ambiente formado por veículos e todos os componentes que formam vias de trânsito, possuem muitos desafios para que possam ser utilizadas em larga escala (BECHLER et al., 2003). Entre estes, destacam-se: a alta mobilidade dos nós, o dinamismo dos cenários, a escalabilidade com relação ao número de nós e o tempo reduzido em que dois nós permanecem conectados (ZHAO; CAO, 2008). Protocolos utilizados em redes *ad hoc* móveis (*Mobile ad hoc Network* - MANETs) não são adequados para suprir estes desafios, mesmo assim as MANETs e as redes *ad hoc* veiculares possuem características comuns como o dinamismo da topologia da rede (ZHAO; CAO, 2008).

Segundo Sichitiu e Kihl (2008), mesmo tendo características em comum, VANETs e MANETs têm uma diferença importante que é a

restrição quanto ao consumo de energia. Nas MANETs, a frequência e o volume dos dados são um fator relevante para o consumo de energia, já nas VANETs as baterias dos veículos estão sendo carregadas frequentemente (SICHITIU; KIHL, 2008).

De acordo com Raya e Hubaux (2005) as principais características das VANETs são:

- **Banda disponível:** as tecnologias sem fio disponíveis atualmente possuem capacidades de transmissão significativamente menores do que aquelas disponíveis em redes cabeadas;
- **Conectividade variável no tempo:** a conectividade da rede é dependente de fatores como sua densidade em determinado ponto, a velocidade de deslocamento dos nós, o sentido desse deslocamento e o raio de alcance dos dispositivos instalados nestes veículos;
- **Cooperação:** a funcionalidade da rede recai totalmente sobre a cooperação dos veículos que a compõe. Sem a participação destes, as informações geradas não se tornam de conhecimento geral;
- **Escala:** com milhares de veículos distribuídos por todos os lugares, as VANETs poderão se tornar o tipo de rede *ad hoc* com o maior número de nós existente;
- **Mobilidade organizada:** diferentemente das MANETs tradicionais, os nós de uma VANET não se movimentam de maneira aleatória, mas sim dentro de vias de tráfego existentes e sob a regência de leis de circulação;
- **Topologia dinâmica:** a alta mobilidade dos nós faz com que a topologia das VANETs mude rápida e frequentemente;
- **Recursos energéticos e computacionais:** ao contrário das MANETs tradicionais, as VANETs possuem recursos suficientes para as aplicações desenvolvidas; e
- **Segurança:** com o acesso compartilhado ao meio, essas redes são muito mais suscetíveis a ataques do que as redes cabeadas convencionais.

Conforme descrevem Lin et al. (2007), as redes veiculares são divididas em redes interveiculares e intraveiculares. As intraveiculares são redes que estão localizadas dentro dos veículos. Estas redes devem permitir que as informações sejam compartilhadas entre diferentes

ECUs (*Electronic Control Unit* - Unidade Eletrônica de Controle). Para tanto, independente da tecnologia de rede adotada, esta deve interagir com a rede pré-existente. Desta forma, a comunicação deve atender ou não a requisitos específicos, decidindo-se, por exemplo, por adotar comunicação sem fio em sensores do sistema de freios ABS (*Anti-lock Braking System*). Neste caso, esta rede sem fio deve atender a requisitos que envolvem altas taxas de amostragem e alta confiabilidade, diferentemente de utilizar a comunicação sem fio para controle de lâmpadas ou vidros elétricos (LIN et al., 2007).

Já as redes interveiculares são redes formadas por veículos que se comunicam com outros veículos ou com a infraestrutura que está presente ao longo das vias. Segundo Papadimitratos et al. (2008), estas redes podem possuir as seguintes características: todos os nós são provedores, encaminhadores e consumidores de dados; os dados difundidos são oriundos de vários sensores e câmeras em cada nó; a rede é aberta e de topologia altamente dinâmica e há uma alteração constante na vizinhança dos nós.

A arquitetura das redes veiculares define a maneira como os nós se organizam e se comunicam, podendo ser classificada em três principais tipos: *ad hoc* puro, infraestruturado ou híbrido (LI; WANG, 2007).

- **Modo *ad hoc* Puro (*Vehicle-to-Vehicle* - V2V):** automóveis funcionam como roteadores, encaminhando o tráfego através de múltiplos saltos. A comunicação é realizada sem a presença de um elemento centralizador;

- **Modo Infraestruturado (*Vehicle-to-Infrastructure* - V2I):** utiliza nós estáticos distribuídos ao longo da via, que funcionam como pontos de acesso. Estes dispositivos podem atuar tanto na geração de novas informações quanto no roteamento de dados gerados por terceiros. Estes nós centralizam todo o tráfego da rede, servindo como nós intermediários das comunicações; e

- **Arquitetura Híbrida:** é utilizada uma infraestrutura mínima para aumentar a conectividade e prover alguns serviços de rede, como interconexão por exemplo. Neste modo, há também a possibilidade dos veículos se comunicarem por múltiplos saltos.

As redes veiculares trazem inúmeras aplicações e estas aplicações são divididas em duas categorias de acordo com Jakubiak e Koucheryavy (2008); conforto e segurança. Aplicações voltadas ao conforto procuram melhorar o conforto dos passageiros e a eficiência do tráfego. Neste aspecto podem ser incluídos os pontos de interesse (POI - *Points*

Of Interest), assim os nós podem receber dados de veículos comerciais e da infraestrutura rodoviária sobre seus negócios. Empresas (shoppings, restaurantes, postos de combustível e hotéis) podem configurar *gateways* estacionárias para transmitir dados de *marketing* para clientes em potencial que passam pela via. A característica importante de aplicações de conforto/comercial é a de que essas não devem interferir nas aplicações de segurança. Neste contexto a priorização de tráfego e uso de diferentes canais físicos é uma solução viável.

Segundo Jakubiak e Koucheryavy (2008) as aplicações relacionadas à segurança podem ser agrupadas em três classes principais: **assistência** (navegação, prevenção cooperativa de colisões e mudança de faixa de rodagem), **informação** (limite de velocidade) e de **alerta** (pós acidente, obstáculos, ou avisos referentes as condições da via). Essas aplicações geralmente exigem comunicação direta devido ao seu caráter crítico. Nestas aplicações, os principais desafios são reduzir o tempo de divulgação de notificações de forma que o condutor possa reagir de acordo com o potencial obstáculo e garantir a integridade destas notificações. Esta dissertação visa, principalmente, prover um mecanismo confiável para aplicações de segurança no trânsito.

2.2 PADRÕES DE COMUNICAÇÃO SEM FIO UTILIZADOS EM REDES VEICULARES

Como existem vários padrões de comunicação sem fios disponíveis para implementar redes interveiculares, foi necessário estabelecer um critério inicial de pré-seleção para a escolha dos padrões que serão analisados em mais detalhes nesta seção. O critério adotado foi o número de citações e referências encontrado a partir de uma revisão da literatura que considerou vinte e oito trabalhos científicos relacionados a aplicações de redes veiculares (LUNDGREN; NORDSTRö; TSCHUDIN, 2002); (REICHARDT et al., 2002); (NADEEM et al., 2004); (OTT; KUTSCHER, 2004); (CONSORTIUM, 2005); (KOSCH, 2005); (BISWAS; TATCHIKOU; DION, 2006); (CALISKAN; GRAUPNER; MAUVE, 2006); (GASS; SCOTT; DIOT, 2006); (OSAFUNE; LIN; LENARDI, 2006); (PANAYAPPAN et al., 2007); (RIZVI et al., 2007); (OSTERMAIER; DOTZER; STRASSBERGER, 2007); (ZHANG; ZHANG; JIA, 2007); (TOULMINET; BOUSSUGE; LAURGEAU, 2008); (SARAVANAN; THANGAVELU; RAMESHBABU, 2009); (PAULA; OLIVEIRA; NOGUEIRA, 2010); (AUGUSTO C. H. P.; REZENDE, 2010); (CAMBRUZZI et al., 2010); (CARVALHO; REZENDE, 2010); (GOMES et al., 2010); (PASSOS; ALBUQUERQUE, 2010); (MITROPOULOS et

al., 2010); (ARNOULD et al., 2011); (ECKHOFF et al., 2011); (GEISSLER; SCHINDHELM; LUEDEKE, 2011); (KARGL; PAPADIMITRATOS, 2011); (PANDAZIS, 2012).

De acordo com o levantamento feito, apresentado na Tabela 1, verificou-se que os padrões de comunicação mais utilizados nos trabalhos analisados foram: o padrão 802.11p, sendo o mais utilizado, seguido pelo padrão 802.11g com sete utilizações, os padrões 802.11b e 802.11a ambos com seis utilizações e a solução VehiCular-MAC (VC-MAC) utilizada uma único trabalho.

Tabela 1: Relação entre padrões e número de utilização nos trabalhos

Padrão	Número de Utilização nos Trabalhos
802.11a	6
802.11b	6
802.11g	7
802.11p	8
VC-MAC	1

A partir dos resultados obtidos, foram pré-selecionados para análise e breve descrição os padrões de comunicações sem fios 802.11g e 802.11p. O protocolo VC-MAC é uma solução proposta por Zhang, Zhang e Jia (2007), desenvolvida para redes com arquitetura híbrida, é baseado na comunicação cooperativa e utiliza o conceito de reutilização espacial (ZHANG; ZHANG; JIA, 2007). Como o protocolo VC-MAC é uma solução proposta e não um padrão *de jure ou de fato*, este não foi analisado neste trabalho.

2.2.1 IEEE 802.11

O padrão 802.11g por operar na mesma frequência do padrão 802.11b, torna-se possível a adição de adaptadores de rede e pontos de acesso 802.11g a uma rede 802.11b já existente. A velocidade de transmissão é de 54 Mbps. Com a utilização deste padrão, é possível transmitir informações simultaneamente em dois canais diferentes, dobrando a taxa de transmissão e o nível de interferência com outras redes próximas (DOEFEXI et al., 2003).

Em 2004, com o objetivo de padronizar as comunicações em redes veiculares, foi definido um novo padrão, denominado 802.11p WAVE

(Wireless Access in the Vehicular Enviroment). Segundo Weil (2009), a arquitetura WAVE é dividida em seis documentos: IEEE P1609.1, IEEE P1609.2, IEEE P1609.3, IEEE P1609.4, IEEE 802.11 e IEEE 802.11p. Na Figura 1, pode ser observada a pilha de protocolos WAVE.

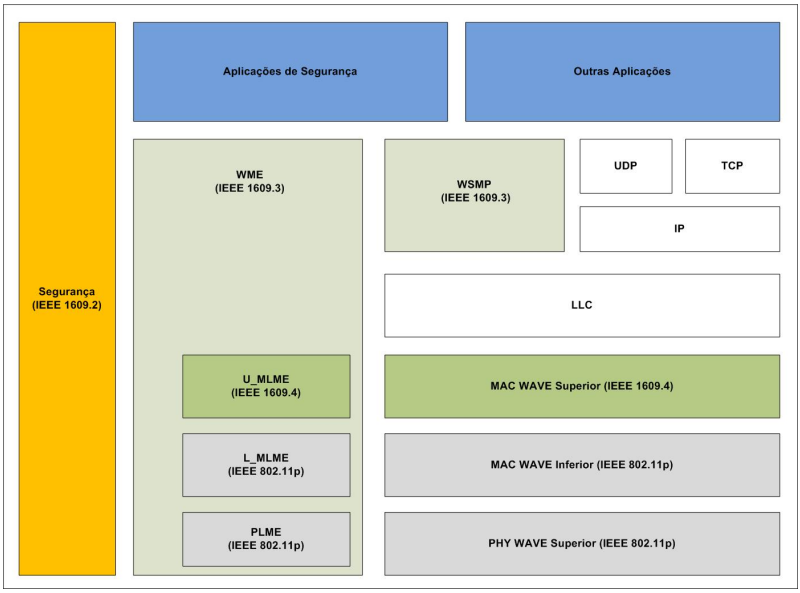

Figura 1: Pilha de protocolos WAVE.

- **IEEE P1609.1:** especifica serviços e interfaces da aplicação de gerenciamento de recursos. Seu objetivo principal é favorecer a interoperabilidade de aplicações WAVE, de forma a simplificar as Unidades de Bordo , reduzindo seu custo e aumentando o desempenho (WEIL, 2009). Essa comunicação permite o acesso a recursos como memória, interfaces de usuários e interfaces com outros dispositivos no veículo (WEIL, 2009);

- **IEEE P1609.2:** define formatos e processamento seguros de envio de mensagens, bem como as circunstâncias e momentos em que devem ser utilizadas estas mensagens. Determina a utilização de ferramentas de segurança tradicionais, como Infraestrutura de Chaves Públicas (PKI - *Public Key Infrastructure*). Define também a existência de autoridades de certificação, responsáveis por

autorizar outras entidades por meio da emissão de certificados. O padrão descreve uma aplicação denominada gerente de segurança, responsável por gerenciar o certificado raiz e armazenar as listas de certificados revogados (WEIL, 2009);

- **IEEE P1609.3:** especifica os serviços das camadas de controle de enlace lógico (LLC – *Logical Link Control*), rede e de transporte. A comunicação WAVE pode utilizar o IPv6 (Internet Protocol Version 6) ou mensagens curtas WAVE (WEIL, 2009);

- **IEEE P1609.4:** define modificações no padrão IEEE 802.11, para a operação em múltiplos canais (WEIL, 2009);

- **IEEE 802.11:** protocolo tradicional (WEIL, 2009); e

- **IEEE 802.11p:** extensão da família de protocolos IEEE 802.11, baseando-se principalmente na extensão "a" do IEEE 802.11 e operando na frequência de 5,9 GHz. Na arquitetura WAVE, o MAC é responsável pela definição das diferenças específicas do controle de acesso ao meio em relação ao padrão 802.11 tradicional (WEIL, 2009).

2.3 APLICAÇÕES QUE UTILIZAM REDES VEICULARES

De acordo com Jakubiak e Koucheryavy (2008), as redes veiculares devem ser utilizadas para aumentar a segurança e também a eficiência do tráfego nas vias urbanas e rodoviárias por meio da troca de dados entre os veículos pertencentes à via. Inúmeras aplicações voltadas à segurança em rodovias foram desenvolvidas, dentre estas aplicações, destacam-se as de Alertas de Perigo Local (LDW - *Local Danger Warnings*). Segundo Ostermaier, Dotzer e Strassberger (2007), este tipo de aplicação mostra-se como um dos mais promissores, devido ao significativo benefício coletivo trazido pela disseminação de mensagens informando as situações de risco na via. Nas redes veiculares, a cooperação entre os nós se faz necessária para um desempenho adequado, visto que existe uma frequente troca de dados entre os veículos (KOSCH, 2004).

Essas aplicações LDW possuem requisitos estritos de latência e confiabilidade para as mensagens, devem ser robustas à inserção de mensagens falsas e serem capazes de lidar com informações conflitantes (BENSLIMANE, 2005). Kosch (2004) define uma aplicação para troca de

mensagens de perigo local, que consiste em informações baseadas nas leituras obtidas pelos sensores locais dos veículos.

Paula, Oliveira e Nogueira (2010) abordam a necessidade dos condutores serem avisados o mais rápido possível a cerca de qualquer evento que ponha em risco a segurança de pessoas. Propõe então a tomada de ações paliativas para diminuir as possíveis consequências destes eventos, como o desenvolvimento de uma aplicação de mensagem de perigo local. Pode-se observar na Figura 2 uma situação como esta.

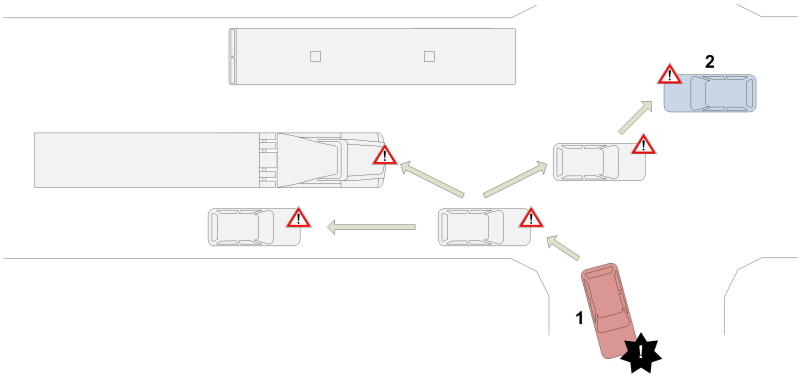

Figura 2: Detecção de eventos de risco.

Na Figura 2, o veículo 1, ao detectar o acúmulo de óleo na pista, dissemina na rede uma mensagem informando o problema aos veículos que estão próximo ao local. Estes então atuam como roteadores da mensagem, aumentando o alcance deste aviso. Desta forma, os motoristas terão tempo hábil para reagir a esta situação da maneira mais segura possível.

Existem aplicações voltadas à assistência ao condutor para auxiliar na condução do automóvel a partir de informações úteis. Algumas destas informações são recebidas a partir de serviços que podem ser oferecidos ao condutor. Serviços como, auxílio ao estacionar, controle de tráfego, sinalização em cruzamentos próximos ao automóvel, localização geográfica e aumento da percepção do condutor (CALISKAN; GRAUPNER; MAUVE, 2006). Uma destas aplicações vem sendo utilizada em cidades da Alemanha, como por exemplo, a cidade de Munique. Esta aplicação auxilia o condutor ao procurar por vagas para estacionar, e se mostra muito eficaz, podendo em muitos casos diminuir os congestionamentos comuns em áreas de estacionamento. A aplicação utiliza o

padrão 802.11b e foi simulada utilizando o simulador NS-2 (CALISKAN; GRAUPNER; MAUVE, 2006).

Rizvi et al. (2007) apresentam uma aplicação que utiliza redes veiculares para segurança no trânsito e que utiliza o padrão IEEE 802.11p. Trata-se de uma aplicação criada para alertar a chegada de veículos de emergência, fazendo com que os condutores abram caminho. O funcionamento consiste no envio de mensagens por difusão pelos veículos de emergência, informando a origem, o destino, e a identificação da rota, entre outros dados. Os demais veículos recebem estas informações com antecedência, de maneira que possam ter tempo o suficiente para decidir de que maneira agir.

O sim^{TD} (*Safe and Intelligent Mobility: Test Field Germany*) (ECKHOFF et al., 2011) é um projeto de pesquisa voltado para a comercialização de aplicações para VANETs. Uma das aplicações desenvolvidas no projeto é o *Traffic Information System* (TIS) que tem por objetivo fornecer aos condutores informações sobre as condições da estrada à sua frente e também um serviço de geração de rotas. Outro objetivo do projeto é também apoiar e incluir veículos que não estão equipados com mapas digitais (comerciais). Em vez de usar mapas préinstalados, os veículos geram seus mapas de forma autônoma, usando um receptor GPS e uma grade de referência mundial conhecida por todos os veículos (ECKHOFF et al., 2011).

Outro projeto voltado ao desenvolvimento de aplicações para VANETs é o WiSafeCar (ARNOULD et al., 2011), que consiste na pesquisa e prototipagem eficiente de mecanismos para redes veiculares, a fim de fornecer suporte a uma ampla gama de serviços para os usuários em movimento, mesmo que estes estejam fora de seus veículos. O WiSafeCar utiliza o protocolo IEEE 802.11p. Os serviços prestados vão desde serviços de segurança, tais como informações meteorológicas para regiões onde ocorrem acidentes por conta das condições climáticas a uma solução de transporte urbano dinâmico (ARNOULD et al., 2011).

Outras aplicações que visam aumentar a segurança no trânsito, e que se destacam são descritas no Apêndice B.

2.4 MODOS DE ORGANIZAÇÃO DA COMUNICAÇÃO EM VANETS

A comunicação em redes veiculares pode ser organizada para maximizar a eficácia no encaminhamento de informações. Protocolos da camada de rede devem ser cuidadosamente selecionados para oferecer uma organização que leve a uma utilização eficiente dos limitados

recursos de canal sem fio, sem comprometer a conectividade de rede (WILLKE; TIENTRAKOOL; MAXEMCHUK, 2009).

Segundo Xu e Gerla (2002) a comunicação nas redes veiculares *ad hoc* pode ser organizada nos modos plano ou hierárquico. Na organização plana, os nós estão em um mesmo nível, todos os nós têm a mesma função dentro da rede. O envio de mensagens desta rede ocorre por meio de difusão, utilizando mecanismos de inundação semelhantes aos descritos na Seção 2.5.1. Na Figura 3, pode ser observado como os nós são organizados em uma comunicação plana. A utilização da organização plana em redes veiculares traz como desvantagem a escalabilidade limitada, devido ao grande número de transmissões e retransmissões geradas durante a comunicação.

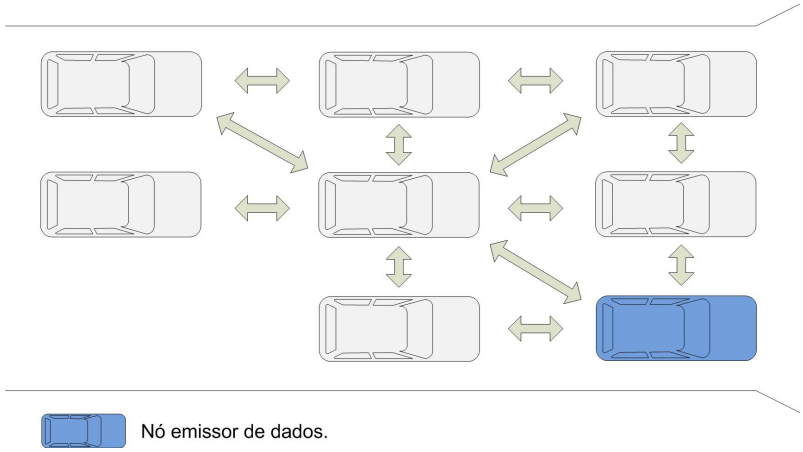

Figura 3: Organização plana.

Já na organização hierárquica, os nós da rede são separados em grupos (*clusters*). Nesses grupos, os nós podem assumir diferentes funções. Em um grupo existirá o nó que assumirá a função de líder, este nó será responsável pela disseminação das mensagens dentro do seu grupo, como pode ser observado na Figura 4. Os *clusters* podem se movimentar juntamente com os veículos ou serem fixados em certos locais, tais como intersecções. Os protocolos em (CHEN; CAI, 2005), (CHISALITA; SHAHMEHRI, 2002) e (REUMERMAN; ROGGERO; RUFFINI, 2005) apoiam ambas as definições. O primeiro nível de hierarquia é tipicamente um protocolo de encaminhamento, que liga os grupos diferente. As mensagens podem ser enviadas por veículos *gateways* e *clus-*

ters adjacentes podem utilizar a comunicação em malha para reduzir a latência de encaminhamento, como o que ocorre no protocolo BROADCOMM (DURRESI; DURRESI; BAROLLI, 2005). Um inconveniente proveniente destes agrupamentos é o *overhead* necessário para formar e manter a organização. Como um exemplo de formação, o primeiro veículo a transmitir uma mensagem pode eleger-se líder e depois definir que seu grupo seja todos os vizinhos a dois saltos de distância. No protocolo BROADCOMM (DURRESI; DURRESI; BAROLLI, 2005), *beacons* são utilizados para estabelecer os limites de comunicação. Ao contrário da comunicação plana, a comunicação hierárquica melhora a escalabilidade. Se houver problemas de comunicação, estes são tratados dentro do grupo, evitando que os problemas se propaguem pela rede (OHTA; INOUE; KAKUDA, 2003).

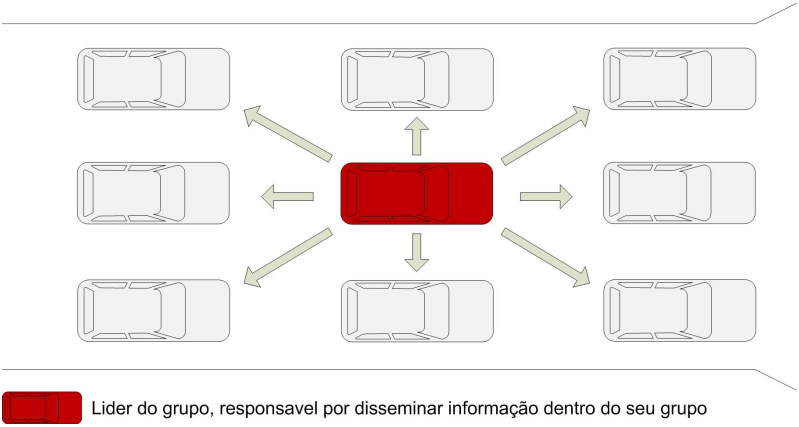

Figura 4: Organização hierárquica.

2.5 DISSEMINAÇÃO DE DADOS EM REDES VEICULARES

O mecanismo de difusão de mensagens (*broadcast*) é muito usado no âmbito das redes veiculares. Muitas aplicações voltadas as VANETs disseminam dados pela rede sem ao menos conhecer a identificação dos nós que efetivamente receberam estes dados. Muitas aplicações de segurança para rodovias utilizam difusão para alertar os condutores de perigos à frente (KOSCH, 2004).

Segundo Chang e Maxemchuk (1984), protocolos voltados a dis-

seminação de informações são divididos em duas classes, protocolos de difusão não confiável e de difusão confiável. Para Chang e Maxemchuk (1984) protocolos de difusão não confiáveis oferecem melhor esforço, desta forma priorizam a disseminação da informação sem garantir a entrega dos dados a todos os nós existentes na rede. Koubek, Rea e Pesch (2010), definem que um protocolo de difusão confiável deve garantir a entrega de uma mensagem a todos os nós pertencentes a uma rede, dentro de um intervalo de tempo, mesmo operando em um meio compartilhado, não confiável e sem fio em que a largura de banda é limitada. O protocolo confiável também deve garantir taxas de entrega elevadas para mensagens prioritárias para todas as densidades de veículos existentes na via (KOUBEK; REA; PESCH, 2010).

2.5.1 Protocolos de Difusão Não Confiáveis

Os protocolos de difusão não confiáveis têm como objetivo principal entregar uma mensagem ao maior número de nós pertencentes a rede dentro de um curto espaço de tempo. A disseminação de mensagens em redes *ad hoc* têm certos desafios, como a alta mobilidade dos nós e o pequeno período que os nós permanecem conectados (BECHLER et al., 2003). Pesquisadores, como Ni et al. (1999), Heissenbuttel et al. (2006), Zanella, Pierobon e Merlin (2004), Korkmaz et al. (2004) e Fasolo, Zanella e Zorzi (2006), desenvolveram abordagens para melhor a disseminação de dados em protocolos de difusão não confiáveis, estas abordagens são apresentadas a seguir.

2.5.1.1 Inundação

Segundo Jacobsson, Guo e Niemegeers (2005), protocolos de inundação são altamente distribuídos, uma vez que é da responsabilidade de cada nó determinar se vai participar na retransmissão ou não. Esta tomada de decisão normalmente é baseada no número de mensagens já recebidas pelo nó e também leva em consideração a localização atual da fonte de informações (JACOBSSON; GUO; NIEMEGEERS, 2005).

Ni et al. (1999) foram os primeiros a utilizar técnicas de inundação em redes *ad hoc* moveis e introduzir o termo *Broadcast Storm*. Esse termo denomina o problema que acontece quando se tenta enviar mensagens destinadas a todos os nós que formam a rede, forçando cada nó retransmitir a mensagem (inundação simples). A Inundação simples

resulta em três problemas graves, **mensagens duplicadas** (todos os vizinhos receberão a mensagem varias vezes), **disputa** (os nós disputarão o canal) e **colisão** (transmissões simultâneas e terminal oculto). Ni et al. (1999) apresentaram métodos diferentes para reduzir a redundância, inibindo alguns nós de retransmissão. Estes métodos são:

- **Método Probabilístico**: um nó retransmite a mensagem com uma probabilidade p, onde $0 \leq p \leq 1$. Pode-se notar que quando $p = 1$, este método será idêntico à inundação simples;
- **Método baseado em Contador**: ocorre quando um nó retransmite uma mensagem apenas se ouvir a mensagem c vezes, sendo que $c < C$ e C é uma constante (igual a 3 ou 4, tal como recomendado por Ni et al. (1999));
- **Método baseado na Distância**: um nó retransmite a mensagem somente se a distância entre o receptor e transmissor é $d > D$, sendo que D é uma constante.
- **Método baseado em Localização**: cada nó compara a sua localização com a localização do transmissor e calcula a cobertura adicional que pode ser fornecida assumindo que todos os nós têm cobertura omnidirecional. Um nó retransmite a mensagem somente se a cobertura adicional for maior que A, sendo que A é uma constante; e
- **Método baseado em *Clusters***: neste esquema, Ni et al. (1999) sugerem dividir a rede em grupos circulares (*clusters*), cada *cluster* tem um conjunto pequeno de nós atuando como um *gateway* para os *clusters* vizinhos. Neste método, apenas um *gateway* tem o direito de retransmitir a mensagem.

Finalmente, com experimentos realizados, Ni et al. (1999) puderam concluir que o regime baseado em localização resultou na mínima quantidade de mensagens duplicadas. Embora fosse a primeira vez que o problema associado à difusão por múltiplos saltos em redes *ad hoc* tenha sido estudado, Ni et al. (1999) apresentaram uma boa análise. Os experimentos realizados por Ni et al. (1999), segundo Heissenbuttel et al. (2006), apresentaram algumas deficiências fundamentais como, o algoritmo não ser eficaz em cargas elevadas de pacotes e não tratar do problema de nó oculto.

O protocolo *Dynamic Delayed Broadcasting* (DDB), proposto por Heissenbuttel et al. (2006), é apenas uma versão atualizada do método baseado em localização proposto por Ni et al. (1999). Nesse

protocolo, os nós que recebem o pacote difundido devem calcular a cobertura adicional que pode ser fornecida. Dependendo do tamanho da área, cada nó introduz um atraso antes de retransmitir o pacote, sendo que o atraso é mais longo para áreas de cobertura menores. Desta forma, os nós que têm uma probabilidade maior de atender a nós mais distantes irão transmitir primeiro o pacote. Este protocolo tem como ponto forte a escolha distribuída dos nós que deverão retransmitir as mensagens sem a utilização de qualquer informação prévia da topologia da rede. Segundo Heissenbuttel et al. (2006), o protocolo também reduz a quantidade de mensagens duplicadas de forma eficiente, mas não diminui a probabilidade de colisões e, por não utilizar uma confirmação de recebimento das mensagens, a confiabilidade global é degradada.

2.5.1.2 Única Retransmissão

Pode-se verificar que os protocolos de única retransmissão têm comportamento subsequente quando o nó transmissor lida com a responsabilidade de transmitir uma mensagem a um nó que o segue. O melhor nó para lidar com a função de retransmissão em protocolos de disseminação é o mais distante, por estar nas bordas do raio de cobertura do transmissor, assim podendo alcançar maiores distâncias. O problema presente nestes protocolos é como escolher o nó mais distante, sem qualquer informação prévia (KORKMAZ et al., 2004).

No protocolo *Minimum Connected Dominating Set* (MCDS), Zanella, Pierobon e Merlin (2004) definiram um conjunto mínimo de nós conectados e cada outro nó na rede localizado a um salto de distância está conectado a um nó pertencente a esse conjunto. Nos protocolos de transmissão baseados em MCDS, a mensagem é encaminhada apenas pelos nós dos MCDS. Esses protocolos atingem o maior progresso ao longo da linha de propagação, garantindo a cobertura de toda a rede. Os MCDS apresentam desempenho teórico ótimo. No entanto, esses protocolos precisam de informações em tempo real sobre a localização exata de cada nó da rede, que não é prático em redes veiculares. Este aspecto afeta qualquer solução que se baseie em um conhecimento completo ou parcial da topologia da rede (ZANELLA; PIEROBON; MERLIN, 2004).

O protocolo baseado em disseminação de informações chamado *Urban Multi-hop Broadcast Protocol* (UMB) tem como objetivo evitar o terminal oculto utilizando uma técnica na camada de aplicação semelhante ao *Request-To-Send* (RTS) e o *Clear-To-Send* (CTS) usados

no protocolo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), para diminuir o excesso de carga de controle e aumentar a confiabilidade na difusão em múltiplos saltos (KORKMAZ et al., 2004). Este protocolo trabalha em dois modos, difusão direcional e no modo interseção. O modo de difusão direcional seleciona o nó mais distante da origem para continuar a difusão. No modo interseção, o protocolo assume que repetidores são instalados nos cruzamentos para encaminhar a difusão (KORKMAZ et al., 2004).

Neste protocolo, o mecanismo de seleção do nó mais distante funciona da seguinte maneira: quando um nó recebe uma mensagem de *Request-To-Broadcast* (RTB), este nó transmite um sinal de interferência no canal de um comprimento proporcional à sua distância atual a partir do transmissor. Então, o nó que tem a intenção de transmitir uma determinada mensagem verifica o *status* do canal sem fio. Se o canal está ocupado com outro sinal de interferência, é por que outro nó ainda está transmitindo. Caso contrário, se o nó verifica que o canal está inativo, este nó será o mais distante e irá enviar uma mensagem de *Clear-To-Broadcast* (CTB). No caso em que há mais de um nó no segmento mais distante, os seus CTBs podem colidir. Em tal situação, o transmissor deverá reenviar o RTB novamente e refazer o mesmo procedimento (KORKMAZ et al., 2004).

O algoritmo proposto tem como pontos fortes não requerer informações sobre a densidade ou coordenadas geográficas de todos os nós presentes na vizinhança do transmissor e a robustez da topologia em qualquer volume de tráfego. Por utilizar o envio de um sinal de interferência para determinar o nó mais distante, este possui alta latência e limita a sua utilização em situações de emergência (YI et al., 2010).

O *Smart Broadcasting Protocol* (FASOLO; ZANELLA; ZORZI, 2006) possui o mesmo objetivo que o UMB, porém utilizando uma metodologia diferente. Após a recepção de uma mensagem de RTB, cada nó deve determinar seu segmento e, consequentemente, definir um tempo de *backoff* aleatório. Segmentos serão associados com janelas de contenção não sobrepostas ordenadas da mais externa para a mais interna (FASOLO; ZANELLA; ZORZI, 2006). Por exemplo, suponha que a janela de contenção tenha tamanho 4; os nós no segmento mais distante devem escolher aleatoriamente um tempo de *backoff* entre 0 e 3, nós no segmento mais próximo devem escolher um valor entre 4 e 7, e assim por diante.

Os nós irão diminuir seus temporizadores de *backoff* por 1 a cada *time slot* enquanto ouvem o canal. Enquanto espera, se algum nó receber uma mensagem CTB válida, este deve mudar da fase de

contenção para a fase de espera da transmissão. Caso contrário, se qualquer nó terminar a contagem de *backoff*, este enviará a mensagem CTB, contendo a sua identidade e retransmitirá qualquer mensagem entregue (FASOLO; ZANELLA; ZORZI, 2006).

Este protocolo realiza a mesma operação presente no protocolo UMB, porém depende apenas do tempo mínimo de espera. Segundo Fasolo, Zanella e Zorzi (2006), mesmo com os bons resultados obtidos durante os experimentos, o protocolo também tem deficiências como depender do tamanho da janela de contenção. Ainda segundo Fasolo, Zanella e Zorzi (2006) existem vários valores ideais para volumes de tráfego diferentes. O protocolo não proporciona um método para a estimativa do volume de tráfego atual, desta forma, o tamanho da janela de contenção será estático com um valor predeterminado, desta forma, a execução nunca chegará aos valores ideais.

2.5.2 Protocolos Confiáveis

A transmissão em redes sem fio pode servir para inúmeras aplicações em que a confiabilidade não é necessária e o tempo não é um requisito crítico. Com o surgimento das redes veiculares, trabalhos como, Xu et al. (2004), Alshaer e Horlait (2005) tornaram o tempo um requisito crítico e a confiabilidade extremamente importante para serviços destinados a grupos de aplicações de segurança no trânsito, pois a entrega confiável de mensagens pode evitar novos acidentes. Diante deste cenário, busca-se criar de um protocolo que entregue mensagens de uma única fonte para cada nó em sua faixa de transmissão com confiabilidade e minimo atraso.

Segundo Nakorn e Rojviboonchai (2010), as métricas relacionadas ao desempenho dos protocolos confiáveis são:

- **Taxa de sucesso**: o número de nós que têm recebido com sucesso a transmissão, dividido pelo número de nós na faixa de comunicação do transmissor; e
- **Latência**: o tempo total exigido para a entrega da mensagem.

Xu et al. (2004), Alshaer e Horlait (2005), Xie et al. (2005) e Balon e Guo (2006) utilizaram três métodos para aumentar a confiabilidade da transmissão, que são: Reenvio (do inglês *Rebroadcasting*); Reconhecimento Seletivo (do inglês *Selective Acknowledgment*); e Mudança de Parâmetros (do inglês *Changing Parameters*). Estes métodos estão descritos a seguir.

2.5.2.1 Reenvio (*Rebroadcasting*)

O termo *rebroadcasting* está relacionado diretamente com conceito de diversidade temporal. Este conceito define que um mesmo sinal pode ser enviado duas ou mais vezes durante um determinado espaço de tempo. Desta forma, é necessário que o transmissor armazene a informação para que posteriormente possa reenviá-la (LIU; XU, 2004). O primeiro método para aumentar a confiabilidade da transmissão resume-se em reenviar a mesma mensagem de forma redundante. Este método traz como questão principal a quantidade necessária de reenvios que devem ser realizados para que a transmissão seja confiável.

Em (XU et al., 2004), os autores exploraram o efeito do reenvio com o objetivo de aumentar a confiabilidade e, a partir de seus estudos, desenvolveram seis protocolos:

- ***Asynchronous Fixed Repetition* (AFR)**: a mensagem é repetida em cada intervalo de tempo um número fixo de vezes;
- ***Asynchronous p-persistent Repetition* (APR)**: o nó transmissor reenvia a mensagem em cada intervalo de tempo com probabilidade P, tal que P é um parâmetro configurável. Esta probabilidade P define se o nó irá ou não reenviar a mensagem;
- ***Synchronous Fixed Repetition* (SFR)**: é o mesmo que AFR, exceto que todos os nós da rede são sincronizados com um relógio global;
- ***Synchronous p-persistent Repetition* (SPR)**: é o mesmo que APR, exceto que todos os nós da rede são sincronizados com um relógio global;
- ***Asynchronous Fixed Repetition with Carrier Sensing* (AFR-CS)**: é o mesmo que AFR, exceto por verificar se o canal está livre antes da transmissão; e
- ***Asynchronous p-persistent Repetition with Carrier Sensing* (APR-CS)**: é o mesmo que APR, exceto por verificar se o canal está livre antes da transmissão.

Nos experimentos, embora os protocolos SFR e AFR-CS terem obtido a melhor taxa de sucesso, os autores sugerem a utilização do AFR-CS, uma vez que este não requer uma sincronização global, além de prover sobrecarga mínimo (XU et al., 2004).

Xu et al. (2004) foram os primeiros a abordar o reenvio como um método para aumentar a confiabilidade, porém os métodos desenvolvidos não resolveram o problema do nó oculto e o protocolo AFR-CS exige o mesmo número de repetições independente das condições da rede e do volume de tráfego.

Alshaer e Horlait (2005) propuseram um algoritmo de reenvio adaptativo, no qual cada veículo determina a sua própria probabilidade de reenvio de acordo com uma estimativa da densidade de veículos em seu entorno dentro de dois saltos. As informações de densidade são obtidas a partir dos pacotes periódicos (*beacons*[1]) que são trocados entre os nós da rede, estes pacotes estão envolvidos diretamente com protocolos de roteamento. Este algoritmo tem como maior fraqueza a dependência do protocolo de roteamento utilizado. Além disso, este ignora o efeito do problema do nó oculto.

2.5.2.2 Reconhecimento Seletivo (*Selective Acknowledgment*)

Segundo Xie et al. (2005), reconhecimento seletivo é um método de comunicação confiável amplamente aplicado em mensagens *unicast*. Porém, muitas vezes na difusão, o nó de destino é desconhecido. O problema discutido nesta subseção é como o reconhecimento pode ser usado para prover confiabilidade à transmissão *broadcast*.

O protocolo *Broadcast Medium Window* (BMW) (TANG; GERLA, 2001) trata a difusão como múltiplos *unicasts*. Cada mensagem *unicast* é processada usando o protocolo MAC IEEE 802.11 DCF (CSMA / RTS / CTS / DATA / ACK). Cada nó armazena 3 listas:

1. *Neighbor List*: lista dos nós vizinhos;
2. *Send Buffer*: lista das mensagens já transmitidas; e
3. *Receiver Buffer*: lista do número de sequência recebida.

Um nó, ao receber uma mensagem, atualiza logo a sua tabela *Neighbor List* que contém a lista dos nós vizinhos. Cada nó armazena as mensagens que transmite na tabela *Send Buffer*, pois poderá ser necessário a sua retransmissão, e só as apaga do *Buffer* quando todos os receptores as recebem. Finalmente, cada nó mantém na tabela *Receiver Buffer* o número de sequência recebido correspondente a uma determinada mensagem.

[1] Pequenos pacotes de dados que armazenam informações pertinentes aos nós (HARTENSTEIN; LABERTEAUX, 2010).

O protocolo BMW é confiável porque o emissor retransmitirá uma mensagem de dados quantas vezes for necessário até receber um ACK dos seus receptores, ou seja, com este procedimento consegue garantir que todos os nós de destino receberão as mensagens que lhes são destinados. Mas por outro lado, este tipo de comportamento introduz alguma ineficiência de desempenho devido a necessidade de pelo menos uma fase de contenção cada vez que precisar enviar uma mensagem. Como o acesso ao meio é justo (oportunidades de acesso semelhantes para todos os nós), o nó emissor também terá de se conter perante os outros nós para acessar o canal. Dessa forma, os outros nós podem ter acesso ao meio, interrompendo o procedimento de *multicast*. Segundo Tang e Gerla (2001), em muitas aplicações que utilizam *multicast*, se o pedido *multicast* não for realizado dentro de um determinado período de tempo as camadas acima do MAC podem considerar o pedido como inválido, fazendo com que seja sempre atingido o *timeout* e, consequentemente, irão gerar mais mensagens na rede. Ainda segundo Tang e Gerla (2001), este protocolo tem como ponto fraco a alta latência, especialmente em casos de elevada densidade de nós.

No protocolo *Round-Robin Acknowledge and Retransmit* (RRAR), Xie et al. (2005) sugerem que cada mensagem de difusão deve conter um pedido de ACK para apenas um dos vizinhos, o vizinho selecionado ao receber a mensagem deve confirmar o recebimento. Para cada novo pacote a ser transmitido, o transmissor seleciona um nó diferente em estilo *round-robin*. Este protocolo assume que cada nó tem uma lista atualizada dos nós da vizinhança, assim poderá selecionar apenas um vizinho para responder a entrega da mensagem.

Conclui-se com a analise feita que protocolos de única retransmissão e os protocolos de reconhecimento seletivo parecem semelhantes, porém são projetados para diferentes objetivos. Os protocolos de única retransmissão são projetados para disseminarem o mais rápido possível as informações e oferecem melhor esforço, desta forma, sacrificam a confiabilidade. No entanto, protocolos que utilizam reconhecimento seletivo são projetados para uma melhor confiabilidade por meio do reconhecimento de cada nó vizinho, um por um.

2.5.2.3 Mudança de Parâmetros (*Changing Parameters*)

Balon e Guo (2006) propuseram um protocolo que minimiza a taxa de colisão variando o tamanho da janela de contenção, os autores também buscaram aumentar a confiabilidade da transmissão utilizando

o reenvio das mensagens a cada 100 ms. Balon e Guo (2006) usaram uma aplicação DSRC[2] (com a premissa de que cada nó deve transmitir uma mensagem de *status* a cada 100 ms) como fonte de informações sobre o estado da rede. Nesse protocolo, cada nó deve incluir seu próprio endereço MAC e um número de sequência dentro da mensagem de *status*. Assim, é possível estimar a quantidade de mensagens perdidas e alterar o tamanho da janela de contenção. Em caso de taxa de perdas baixa, que indica uma condição boa da rede e pequeno número de veículos, o protocolo deve tentar diminuir o tamanho da janela de contenção e, portanto, diminuir a latência. Em caso contrário, se a taxa de perdas é alta, o protocolo aumenta o tamanho da janela de contenção. Embora o protocolo minimize a probabilidade de colisão, este ignora problemas como, o do nó oculto (BALON; GUO, 2006).

2.6 CODIFICAÇÃO DE REDE

Atualmente, a disseminação da informação é realizada juntamente com o roteamento, sendo a informação armazenada por nós intermediários e, em um segundo momento, encaminhada para os nós seguintes até chegar a seu destino (YEUNG; CAI, 2006). Segundo Yeung e Cai (2006) há estudos que comprovaram que o processamento da informação nos nós intermediários trazem benefícios na replicação e difusão dos dados.

Ahlswede et al. (2000) mostraram que o processamento nos nós intermediários é necessário para que uma maior vazão nos dados possa ser obtida, dando origem à denominada codificação de rede (do inglês *Network Coding*). Os dados que são independentemente produzidos e consumidos não precisam ser necessariamente mantidos separados, enquanto eles são transportados pela rede. Há maneiras de combinálos e depois extrair as informações originais de forma independente (AHLSWEDE et al., 2000). Com a codificação de rede, diversos tipos de ganhos podem ser obtidos, seja em termos de vazão, segurança e desempenho (FRAGOULI; SOLJANIN, 2007).

Para uma rede *unicast* o roteamento é suficiente para atingir o fluxo máximo da rede. Porém, em redes *broadcast*, a codificação de rede pode ser necessária (AHLSWEDE et al., 2000). Os primeiros benefícios de

[2] Aplicação desenvolvida propriamente para redes veiculares, O DSRC (*Dedicated Short Range Communications*) é um serviço de comunicação, na banda de 5.9 GHz destinado entre o pequeno e médio alcance, que suporta operações de segurança pública rodoviária bem como operações privadas entre veículos e entre a via pública e os veículos (ZEADALLY et al., 2010).

codificação de rede foram demonstrados em termos de vazão em uma rede *multicast*, através da rede borboleta (AHLSWEDE et al., 2000). A rede borboleta é representada na Figura 5, a qual representa uma rede de comunicação na forma de um grafo direcionado, no qual os vértices correspondem aos nós da rede e as arestas representam os canais. A rede é composta por duas fontes *F1* e *F2* e dois destinos *R1* e *R2*. Assume-se que as fontes *F1* e *F2* podem enviar somente um bit por instante de tempo, denotados por *b1* e *b2*, respectivamente. Se o receptor *R1* utiliza todos os recursos da rede para si próprio, ele pode receber a informação de ambas as fontes, de acordo com o apresentado na Figura 5(a). O mesmo acontece para o receptor *R2* na Figura 5(b).

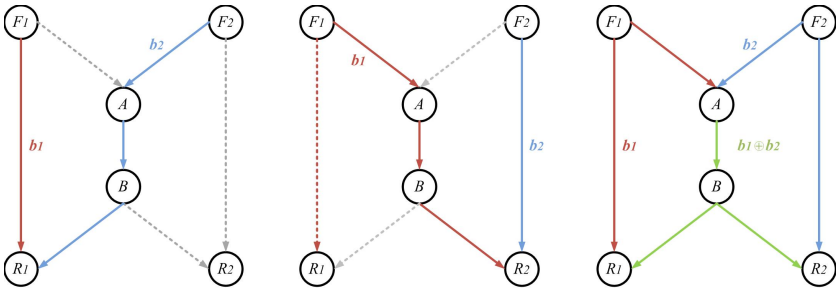

Figura 5: Rede borboleta. As fontes *F1* e *F2* realizam a difusão de suas mensagens para os receptores *R1* e *R2*.

Agora, se ambos os receptores precisam receber os sinais de ambas as fontes (*broadcast*), há uma limitação no ramo *AB*, visto que através deste ramo pode-se enviar somente um bit por instante de tempo e deseja-se enviar simultaneamente o bit *b1* para o receptor *R2* e o bit *b2* para o receptor *R1*. Tradicionalmente, o fluxo de informação era tratado de forma semelhante ao tráfego de automóveis (AHLSWEDE et al., 2000). Informações independentes eram mantidas separadas. Aplicando este conceito ao exemplo em questão, somente um dos bits *b1* e *b2* poderia ser enviado pelo ramo *AB* por instante de tempo.

Em Ahlswede et al. (2000), foi observado que os nós intermediários podem ser aptos a processar as informações recebidas, ao invés de simplesmente as encaminharem. No exemplo da Figura 5(c), o nó A pode realizar a operação XOR (adição no campo binário, denotada por $\oplus$) com os bits *b1* e *b2* e criar um terceiro bit $b3 = b1 \oplus b2$. O receptor *R1* poderia recuperar *b1* e *b2* ao receber *b1*, $b1 \oplus b2$. De

forma análoga, o receptor *R2* poderia recuperar *b1* e *b2* a partir de *b2*, $b1 \oplus b2$. O exemplo anterior mostra que ao permitir que nós intermediários combinem informações e as mesmas possam ser extraídas nos receptores, um ganho em termos de taxa de transmissão é obtido. Além do aumento no fluxo de informação, codificação de rede tem sido utilizada atualmente para outros fins, tais como aumentar a segurança e prover um melhor tratamento de erros em redes sem fio. Trabalhos como (OLIVEIRA et al., 2011) e (CRUZ et al., 2012) utilizam o XOR para melhorar o roteamento de mensagens em redes veiculares, já Zhang et al. (2011) utilizam o XOR para diminuir a quantidade de reenvios em redes sem fio. Nesta dissertação, a codificação de rede foi utilizada com o intuito de diminuir a quantidade de reenvios de alertas em um cenário veicular.

2.7 SIMULAÇÃO DE APLICAÇÕES EM REDES VEICULARES

Para realizar testes e avaliar protocolos voltados as redes veiculares em um ambiente real, é preciso utilizar veículos, condutores e equipamentos, o que torna os custos com testes elevados. Certamente, haverá repetições de um determinado experimento em um ambiente com muitos parâmetros que podem variar e isto se torna difícil, pois em algum momento uma ou mais variáveis podem não se mostrar satisfatórias para os testes (PUNZO; CIUFFO, 2011). A utilização de simuladores se mostra atraente por permitir o controle sobre o ambiente e por consumir menos recursos. Mesmo assim, reproduzir condições encontradas num ambiente real se torna um desafio, pois envolve inúmeras variáveis como, interferências, velocidade dos nós, distância entre os nós, transmissão de dados, etc. Além disso, trata-se de uma rede móvel, para a qual devem ser desenvolvidos modelos de mobilidade específicos (PUNZO; CIUFFO, 2011).

Segundo Sommer e Dressler (2008) simuladores voltados a redes veiculares geram suas simulações por meio da utilização de duas partes complementares, o modelo de rede e o modelo de mobilidade. O modelo de rede é responsável por identificar a pilha de comunicação, ou seja, o modelo do canal sem fio, modelo de propagação, camada MAC, camada de rede, camada de aplicação, etc. O modelo de rede utilizado em simulações voltadas as redes veiculares é o mesmo utilizado em redes móveis (SOMMER; DRESSLER, 2008).

De acordo com Tampere e Arem (2001), o modelo de mobilidade é responsável por identificar os diferentes aspectos da mobilidade dos

veículos. Modelos de mobilidade para simulações são classificados, segundo Tampere e Arem (2001), de acordo com o nível de detalhe com o qual representam o sistema de tráfego. Estes níveis são: microscópico, mesoscópico e macroscópico. O modelo microscópico descreve os veículos e suas interações em um alto nível de detalhe, de forma inteiramente individualizada. Desta forma, os resultados de saída dos modelos microscópicos são bem mais detalhados, sendo possível obter valores de diversas variáveis de forma totalmente desagregada, para qualquer momento ou intervalo de tempo desejado da simulação (PUNZO; CIUFFO, 2011).

Segundo Tampere e Arem (2001), o modelo mesoscópico forma uma classe intermediária quanto ao realismo e detalhamento. Geralmente, neste nível de modelagem, os veículos são agrupados em pelotões de tráfego e tratados desta forma quanto a tamanho, localização, velocidade e aceleração. Os modelos mesoscópicos são normalmente utilizados em redes semafóricas e procuram explicar a dispersão dos pelotões de tráfego ao longo do tempo e do espaço (TAMPERE; AREM, 2001). Estes modelos são capazes de lidar com pequenas mudanças nos padrões de tráfego em curtos períodos de tempo, os quais podem ser da ordem de alguns segundos. Assim, estes modelos são bastante utilizados na representação de formação e dispersão de filas em interseções que utilizam semáforos, o que torna alguns modelos aptos a simularem a escolha de rotas por parte dos condutores. O nível de detalhe nesses modelos de simulação pode mudar ao longo do tempo dependendo das condições de tráfego (TAMPERE; AREM, 2001).

O modelo macroscópico descreve tanto os veículos quanto as interações entre estes em um alto nível de abstração. Por exemplo, o tráfego é representado na forma de variáveis como, volumes, densidades e velocidades. O movimento referente a mudança de pista não é representada uma vez que os veículos são representados por blocos (pelotões), desta forma não existem distinções entre os veículos e sim entre grupos formados por veículos (TAMPERE; AREM, 2001). Porém, os modelos macroscópicos têm a vantagem de serem eficientes com relação ao processamento computacional e são úteis para simulações quem envolvem valores grosseiros de densidade, velocidade e fluxo. Em geral, estes modelos são altamente sensíveis aos parâmetros iniciais o que pode ter um impacto arbitrário sobre o comportamento global do sistema (HARRI; FILALI; BONNET, 2009).

Por mais que os modelos microscópicos sejam geralmente complexos, de desenvolvimento custoso e exigirem uma quantidade muito maior de parâmetros. Ainda assim, estes são a realidade ou a tendên-

cia em simulações de tráfego uma vez que são a única forma de se lidar com comportamentos individuais que estão se tornando importantes no processo de planejamento e principalmente controle de tráfego (PUNZO; CIUFFO, 2011).

Segundo (HARRI; FILALI; BONNET, 2009), um modelo de mobilidade realista deve incluir as seguintes características:

- Mapas topológicos precisos e realistas: os mapas devem incluir diferentes tipos de estradas, cada estrada com a quantidade correta de faixas de rodagem;
- Interseções com semáforos: mapas deve conter cruzamentos onde os veículos devem diminuir a velocidade. Os veículos também devem reagir de forma apropriada aos semáforos;
- Mudança de faixas: motoristas mudam de faixa durante o trajeto. Por isso, este comportamento deve ser modelado durante as simulações;
- Desaceleração e aceleração: os veículos não param ou aceleram abruptamente, modelos de desaceleração e aceleração devem ser incluídos nas simulações;
- Padrões de condução inteligente: motoristas interagem com seus ambientes, não só com relação aos obstáculos estáticos, mas também com obstáculos dinâmicos, como carros vizinhos e pedestres;
- Comportamento humano: condutores são seres humanos e não máquinas. Todos os modelos de condução devem ser probabilísticos, com certa tolerância a erros que podem resultar em acidentes simulados.
- Distribuição de veículos não aleatória: como pode-se observar na vida real, as posições iniciais dos veículos não são uniformemente distribuídas na área de simulação.
- Diferentes tipos de veículos: A tecnologia VANET não é dirigida apenas aos veículos de passeio, outros veículos como, ônibus, vans, caminhões, trens e motos também podem usufruir desta tecnologia. Cada tipo de veículo deve ter seu próprio modelo.
- Efeito do protocolo implementado sobre a mobilidade: Quase todos os modelos de mobilidade são usados para gerar um tráfego predefinido antes da simulação em si, sem qualquer efeito do protocolo implementado. Se o pesquisador deseja medir a melhoria

de sua rede, de acordo com as mudanças no fluxo de veículos provocadas pelo protocolo testado, este deve ter um simulador que permita a mudança dos movimentos futuros de acordo com os eventos do modelo de rede.

Todos esses recursos são recomendados para um modelo de mobilidade ser o mais realista possível, porém, torna-se muito complexo forçando a utilização de muitas variáveis e seu desenvolvimento torna-se dispendioso. Segundo Punzo e Ciuffo (2011), modelos complexos podem ser úteis apenas na avaliação final do protocolo, mas não durante o ciclo de desenvolvimento do mesmo, no que o pesquisador deve estudar o efeito de seu protocolo em situações específicas. Note-se que, o modelo de rede utilizado no simulador deve também ser adequado para as suas necessidades, com a possibilidade de desenvolvimento de novos protocolos.

Existem diversos simuladores de redes veiculares disponíveis, dentre os mais difundidos tem-se: NS-2, OMNeT++, GloMoSim, QualNet, OPNET, NCTUns e MATLAB. Dentre os geradores de mobilidade disponíveis, destacam-se SUMO, Ghost, VanetMobiSim e CanuMobiSim.

2.7.1 Modelos de Mobilidade

A evolução histórica dos modelos de mobilidade utilizados em simulações de protocolos e aplicações para redes veiculares está ilustrada na Figura 6. Segundo Dressler et al. (2008), os primeiros modelos de mobilidade são relativamente simples, os nós utilizam apenas movimentos aleatórios. Estes modelos de mobilidade aleatórios não refletem de forma realista os movimentos dos veículos nas estradas. As soluções mais complexas vêm sendo desenvolvidas com base no mundo real, sendo acopladas à micro-simulação de tráfego rodoviário e de rede. Em (DRESSLER et al., 2008), os quatro modelos de mobilidade citados na Figura 6 são definidos e explicados. Neste trabalho foi adotado o modelo de simulação bidirecionalmente acoplada.

Nos casos em que, por exemplo, informações de acidentes, avisos de perigo, ou a informações relevantes ao tráfego rodoviário, podem influenciar no comportamento dos condutores, estas informações podem ser transmitidas através de uma rede veicular. Isto requer uma cooperação intensa entre as diferentes ferramentas de simulação. Os simuladores bidirecionalmente acoplados têm sido recentemente desenvolvidos e podem ser utilizados, não só para fornecer informações mais detalhadas sobre os efeitos de determinados parâmetros sobre o trá-

fego na rede, mas ao mesmo tempo ter um impacto significativo sobre as simulações. Este modelo permite movimentos realistas, a obtenção de informações sobre o comportamento dos nós e facilita a analise dos resultados. Também permite a parametrização da rede e das aplicações desenvolvidas. Simuladores como ns-2 e OMNeT++ suportam tal modelo.

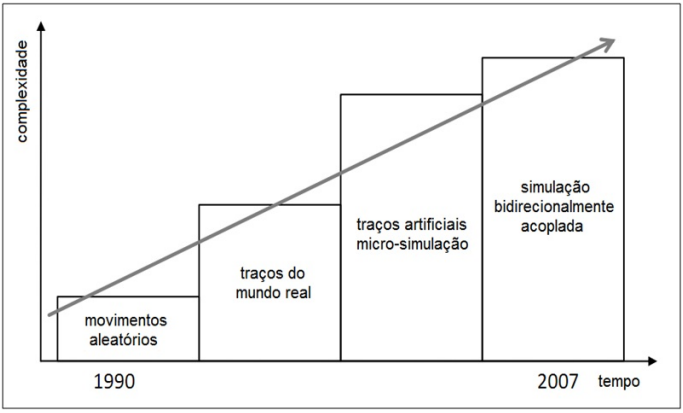

Figura 6: Evolução dos modelos de mobilidade.

2.8 CONSIDERAÇÕES DO CAPÍTULO

As aplicações de trocas de mensagens de alerta surgem como uma boa alternativa para criar condições seguras de circulação para os veículos que trafegam em uma via. Neste tipo de aplicação, eventos de riscos detectados pelos sensores dos veículos geram mensagens de avisos que são disseminadas pela rede nas quais são divididas por regiões, fazendo com que as mensagens sejam propagadas de forma otimizada.

Nas redes veiculares, pelo fato de diversos nós colaborarem sem um ponto central, algumas tarefas tornam-se mais difíceis de serem realizadas de forma eficiente. Portanto, um dos desafios neste tipo de rede é a inserção de novos mecanismos que possam torná-las mais seguras e confiáveis, sem adicionar riscos no comprometimento de seu desempenho.

A confiabilidade é extremamente importante para serviços destinados a aplicações de segurança no trânsito, pois a entrega confiável de

mensagens pode evitar novos acidentes. Diante deste cenário, o maior desafio é a concepção de um protocolo que possa entregar mensagens com maior confiabilidade possível e com latência mínima.

A transmissão confiável de mensagens de dados surge por meio de implementações de mecanismos e protocolos voltados ao gerenciamento das informações vindas da rede veicular e que procuram garantir a entrega de mensagens a todos os nós da rede. Os trabalhos descritos neste capítulo são os mais relevantes no contexto das redes veiculares e serviram de base para o entendimento sobre a confiabilidade na entrega de mensagens em redes veiculares e para definição do protocolo proposto neste trabalho.

3 TRABALHOS RELACIONADOS

3.1 INTRODUÇÃO

A abordagem tradicional para a difusão de informações é usar protocolos de inundação (KOUBEK; REA; PESCH, 2010). Após a recepção de uma mensagem transmitida, o nó retransmite a mensagem imediatamente. Esta abordagem pode fornecer rapidez à difusão de dados e é simples por não precisar obter informações dos nós vizinhos. No entanto, esta abordagem não funciona bem em áreas densas e em redes esparsas. Em áreas que possuem densidade elevada de nós, como por exemplo, congestionamento de veículos em horários de pico, fazem com que o uso da inundação acarrete uma alta quantidade de colisões de pacotes e uma baixa confiabilidade por gerar alta taxa de perdas de pacotes de dados (KOUBEK; REA; PESCH, 2010).

Um problema enfrentado por protocolos de transmissão voltados às redes veiculares é a disputa do canal pelos nós pertencentes a rede. Estes protocolos devem prover uma elevada cobertura, independentemente da densidade da rede ou da alta taxa de desconexões. Também devem funcionar diante de veículos com velocidades diferentes, tanto veículos parados ou em alta velocidade (NAKORN; ROJVIBOONCHAI, 2010).

Em um cenário esparso como as rodovias durante a noite, os veículos movem-se em alta velocidade e, possivelmente, não possuem vizinhos em sua faixa de transmissão. Partindo deste cenário, a inundação pode não atender de forma adequada a rede, pois não existem vizinhos suficientes para que a mensagem seja difundida (TONGUZ et al., 2007).

No âmbito das redes veiculares, protocolos de difusão confiável foram propostos. Neste trabalho, foram selecionados, por meio de uma revisão sistemática (Apêndice A), os seguintes protocolos: *Preferred Group Broadcast* (PGB) (NAKORN; ROJVIBOONCHAI, 2010), *Edge-Aware Epidemic Protocol* (EAEP) (NEKOVEE; BOGASON, 2007), *Position-aware Reliable Broadcasting protocol* (POCA) (NAKORN; ROJVIBOONCHAI, 2010), *Acknowledged Parameterless Broadcast in Static to Highly Mobile* (ackPBSM) (NAKORN; ROJVIBOONCHAI, 2010), *Reliable Broadcast routing based on Gain Prediction* (RB-GP) (CHUAN; JIAN, 2012), *Reliable Opportunistic Broadcast in VANETs* (R-OB-VAN) (LAOUITI; MUHLETHALER; TOOR, 2009), *Density-aware Reliable Broadcasting Protocol* (DECA) (KAMOLTHAM; NAKORN; ROJVIBOONCHAI,

2011) e *Reliable Routing scheme based on Vehicle Moving Similarity* (RR-VMS) (WEI; WANG; HSIEH, 2011). Estes protocolos foram escolhidos por empregarem a técnica *store-and-forward*, que consiste em armazenar a mensagem recebida e posteriormente retransmiti-la. Esta técnica permite minimizar o problema de conectividade intermitente. Estes protocolos serão discutidos e detalhados nas seções seguintes. Por fim, uma análise comparativa é descrita no final do capítulo.

3.2 EDGE-AWARE EPIDEMIC PROTOCOL (EAEP) (2007)

Protocolos epidêmicos são baseados em disseminação de informação probabilística. Desta forma, não utilizam *beacons* e não exigem nenhum conhecimento da topologia da rede local ou global. Estes algoritmos são propensos a desempenhos pouco confiáveis em redes conectadas de forma intermitente, por exemplo, quando é preciso entregar uma única mensagem a todos os nós da rede (NAGARAJ; DHAMAL, 2011).

O protocolo EAEP foi projetado especificamente para redes veiculares e tem como um de seus objetivos resolver o problema da conectividade intermitente existente em protocolos epidêmicos anteriores. Nesse protocolo, assume-se que cada veículo conhece sua própria localização geográfica. Cada mensagem contém a posição do veículo fonte e pode também conter um parâmetro que determina se a mensagem deve ser propagada em um direção específica ou se a propagação é omnidirecional. Além disso, as mensagens propagadas contêm o parâmetro TTL (*Time-To-Live*) que determina a quantidade de saltos que a mensagem dará na rede (NEKOVEE; BOGASON, 2007).

Segundo Nekovee e Bogason (2007), o protocolo trata tanto a disseminação de mensagens direcionais, quanto a disseminação de mensagens omnidirecionais. Para a propagação omnidirecional o protocolo funciona da seguinte maneira: o nó, ao receber uma nova mensagem, espera um tempo aleatório antes de definir se retransmite ou não a mensagem. Este tempo de espera cresce exponencialmente de acordo com a distância que o nó receptor está do nó transmissor. Este tempo aleatório é definido a partir do intervalo $[0, T_{max}]$, sendo que:

$$T_{max} = \min \begin{cases} \frac{T_0}{U} \exp\left(\frac{|x_{rec} - x_{sou}|}{L}\right) \\ T_{min} = \frac{T_0}{2U}, \end{cases} \tag{3.1}$$

Com U é o parâmetro usado para indicar a urgência da mensagem e L e T_0 são parâmetros do protocolo. x_{rec} e x_{sou} representam respectivamente a posição do nó receptor e do nó transmissor. Para de-

finir o tempo de espera, o nó conta quantas vezes recebeu a mensagem dos veículos que estão a sua frente e também dos veículos que estão lhe seguindo. Com base na diferença destas contagens, o nó toma uma decisão probabilística para retransmitir ou não a mensagem recebida. A probabilidade de retransmissão P, é obtida a partir de:

$$T_{max} = \min \begin{cases} 1 & \text{if } N_f \text{ or } N_b = 0 \\ 1 - \exp\left(-\alpha \frac{|N_f - N_b|}{N_f + N_b}\right) & \text{caso contrário.} \end{cases} \tag{3.2}$$

Na Equação 3.2 N_f e N_b representam o número de vezes que o veículo recebeu a mensagem, vindas de sua frente e de trás, respectivamente, e o parâmetro α tem como objetivo controlar as retransmissões redundantes. Tomada a decisão de retransmitir, o nó volta para a fase de espera durante o qual continua a atualizar seus contadores. Desta forma, apenas os nós que possuírem uma contagem de mensagens "desequilibrada" irão manter a mensagem viva na rede.

No caso da transmissão direcional, a Equação 3.2 é modificada de tal modo que se uma mensagem é de propagação *forward/backward*, a mensagem é mantida viva apenas pelos nós mais distantes dentro do raio de cobertura do transmissor. Neste caso, a probabilidade de transmissão P é calculada a partir de:

$$P = \begin{cases} 1 & \text{if } N_k = 0 \\ 1 - \exp\left(-\alpha \frac{|N_k|}{N_k + N_{\bar{k}}}\right) & \text{caso contrário.} \end{cases} \tag{3.3}$$

sendo que N_k é a quantidade de mensagens recebidas a partir da direção de propagação da mensagem (por exemplo, se k determinar que a mensagem veio de um transmissor a frente, então N_k é o número de mensagens recebidas a partir de veículos que estão a frente do receptor), e $N_{\bar{k}}$ é o número de mensagens recebidas a partir da direção oposta.

Esse protocolo supera a técnica de inundação simples em termos de confiabilidade e introduz menor sobrecarga. No entanto, o protocolo acarreta elevado atraso na disseminação das mensagens. De acordo com Nagaraj e Dhamal (2011), em cenários simulados foram preciso mais de 30 segundos para entregar uma única mensagem para a maioria dos veículos presentes na rede.

3.3 RELIABLE OPPORTUNISTIC BROADCAST IN VANETS (R-OB-VAN) (2009)

O objetivo principal do protocolo R-OB-VAN (LAOUITI; MUHLETHALER; TOOR, 2009) é fazer com que os veículos que estiverem impossibilitados de receber mensagens dos transmissores designados, recebam estas mensagens, por meio de qualquer outro receptor que seja capaz de se comunicar com estes nós. Mais precisamente, se existir algum veículo vizinho de tais veículos bloqueados na rede, estes vão assumir a responsabilidade de repassar a mensagem de emergência. Isto pode resultar na mensagem ser retardada ligeiramente, porém, os veículos bloqueados receberão a mensagem eventualmente (LAOUITI; MUHLETHALER; TOOR, 2009).

O protocolo R-OB-VAN tem como suposição básica que a sombra que impede certo veículo de receber as mensagens, seja, a longo prazo, da ordem de dezenas de segundos. Se uma mensagem de emergência é gerada durante este período, várias transmissões serão perdidas. Além disso, o veículo bloqueado, provavelmente, desaparecerá da lista de informações de seus vizinhos. A implicação desse pressuposto é que Laouiti, Muhlethaler e Toor (2009) não consideraram o desvanecimento que tem curta duração. Partindo desse pressuposto, os autores desenvolveram três variantes para fornecer confiabilidade em abordagens de disseminação oportunística (LAOUITI; MUHLETHALER; TOOR, 2009).

Os autores consideraram um cenário de rodovia, na qual as chances de um acidente em alta velocidade são maiores. Foram assumidos que a densidade de veículos na vizinhança do acidente é uniforme e a partir do momento que ocorreu o acidente uma mensagem de emergência deverá ser transmitida pelos veículos envolvidos. O componente OB-VAN do R-OB-VAN irá transmitir esta mensagem rapidamente na rede, enquanto a componente de confiabilidade vai tentar garantir que todos os veículos recebam a mensagem. A seguir, são descritas as variantes desenvolvidas para obter confiabilidade no R-OB-VAN (LAOUITI; MUHLETHALER; TOOR, 2009).

3.3.1 R-OB-VAN Primeira Variação (2009)

A primeira variação é baseada na exigência de que os veículos tenham informações básicas sobre a sua vizinhança ou seja, eles sabem o número de vizinhos que cada veículo a um salto de distância tem. Estas informações podem ser facilmente fornecidas para os vizinhos

de um veículo usando *beacons*. Supondo que cada veículo tem informações sobre a vizinhança, então a primeira variante é simplesmente descrita como: *Um veículo irá retransmitir uma mensagem de emergência que recebeu corretamente* ***se*** *um de seus vizinhos tiver menos vizinhos do que um número mínimo pré-definido*. Este limite é chamado de (*MIN_NEIGHBORS*) e seu valor pode ser maior ou igual a 1, dependendo da densidade da rede. Este é o mais simples das três variantes, no entanto, a escolha deste limite mínimo é importante porque um valor alto criará sobrecarga inútil devido às retransmissões extras (LAOUITI; MUHLETHALER; TOOR, 2009).

3.3.2 R-OB-VAN Segunda Variação (2009)

A segunda variação baseia-se também na exigência de que os veículos devem conhecer o número de vizinhos que cada veículo tem a um salto de distância. Esta informação pode ser obtida através da troca de *beacons*, como descrito anteriormente. Esta variante é mais dinâmica porque a decisão para retransmitir não baseia-se em um número pré-definido. Supondo que cada veículo sabe o número de vizinhos que cada um de seus vizinhos tem, então pode-se descrever a segunda variante simplesmente como: *Um determinado veículo irá retransmitir uma mensagem de emergência, se um de seus vizinhos tiver muitos vizinhos a menos do que o próprio veículo*. Um veículo vizinho, normalmente tem muito menos vizinhos se ele está sendo bloqueado, assim é incapaz de contactar-se com os veículos ao seu redor. Neste ponto, o fator importante que determina a eficácia da variante é decidir quando a diferença no número de vizinhos é suficientemente grande. A escolha da diferença é importante porque uma escolha errada poderá causar sobrecarga extra (LAOUITI; MUHLETHALER; TOOR, 2009).

3.3.3 R-OB-VAN Terceira Variação (2009)

A terceira variação é baseada na exigência de que os veículos trocam suas posições e suas listas com seus vizinhos por meio de *beacons*. A variante assume que os veículos estejam equipados com equipamentos de GPS. Esta é uma suposição razoável, já que muitos veículos novos possuem este equipamento. Assim, a terceira variante pode ser descrita como: *Um veículo irá retransmitir uma mensagem de emergência que recebeu corretamente de um nó transmissor que está lhe seguindo,*

se *nenhum de seus vizinhos tiver qualquer um dos transmissores da mensagem em sua vizinhança.* A variante não é ativada se o veículo recebe a mensagem de emergência de um nó localizado entre a fonte da mensagem de emergência e o nó receptor. Esta só é ativada se o transmissor está na direção da propagação. Isto é necessário porque num cenário correspondente a um rodovia linear, o veículo receptor irá geralmente ser coberto por dois transmissores; um em frente e um por trás (LAOUITI; MUHLETHALER; TOOR, 2009).

Os autores concluem que as abordagens propostas são eficazes em cenários com alta densidade, no qual o protocolo e suas variações tem alta taxa de entrega, porém pode sofrer com atrasos. Também concluíram que, em cenários como as rodovias, o total sombreamento de um nó é raro, porém, caso esta situação aconteça o protocolo proposto leva vantagem perante os protocolos de transmissão oportunística clássicos. Assim o protocolo torna-se eficiente em redes de conectividade intermitente (WEI; WANG; HSIEH, 2011).

3.4 ACKNOWLEDGED PARAMETERLESS BROADCAST IN STATIC TO HIGHLY MOBILE (ACKPBSM) (2010)

O protocolo PBSM (*Parameterless Broadcast in Static to Highly Mobile*), tem por objetivo controlar a quantidade de mensagens geradas na rede por meio da escolha de grupos com maior prioridade para retransmissão das mensagens, os CDS (*Connected Dominating Set*). Desta forma, o protocolo evita retransmissões mutuas e desnecessárias. As mensagens trocadas na rede não têm suas entregas confirmadas, deste modo a confiabilidade não é maximizada (KHAN; STOJMENOVIC; ZAGUIA, 2008).

Para prover confiabilidade na entrega das mensagens, o protocolo ackPBSM surge como uma extensão do protocolo PBSM. A principal novidade em relação ao PBSM, é a modificação do algoritmo para lidar com confirmações (ACK - *Acknowledged*) de mensagens difundidas. Tais confirmações são obtidas por meio de *beacons* periódicos. Por esse motivo, o protocolo é chamado de *Acknowledged* PBSM. Embora o PBSM seja definido com a obtenção de informação topológica num raio de até dois saltos, este também pode trabalhar com um raio de apenas um salto. A extensão do protocolo PBSM utiliza a última alternativa, segundo Nakorn e Rojviboonchai (2010), esta abordagem introduz menor sobrecarga aos *beacons*. Como PBSM, o ackPBSM implementa o paradigma *store-and-forward* para entregar a mensagem em redes al-

tamente particionadas. Assim, cada veículo armazena a mensagem de difusão em um *buffer* até que esta expire (NAKORN; ROJVIBOONCHAI, 2010).

Ao utilizar o protocolo ackPBSM os veículos emitem *beacons* periódicos, a fim de adquirir conhecimento sobre a topologia da rede local. Depois de cada troca, esta informação é utilizada para determinar se o próprio veículo faz ou não parte do CDS. Além disso, os *beacons* contêm os identificadores das mensagens que tenham sido recebidos recentemente. Esta troca de *beacons* periódicos pode gerar sobrecarga e problemas de congestionamento de transmissões em cenários com alta densidade de nós. O protocolo também constrói grupos de entrega CDS com as informações obtidas na troca de *beacons*, como no PBSM. No entanto, como os recebimentos das mensagens de difusão já foram confirmados, os novos vizinhos verificam que anteriormente receberam a mensagem, desta forma, tenta-se evitar novas retransmissões (ROS; RUIZ; STOJMENOVIC, 2009).

Um exemplo da operação do ackPBSM é apresentada na Figura 7, um veículo A gera uma mensagem de difusão que também é armazenada por A (no caso de novos vizinhos sem a mensagem serem encontrados no futuro) e, em seguida a mensagem é recebida por B, C e D. Assim, os veículos que receberam a mensagem configuram um tempo de espera, que é mais curto, caso o veiculo pertença ao CDS (grupo dominante pertencente à rede). Como D faz parte do grupo dominante, retransmite primeiro. B e C cancelam suas retransmissões, porque todos os seus vizinhos foram atendidos por D. Os veículos E e D recebem a mensagem. No entanto, nenhum destes nós descobriu novos vizinhos, de modo que a retransmissão não ocorre. Ao longo deste processo, os receptores confirmam a recepção da mensagem. No caso de qualquer veículo não receber a mensagem, os seus vizinhos detectarão a situação por causa da falta de confirmação e repetirão os passos anteriores, a fim de atendê-lo. Em situações que existem muitas mensagens em um mesmo ponto da rede, podem ocorrer retransmissões redundantes e colisões, isto deve-se ao algoritmo permitir que o nó pertencente ao grupo CDS tenha prioridade ao transmitir as mensagens, assim quando houver um grande número de mensagens na mesma área deste nó, este monopolizará as retransmissões (ROS; RUIZ; STOJMENOVIC, 2009).

Também pode-se supor que A acelera e ultrapassa os veículos B e F. Apesar de A e E não serem vizinhos anteriormente de F, não ocorre uma nova transmissão, porque através da troca de *beacons* sabe-se que nenhum dos veículos precisa da mensagem. Protocolos que não utilizam a confirmação de recebimento de mensagens, como o PBSM,

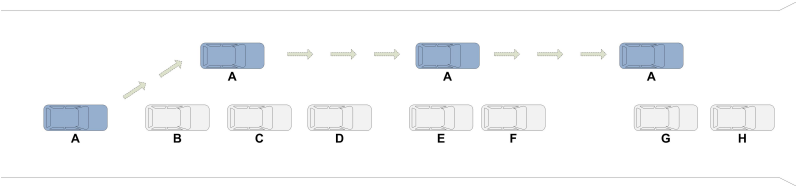

Figura 7: Funcionamento do protocolo AckPBSM.

neste caso, retransmitiriam de forma desnecessária a mensagem. Seguindo o exemplo, A aproxima-se de G, verifica que G não confirma o recebimento da mensagem e então A pode retransmitir a mensagem que havia armazenado. Como G tem conhecimento que o veículo H não recebeu a mensagem, G retransmite a mensagem, H à recebe e a rede é inteiramente coberta (ROS; RUIZ; STOJMENOVIC, 2009).

Seja X o veículo em questão. Para cada mensagem de difusão, os veículos criam duas listas: R e N. A lista R consiste nos vizinhos de X que deveriam ter recebido a mensagem (com base no conhecimento da topologia local de X). Já a lista N, contém os vizinhos restantes de X que estão no raio de cobertura de no máximo um salto. Existe uma função de tempo limite to_{ev} que atribui o tempo de espera para cada veículo antes de uma possível retransmissão. O valor retornado por to_{ev} pode ser proporcional a $1/|N|$, sendo $|N|$ o número de elementos em N, e depende do fato do nó estar atualmente nas CDS ou não (tempo de espera mais curto se o nó estiver em CDS) (ROS; RUIZ; STOJMENOVIC, 2009).

Segundo Ros, Ruiz e Stojmenovic (2009), o protocolo é capaz de alcançar alta confiabilidade, minimizando o número de retransmissões. Seu desempenho foi avaliado por meio de simulações, nas quais o ackPBSM superou seu antecessor numa variedade de cenários. Ainda sim, por utilizar *beacons* periódicos em cenários com maiores densidades apresentou atraso na entrega das mensagens e também pode gerar sobrecarga com a utilização das mensagens de confirmação. Um dos pontos fortes apresentados pelos autores, é a utilização dos grupos prioritários, desta forma a disputa do canal é minimizada e permite o protocolo não sofrer tanto com as colisões em cenários de alta densidade, tem-se que sem a utilização dos grupos prioritários o protocolo seria mais prejudicado pela utilização das mensagens periódicas.

3.5 POSITION-AWARE RELIABLE BROADCASTING PROTOCOL (POCA) (2010)

O protocolo POCA tem comportamento semelhante ao DECA, porém, utiliza GPS para obter o posicionamento dos nós vizinhos. Esse protocolo utiliza, a exemplo do DECA, *beacons* periódicos, que são utilizados para obter a posição e a velocidade dos seus vizinhos (NAKORN; ROJVIBOONCHAI, 2010).

Quando o nó desejar transmitir uma mensagem, este irá selecionar os vizinhos que estão posicionados em uma distância considerada ideal para retransmitir a mensagem. Esta distancia é obtida na troca de informações realizadas pelos nós. Cada nó sabe sua posição e velocidade por meio da utilização do GPS, assim o nó insere seus coordenadas atuais nos *beacons* que são trocados entre os vizinhos. Esta distância ideal é baseada na distância entre os nós receptores e os nós de seleção (NAKORN; ROJVIBOONCHAI, 2010).

O nó selecionado irá retransmitir a mensagem imediatamente, após o recebimento da mesma. No caso do nó selecionado não retransmitir a mensagem, outros nós que iniciaram a contagem do tempo limite de espera desde que receberam a mensagem, irão executar essa tarefa em seu lugar. O tempo limite de espera é calculado de acordo com a distância entre o nó e seu nó precursor. Assim, o nó que estiver mais próximo do nó selecionado irá retransmitir as mensagens. O POCA também insere o identificador da mensagem nos *beacons* para lidar com a conectividade intermitente. Os nós podem saber se os vizinhos perderam algumas mensagens e assim, retransmitir as mensagens aos seus vizinhos.

O protocolo POCA tem, segundo seus autores um desempenho aceitável em cenários de baixa e média densidade, porém em cenários com quantidades elevadas de veículos, de forma semelhante ao protocolo ackPBSM também sofre com a troca de *beacons* de forma contínua que acaba gerando sobrecarga e colisões em alguns cenários específicos (NAKORN; ROJVIBOONCHAI, 2010).

3.6 PREFERRED GROUP BROADCAST (PGB) (2010)

Segundo Nakorn e Rojviboonchai (2010), este protocolo visa reduzir as mensagens de controle, eliminando transmissões redundantes, e obter rotas estáveis com a capacidade de auto-correção. Além disso, tem como objetivo prover acesso a 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 (Interoperabilidade Mundial para Acesso de Micro-ondas do inglês *Worldwide Interoperability for Microwave Access*) 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 (NAUMOV; BAUMANN; GROSS, 2006).

O tempo de vida de um enlace é estimado pela área de alcance de rádio dos dois nós, a distância entre estes, 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 nós e 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 (NAUMOV; BAUMANN; GROSS, 2006).

Nakorn e Rojviboonchai (2010) acabam por definir que protocolo não é confiável, porém é uma solução para problemas de *broadcast storm*. Enquanto a minimização da carga no roteamento é muito desejável em qualquer cenário *ad hoc*, a estabilidade de uma rota escolhida torna-se especialmente importante em um ambiente no qual os nós que compõem a rede são veículos que se movimentam rapidamente (NAKORN; ROJVIBOONCHAI, 2010).

3.7 DENSITY-AWARE RELIABLE BROADCASTING PROTOCOL (DECA) (2011)

Veículos que trafegam em vias podem formar grupos, fazendo com que algumas faixas de rodagem tenham maior densidade do que outras faixas da mesma pista. Escolher um veículo que está na área de maior densidade para retransmitir uma mensagem pode maximizar o número de vizinhos que receberão a mensagem por meio de uma única transmissão. Portanto, o protocolo DECA usa informações referentes a densidade local para selecionar o nó que fará a retransmissão seguinte (KAMOLTHAM; NAKORN; ROJVIBOONCHAI, 2011).

O protocolo DECA faz uso do método *store-and-forward* e utiliza *beacons* periódicos. A utilização de *beacons* permite que os nós troquem informações sobre a densidade local e identificadores de mensagens já recebidas com apenas um salto na rede. Quando o nó fonte tem uma mensagem a transmitir, este irá selecionar o nó retransmissor em sua lista de vizinhos que foi construída com as informações obtidas na troca de *beacons*. O vizinho com a maior densidade a sua volta será selecionado. Então, o nó selecionado fará a difusão da mensagem, imediatamente, assim que recebê-la. Como resultado, o DECA pode divulgar dados muito rapidamente. Outros vizinhos, que não foram selecionados, irão armazenar a mensagem e definir um tempo limite de espera. No caso do nó selecionado não retransmitir a mensagem (devido a algum erro de colisão ou canal), outros nós vizinhos irão retransmitir a mensagem em seu lugar. Assim, quando os nós perceberem que algum nó já começou a retransmitir a mensagem, estes irão cancelar o tempo limite de espera (KAMOLTHAM; NAKORN; ROJVIBOONCHAI, 2011).

A Figura 8 ilustra exemplos de comportamentos do protocolo DECA. S quer transmitir uma mensagem. S conhece seus vizinhos A, B, C e D por meio da troca de mensagens de controle. D é o nó que tem a mais alta densidade local, de modo que S seleciona D para ser o nó retransmissor. Além disso, insere na mensagem a identificação de D. S transmite em *broadcast* a mensagem e, desta forma A, B, C e D recebem a mensagem, porém só D retransmitirá a mesma já que seu identificador está contido na mensagem recebida. O processo de retransmissão do nó D será o mesmo utilizado pelo no S, D selecionará um de seus vizinhos que tiver maior densidade e retransmitirá a mensagem com a identificação de seu vizinho escolhido para fazer a retransmissão e este processo irá ocorrer até que a mensagem expire (KAMOLTHAM; NAKORN; ROJVIBOONCHAI, 2011).

Os nós A, B, e C, que também receberam a mensagem, porém

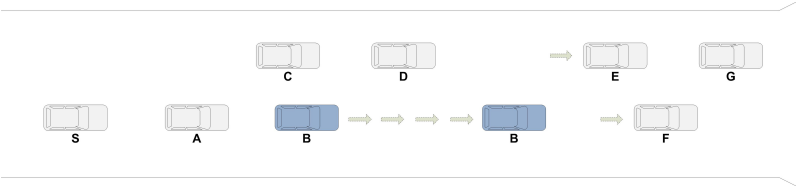

Figura 8: Cenário de conectividade intermitente.

não foram selecionados para retransmitir a mensagem, irão armazenar a mensagem em seus *buffers* e aguardarão um tempo limite aleatório de espera. Caso D não retransmita a mensagem, A, B ou C irá retransmitir a mensagem. Exemplificando, caso B tenha o menor tempo de espera, este retransmitirá a mensagem, esta mensagem terá o identificador do vizinho de B com maior densidade local, os nós A e C ao receberem a retransmissão de B, percebem que sua área de cobertura já foi atendida e cancelam seus tempos de espera (NAKORN; ROJVIBOONCHAI, 2010).

Segundo Nakorn e Rojviboonchai (2010), o nó que utiliza o protocolo DECA tem duas listas; lista de vizinhos e lista de Difusão.

- **Lista de vizinhos**: mantém os identificadores de todos os vizinhos que estão distantes um salto e sua densidade local. A lista é atualizada a cada vez que um *beacon* é recebido; e

- **Lista de difusão**: mantém os identificadores das mensagens transmitidas e seus tempos de espera. Uma mensagem transmitida será removida da lista em duas situações. A primeira é quando o tempo limite de espera expirar, desta maneira, o nó retransmite a mensagem e a retira da lista. A segunda é quando o nó ouve outros nós retransmitirem a mensagem. Desta forma, o número de retransmissões redundantes é minimizado.

Por *beaconing*, termo utilizado para definir a troca de informações por meio de *beacons*, um nó pode saber se os seus vizinhos perderam alguma mensagem ou se o próprio nó perdeu alguma mensagem. Quando o nó recebe um *beacon* de um vizinho, o nó atualiza a lista de vizinhos e verifica se aquele vizinho não tem alguma mensagem vigente na rede. No caso em que o nó verifica que seu vizinho perdeu uma mensagem, este insere o identificador da mensagem na lista de difusão e define um curto tempo limite de espera. Quando o tempo limite expirar, o nó irá retransmitir a mensagem e os outros nós que

ouvirem esta transmissão irão remover a mensagem de suas listas de difusão (NAKORN; ROJVIBOONCHAI, 2010).

No caso em que o nó percebe que ainda não tem a mensagem já transmitida, este irá enviar um *beacon* imediatamente para seus vizinhos, assim seus vizinhos podem retransmitir a mensagem faltante. A maior vantagem do DECA segundo Nakorn e Rojviboonchai (2010), é que não requer conhecimento de coordenadas geográficas para operar, o que torna mais flexível adequando-se a qualquer ambiente de operação.

De acordo com os estudos realizados por Nakorn e Rojviboonchai (2010), o protocolo DECA consegue alcançar seu objetivo que é prover confiabilidade e eficiência na transmissão de dados em redes de conectividade intermitente. O protocolo não faz uso de GPS, porém utiliza a técnica *store-and-forward* e emprega informações de densidade local para maximizar a entrega das mensagens. O protocolo não se comportar de forma adaptativa de acordo com a densidade de veículos no cenário, desta forma sobrecarrega a largura de banda utilizada na troca de informações. Os resultados apontados por Nakorn e Rojviboonchai (2010) mostram que o DECA pode superar outros protocolos. Mesmo nos casos extremos, tais como cenários com densidade muito baixa ou muito alta, o protocolo ainda opera com alta confiabilidade e a maior velocidade de disseminação de dados entre todos os protocolos avaliados pelos autores.

3.8 RELIABLE ROUTING SCHEME BASED ON VEHICLE MOVING SIMILARITY (RR-VMS) (2011)

O objetivo da proposta RR-VMS (WEI; WANG; HSIEH, 2011) é encontrar um caminho confiável para proporcionar um ambiente de transmissão de alta qualidade para roteamento em estradas e reduzir as mensagens de controle. O RR-VMS pode ser dividido em duas fases, a fase de manutenção de informações sobre vizinhos e a fase de descoberta de rota (WEI; WANG; HSIEH, 2011).

A fim de determinar os caminhos confiáveis, as informação sobre vizinhos que estão na área de transmissão do veículo devem ser mantidas. Assim, os veículos devem enviar periodicamente mensagens *HELLO* ou *beacons*. A mensagem *HELLO* foi originalmente concebida para determinar a conectividade da rede. Nós transmitem mensagens de saudação para os seus vizinhos a um salto de distância. Ou seja, o TTL (*time-to-live*) de uma mensagem *HELLO* é definido com o valor 1. Informações referentes aos vizinhos poderão ser registradas em uma

lista de vizinhos. A lista de vizinhos pode ser definida como a tupla <*ID*, tempo de expiração>, no qual *ID* é a identidade de um veículo próximo e tempo de expiração é o período de vigência do vizinho dentro da lista (WEI; WANG; HSIEH, 2011).

Quando um nó recebe uma mensagem *HELLO*, este atualiza ou adiciona as informações do remetente à lista de vizinhos e a tabela de roteamento. No RR-VMS, um novo campo *position* é adicionado à mensagem original *HELLO*, no qual *position* armazena as coordenadas (x,y) de um veículo. Escolher veículos com velocidades semelhantes como nós retransmissores para estabelecer um caminho de roteamento é uma questão importante para a confiabilidade do roteamento em VANETs. Na proposta RR-VMS, não é preciso gravar as velocidades dos vizinhos. Em vez disto, usa-se uma pontuação chamada de *Vehicle Persistence Score* (VPS) para escolher os nós que irão retransmitir. Além de manter uma lista vizinhos, cada veículo precisa manter uma tabela VPS. Tanto a tabela VPS quanto a lista vizinhos são atualizadas quando um veículo recebe uma mensagem *HELLO* de um veículo próximo (WEI; WANG; HSIEH, 2011).

O formato de cada entrada na tabela VPS é <*ID, position, distance, type, VPS*>.

- *ID*: identidade de um vizinho;
- *Position*: a coordenada do GPS (x,y), que representa a posição de um veículo. Nós utilizam esta informação para determinar a distância entre dois veículos;
- *Distance*: a distância entre dois veículos;
- *Type*: o tipo do vizinho; e
- *VPS*: o valor de modo a refletir a estabilidade de um veículo. Os nós utilizam este parâmetro para selecionar os nós de retransmissão.

Os nós calculam a distância entre um nó e um dos seus vizinhos de acordo com as informações fornecidas pelo GPS. O campo de distância é usada para classificar os vizinhos em dois tipos: os vizinhos de alta prioridade e vizinhos de baixa prioridade. Os autores definiram um limite de $1/3$ R para a classificação dos veículos vizinhos, sendo que R é o alcance de transmissão de um veículo. Como mostrado na Figura 9, o raio do círculo interior é $1/3$ de R e o raio do círculo exterior é R. Os veículos vizinhos localizados no interior do círculo exterior são

chamados de vizinhos de alta prioridade. Caso contrário, é um vizinho de baixa prioridade. Na Figura 9, os veículos A, B, E, F e G são vizinhos de alta prioridade da fonte, porque estes não estão localizados no interior do círculo interior, enquanto os veículos C e D são vizinhos de baixa prioridade. O objetivo da classificação é que os veículos vizinhos muito próximos do veículo fonte são menos úteis para a eficiência da rota, eles não cobrem um espaço maior que o coberto pelo nó fonte (WEI; WANG; HSIEH, 2011).

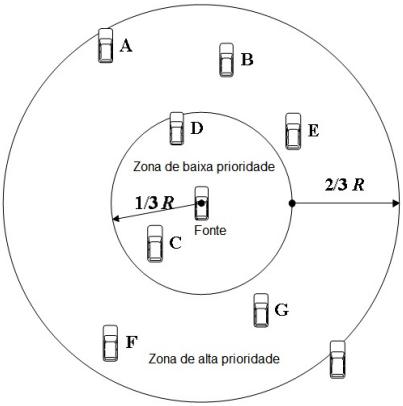

Figura 9: Vizinhos com maior e menor prioridade.

Pode-se descrever o processo para determinar o valor da pontuação VPS de um veículo da seguinte maneira: quando um veículo recebe uma mensagem *HELLO* de um vizinho pela primeira vez, este adiciona as informações relacionadas ao vizinho na lista de vizinhos e também na tabela VPS, e inicializa o VPS do vizinho com valor 1. Caso as informações do vizinho tenham sidas registradas antes, o veículo atualizada as informações do vizinho e incrementa o VPS do vizinho em 1. Para evitar que o valor de VPS cresça de forma ilimitada, define-se um valor máximo para o VPS, chamado *VPS Limit*. Quando o VPS atinge o valor limite, o VPS não será mais incrementado. A definição do limite para o VPS é dependente da aplicação. Uma aplicação que exige elevada confiabilidade pode ter um limite alto para o VPS e viceversa. Um exemplo de manutenção do VPS é mostrado na Figura 10 (a), quando a fonte recebe mensagens *HELLO* dos seus vizinhos, pela

primeira vez, e atualiza a tabela VPS. Nota-se que apenas o campo VPS na tabela VPS está ilustrado (WEI; WANG; HSIEH, 2011).

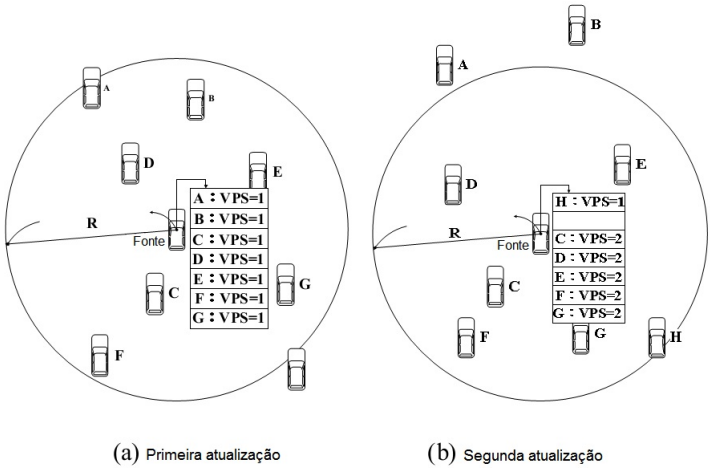

Figura 10: Vizinhos com maior e menor prioridade.

Na Figura 10 (a), a fonte recebe mensagens *HELLO* dos veículos A, B, C, D, E, F e G, de modo que o VPS destes veículos foram inicializados em 1. A Figura 2 (b) mostra os valores de VPS após a segunda atualização. Veículos C, D, E, F e G ainda permanecem na faixa de transmissão e suas mensagens *HELLO* foram recebidas pela fonte, assim que seus VPS foram incrementados em 2. As entradas para os veículos que não são mais vizinhos da fonte serão removidas a partir da tabela VPS, veículos, por exemplo A e B. Uma entrada de um novo veículo, por exemplo veículo H, pode ser adicionada à lista de vizinhos e os seu VPS é definido como 1, se a sua mensagem *HELLO* foi recebida pela fonte. Os veículos com valores de VPS mais elevados tendem a ficar na faixa de transmissão da fonte. Com a informação do valor do VPS, pode-se escolher o veículo mais estável para ser um nó retransmissor (WEI; WANG; HSIEH, 2011).

Para reduzir as mensagens de controle, o RR-VMS restringe o número de nós que podem retransmitir a mensagem. Os autores definem o parâmetro *REBROADCAST_NUMBER* para limitar o número de nós que poderão realizar a retransmissão. Por exemplo, quando um nó gera ou encaminha uma mensagem, apenas três vizinhos vão retransmitir este pedido se *REBROADCAST_NUMBER* for definido

com o valor 3. Para estabelecer os caminhos confiáveis de roteamento, o protocolo deve garantir a estabilidade dos nós que irão retransmitir a mensagem. Na fase de manutenção das informações dos vizinhos, o RR-VMS classifica os vizinhos com prioridade alta ou baixa. Ou seja, os vizinhos de alta prioridade têm maior chance de serem selecionados como nós retransmissores e vice-versa. Porém, a estabilidade dos vizinhos com alta prioridade precisa de ser assegurada. O RR-VMS escolhe os veículos com maior estabilidade a partir da lista de candidatos. Nota-se que quando a velocidade de um veículo próximo a fonte é semelhante à do veículo fonte, a ligação entre estes terá um longo tempo de validade. Em outras palavras, essa ligação é mais confiável. Quando um veículo tem um VPS mais alto, este terá uma maior probabilidade de ser selecionado como um nó de retransmissão (WEI; WANG; HSIEH, 2011).

Os resultados apresentados pelos os autores do protocolo mostraram que este pode aumentar a confiabilidade dos caminhos de roteamento e reduzir mensagens de controle, isto ocorre pois o protocolo utiliza valores para definir a estabilidade dos nós da rede, desta forma, só os nós mais estáveis irão formar a rota. A proposta RR-VMS também pode ser aplicada a outros protocolos de roteamento *ad hoc* voltados a inundação (WEI; WANG; HSIEH, 2011).

3.9 RELIABLE BROADCAST ROUTING BASED ON GAIN PREDICTION (RB-GP) (2012)

No modelo RB-GP, proposto por Chuan e Jian (2012), as informações de cada nó que integra a rede estão disponíveis por meio de trocas de *beacons* ou mensagens curtas feitas de forma periódica. Nestes *beacons* são inseridas informações como, ID (identificação do nó), posição (x, y; coordenadas do GPS), velocidade (a velocidade média relativa Δv_{ij}) e a direção (a direção da velocidade relativa ΔD_{ij} é definida por um ângulo de acordo com o eixo x). Cada nó estabelece a sua própria tabela de informações através da troca de informações entre os nós vizinhos. Estas informações são trocadas apenas entre vizinhos que estão a um salto de distância e não são encaminhadas para outros nós distantes (CHUAN; JIAN, 2012).

O principal objetivo do modelo RB-GP é o de maximizar o raio de cobertura em cada difusão e a diminuir os atrasos nas transmissões, isto é obtido através da seleção do próximo salto mais adequado em todas as direções. Em resumo, o modelo RB-GP tenta localizar o nó

vizinho com o maior ganho em todas as direções, esta busca pelo vizinho que proporciona o maior ganho é ilustrada na Figura 11.

O ganho é obtido através de:

$$G(i,j) = \alpha E(i,j) + (1-\alpha) I(i,j), \tag{3.4}$$

em que $\alpha \in [0,1]$, $E(i,j)$ é definido como o ganho direto e seu valor está contido no intervalo [0,1], já o ganho indireto é definido por $I(i,j) \in [0,1]$, deste modo, $G(i,j) \in [0,1]$.

O funcionamento do modelo RB-GP, ilustrado na Figura 11, é definido pelos seguintes passos:

- **Passo 1**: O nó A verifica se já recebeu a mensagem *p*. Se já, descarta *p*.
- **Passo 2**: O nó A verifica se é de fato o nó selecionado para retransmitir *p* através da análise do cabeçalho da mensagem. Se não, apenas armazena *p*; caso contrário A segue para o próximo passo.
- **Passo 3**: O nó A classifica seus vizinhos em três grupos de acordo com as informações contidas na tabela de vizinhos.
    1. Grupo dos nós localizados na mesma faixa de rodagem de A e que estão a frente de A, como o nó F (ver Figura 11).
    2. Grupo dos nós localizados na mesma faixa de rodagem de A e que estão a atrás de A, como o nó B (ver Figura 11).
    3. Grupo dos nós localizados em faixas de rodagens diferentes do nó A, como nós C, D e G.
- **Passo 4**: O nó calcula o valor de *G* (ganho) que cada nó vizinho proporciona usando a Equação 3.4 e, além disso, seleciona o nó com o maior ganho em cada grupo como o próximo salto, registra o ID de cada um dos vizinhos escolhidos no cabeçalho de *p*, e finalmente envia *p*.

O nó só inicia o mecanismo de *store-and-forward* quando não encontrar qualquer nó adequado no passo 3. O nó armazena *p* em um *buffer* temporariamente e depois continua o encaminhamento para outros nós apropriados dentro de seu alcance de comunicação em algum momento (CHUAN; JIAN, 2012).

Em cenários com baixa e média densidade, o protocolo garante que o nó selecionado pode receber os pacotes com sucesso, consegue

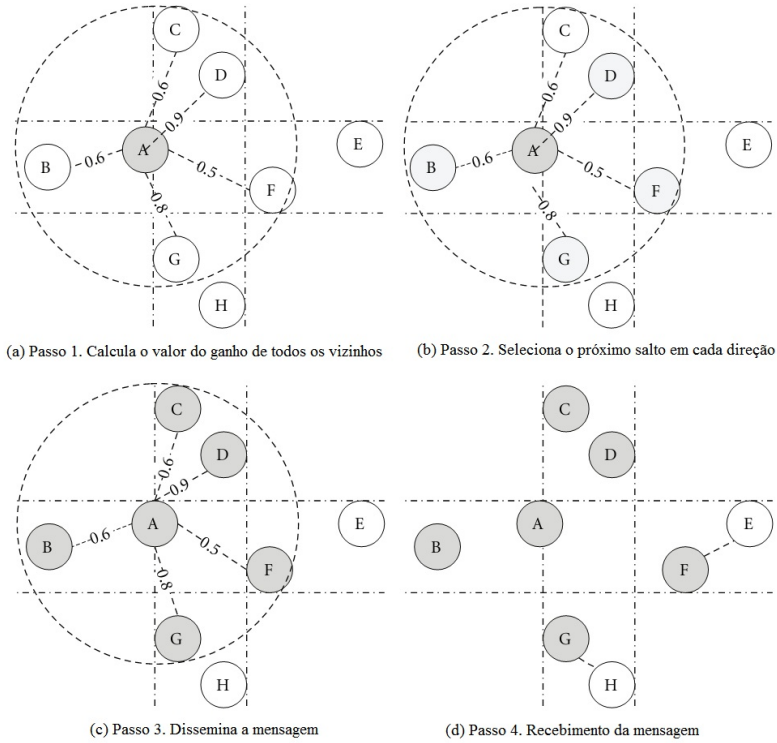

Figura 11: Funcionamento do modelo RB-GP.

assim, diminuir o conflito nos canais e informações retransmitidas de forma desnecessária. Os resultados mostram que o RB-GP é mais eficaz, no que diz respeito a taxa de entrega dos pacotes, e possui atraso médio menor, quando comparado a outros modelos que utilizam inundação, porém sofre com o excesso de *beacons* periódicos em cenários com alta densidade. Os autores deixam claro este problema e o definem como ponto chave a ser resolvido em trabalhos futuros, para que este protocolo possa ser usado em cenários urbanos, já que estes cenários são muito menos esparsos do que os cenários rodoviários (CHUAN; JIAN, 2012).

3.10 DISCUSSÃO DOS TRABALHOS RELACIONADOS

De acordo com o estudo dos protocolos voltados a prover confiabilidade nas transmissões de dados em redes veiculares descritos neste capítulo, foram levantados os seguintes aspectos para comparação entre estes protocolos: (1) a utilização de *beacons* e quais seus tipos; (2) a utilização de mecanismos voltadas a confirmação de entrega das mensagens; (3) como ocorre o armazenamento de informações por meio do uso de listas e históricos; (4) a utilização de informações sobre posição, velocidade e direção dos nós; (5) a forma de seleção do nó retransmissor; e (6) se existe tratamento explícito para o problema do nó oculto. Na Tabela 2, é apresentado um resumo comparativo dos trabalhos relacionados descritos.

Tabela 2: Comparativo - Trabalhos Relacionados

Protocolo	*Beacons*	Confir.	Lista Vizinhos	GPS	Sel. Retransmissor	Trat. Nó Oculto
EAEP	Não utiliza	Não	Não	Sim	Direção	Não
PGB	Aperiódico	Não	Sim	Sim	Direção	Sim
DECA	Periódicos	Não	Sim	Não	Densidade	Sim
ackPBSM	Periódicos	Sim	Sim	Sim	Prioridade	Sim
POCA	Periódicos	Não	Sim	Sim	Distância	Sim
RB-GP	Periódicos	Não	Sim	Sim	Distância e Densidade	Não
R-OB-VAN	Periódicos	Não	Sim	Sim	Densidade	Sim
RR-VMS	Periódicos	Não	Sim	Sim	Direção e Estabilidade	Não

Observa-se que apenas uma das abordagens não utiliza troca de informações por meio de *beacons* (EAEP), já que o protocolo insere as informações pertencentes ao nó diretamente na mensagem a ser propagada, desta forma, não utiliza mensagens de controle e não sofre com a sobrecarga existente em protocolos que utilizam estas mensagens de forma periódica, porém adicionam atraso a retransmissão das

mensagens, já que a mensagem de dados deve ser reconstruída a cada retransmissão. Os protocolos que sofrem com a sobrecarga presente na utilização de *beacons* periódicos são: DECA, ackPBSM, POCA, R-OB-VAN e RR-VMS, estes não obtiveram bons resultados em cenários com alta densidade de veículos, justamente por conta da quantidade de mensagens de controle geradas nestes casos. A solução para esta sobrecarga presente na utilização de *beacons* periódicos pode estar na implementação de mensagens de controle adaptativas que são transmitidas de forma aperiódica, desta forma, a quantidade de *beacons* gerados é reduzida em cenários com alta densidade de veículos e apenas o protocolo PGB implementa este mecanismo. *Beacons* adaptativos evitam *overhead* em cenários com alta densidade, desta forma o canal ficará mais tempo livre para a transmissão das mensagens de dados.

De todos os protocolos estudados, apenas a abordagem ackPBSM utiliza *ack*s para confirmar o recebimento de um mensagem transmitida na rede, desta forma o protocolo tenta mitigar o problema do terminal oculto de forma explícita e também aumenta a confiabilidade nas retransmissões geradas, porém este mecanismos não se mostra eficiente em cenários esparsos, nos quais a distancia entre os veículos é grande. Apenas o protocolo EAEP, não faz uso de listas ou históricos de vizinhança, isto acontece, pois a abordagem utiliza a distância entre o nó transmissor e o nó receptor para definir o tempo de espera, no qual é utilizado para realizar a retransmissão. Esta abordagem é um protocolo epidêmico, sendo assim, o nó envia a mensagem a todos os nós em seu raio de cobertura sem precisar ter conhecimento prévio da topologia da rede, esta postura ocasiona retransmissões desnecessárias e um aumento na quantidade de mensagens geradas na rede.

Sete protocolos estudados fazem uso de informações de posição, velocidade e distância dos nós presentes na rede, sendo que estas informações são obtidas pelo uso de GPS. Apenas o protocolo DECA não utiliza estas informações, pois este apenas utiliza a densidade local dos nós para selecionar o nó retransmissor. Já os outros protocolos, precisam destas informações, pois utilizam as mesmas para definir quais serão os nós retransmissores da mensagem. Para selecionar o nó retransmissor, os protocolos estudados utilizam métodos diferentes, o primeiro método encontrado é a utilização da direção em que o nó está seguindo, os protocolos EAEP, PGB e RR-VMS fazem uso deste método, porém, com implementações diferentes. No caso do protocolo EAEP, cada vez que o nó recebe mensagens de nós à sua frente ou de nós seguidores, são incrementados contadores para definir a direção de propagação, já no caso do protocolo PGB, o mesmo utiliza a direção pra definir ro-

tas de encaminhamento das mensagens. Por fim, o protocolo RR-VMS utiliza a direção com uma das variáveis para definir a estabilidade de um determinado nó, desta forma, o nó mais estável será escolhido para retransmitir a mensagem. O segundo método para determinar o retransmissor é a densidade local de um nó, o protocolo DECA utiliza esta premissa para determinar o nó com maior densidade local, assim, o nó terá maior chance de retransmitir a mensagem ao maior número de nós vizinhos. A seleção do retransmissor por meio da densidade local mostrou-se simples e eficiente perante as outras abordagens.

O protocolo ackPBSM utiliza a prioridade para selecionar o nó retransmissor, o nó que faz parte do grupo prioritário, como por exemplo, ambulâncias, viaturas, veículos de monitoramento da via, etc, retransmiti primeiro, por meio da utilização de um tempo de espera menor que dos outros nós que não fazem parte do grupo prioritário. O último método utilizado para definir o nó retransmissor é a distância entre os nós, o protocolo POCA utiliza este método, só os nós que estão dentro de uma distância ideal do nó transmissor poderão retransmitir a mensagem, já o protocolo RB-GP utiliza a distância para calcular um ganho, o nó que prover maior ganho em determinada direção será o retransmissor da mensagem.

O último aspecto verificado na comparação dos protocolos é o tratamento explícito do problema chamado nó oculto. Todos os trabalhos estudados empregarem a técnica *store-and-forward*, que consiste em armazenar a mensagem recebida e, posteriormente, retransmiti-la. Esta técnica permite minimizar o problema de conectividade intermitente. Porém, em cinco trabalhos os autores buscaram mitigar este problema em suas abordagens utilizando outras técnicas além da *store-and-forward*, os protocolos são: PGB, DECA, ackPBSM, POCA e R-OB-VAN. Em todas estas abordagens o problema do nó oculto não é tratado com estruturas ao longo das vias, nós fixos, apenas são utilizadas mensagens de confirmação e a técnica *store-and-forward*, ambas as técnicas não resolvem o problema do nó oculto em cenários com baixas densidades, sendo necessário buscar outras maneiras de tratar o problema, como por exemplo, a inserção de nós fixos ao longo das vias.

3.11 CONSIDERAÇÕES DO CAPÍTULO

Ao analisar os protocolos estudados neste Capítulo, pode-se verificar que algumas características são importantes e necessárias para que um protocolo possa prover confiabilidade ao transmitir uma men-

sagens em uma rede móvel. Estas características devem ser levadas em consideração no desenvolvimento de novos mecanismos que buscam prover confiabilidade em um meio não confiável, como por exemplo, as redes veiculares.

Sendo assim, compreender os protocolos confiáveis existentes, bem como avalia-los e compará-los é um passo importante para a construção de novos modelos. Este Capítulo apresentou os trabalhos encontrados a partir de uma revisão sistemática da literatura e referenciados por diversos autores que procuram prover confiabilidade na disseminação de dados em redes *ad hoc* móveis. Os trabalhos descritos serviram de embasamento para o desenvolvimento do protocolo proposto descrito no próximo capítulo.

4 PROTOCOLO DE DIFUSÃO PROPOSTO

Conforme Dotzer, Fischer e Magiera (2005), o uso das redes veiculares visa aumentar a segurança do tráfego e melhorar consideravelmente a mobilidade entre os veículos, sendo um dos principais desafios a transmissão de mensagens entre os nós de forma que a entrega destas mensagens seja confiável. O objetivo geral deste trabalho foi desenvolver um protocolo que provê confiabilidade na disseminação de informação de aplicações voltadas a segurança no trânsito em rodovias.

No capítulo anterior foram apresentados métodos e soluções para prover confiabilidade em protocolos voltados a difusão de informações em redes *ad hoc* veiculares. Nesses métodos, aspectos importantes relacionados a mobilidade e comunicação, tais como variações bruscas na densidade de veículos, troca de *beacons* sem controle, queda momentânea de enlaces, problema do nó oculto, comumente encontrados na redes veiculares, são negligenciados.

Para preencher essas lacunas deixadas por essas soluções, propõe-se um protocolo que utilize comunicação em VANETs para coletar informações dos veículos que estejam trafegando sobre as pistas de vias. Além disso, prover confiabilidade à disseminação de dados pela rede veicular, de forma, mitigar o problema do terminal oculto e diminuir a quantidade de mensagens de controle desnecessárias que são trocadas entre os nós móveis. Este protocolo preenche a lacuna deixada pelas atuais propostas de difusão confiável em VANETs, pois se adapta ao ambiente de comunicação encontrado em cenários de tráfego rodoviário.

Este capítulo descreve o protocolo proposto e está organizado da seguinte forma. A Seção 4.1 apresenta a visão geral e as premissas para a especificação do protocolo. Em seguida, a Seção 4.2, apresenta a descrição do módulo de seleção do retransmissor e o mecanismo de seleção adotado nesta dissertação, na Seção 4.3 é apresentado o módulo de comunicação, bem como os tipos de mensagens disseminadas na rede, os algoritmos e mecanismos utilizados nesse módulo. Na Seção 4.4, o módulo de determinação de vizinhança é descrito juntamente com seus mecanismos. E, por fim, são tecidas as considerações finais do capítulo.

4.1 VISÃO GERAL E PREMISSAS

Os elementos fundamentais de uma rede *ad hoc* veicular são seus nós e nesta proposta assume-se que existem dois tipos de nós, os fixos e

os móveis. Nesta dissertação, o termo nó diz respeito a qualquer dispositivo de comunicação conectado a rede *ad hoc* veicular. Considera-se como premissas que cada veículo (nó) tem sua identidade definida de forma única na rede baseada no endereço MAC do módulo de rede do nó. Os veículos participantes da rede possuem componentes que possibilitam a comunicação e a execução dos aplicativos tais como; sensores, unidades de armazenamento, unidade de comunicação sem fio, sistema de posicionamento (GPS) e uma interface com o usuário para mostrar ao condutor os alertas e a localização dos eventos relatados.

Considera-se ainda que, os eventos podem ser sempre detectados pelos sensores presentes nos veículos e que o GPS proporciona uma precisão suficiente para detectar em qual local da rodovia encontra-se o veículo e em qual momento exato houve sinalização. O funcionamento dos sensores e a tecnologia empregada estão fora do escopo deste trabalho. O protocolo proposto foi implementado para uma aplicação desenvolvida durante este trabalho e esta aplicação serve como base para que as funcionalidades do protocolo desenvolvido possam ser avaliadas.

O protocolo proposto é composto de três módulos: Módulo de Seleção do Retransmissor, Módulo de Comunicação e Módulo de Determinação de Vizinhança. A Figura 12 apresenta os módulos e mecanismos que compõem a arquitetura do protocolo proposto.

O Módulo de Seleção é responsável por determinar o nó que terá o papel de retransmitir a mensagem de dados a cada salto. O Módulo de Comunicação define os tipos de mensagens existentes no protocolo, bem como a estrutura da lista de mensagens utilizada na abordagem. Neste módulo também são definidos os mecanismos de adaptação de período entre mensagens de controle e codificação de rede. Por fim, o Módulo de Determinação de Vizinhança define a estrutura da lista de vizinhos e é responsável pelos mecanismos de adaptação dos tempos de espera e detecção de conectividade.

No modelo de organização hierárquica, os nós móveis, ou seja, os veículos que trafegam sobre cada pista, trocam informações entre si, geram alertas, transmitem e retransmitem os alertas presentes na rede. Já os nós fixos, atuam como pontos de coleta para os dados enviados pelos veículos e têm como principal papel armazenar e retransmitir mensagens de dados quando solicitado. Desta forma, estes permitem que os nós verifiquem se receberam ou não a última mensagem vigente na rede. O protocolo de forma a minimizar o impacto que a difusão tem sobre a comunicação, faz uso de mecanismos que diminuem a quantidade de mensagens desnecessárias na rede. Também faz uso de mensagens de controle com períodos entre retransmissões que se adaptam de acordo

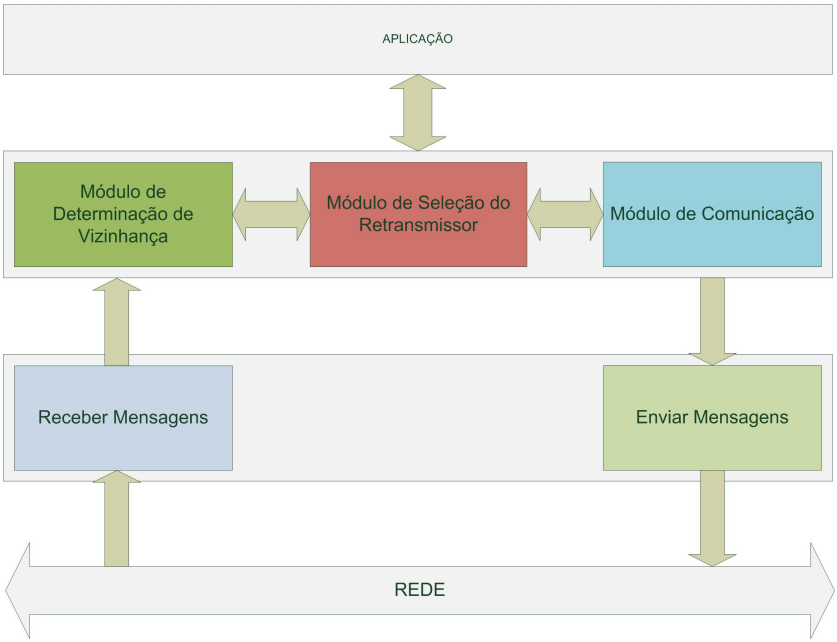

Figura 12: Arquitetura do Protocolo Proposto.

com a densidade de veículos na via, diminuindo assim a quantidade de mensagens de controle em situações de congestionamento. Estas mensagens de controle permitem que os nós verifiquem se seus vizinhos já receberam um alerta vigente na rede, com o objetivo de mitigar o problema do nó oculto.

Para diminuir a quantidade de mensagens na rede, o nó móvel tem a sua disposição uma lista de vizinhos e de mensagens de dados (alertas) já recebidos. Uma vez que um nó reconheça seus vizinhos, esse deve determinar qual dos seus vizinhos vai retransmitir o alerta que o transmissor deve difundir. Esta escolha se dá por meio da troca de *beacons*. Nestes *beacons* estão contidas a identificação, a densidade local, a velocidade no instante e outras informações pertinentes do nó vizinho. De acordo com as informações do nó vizinho, o nó transmissor calcula o ganho W referente ao seu vizinho, assim o nó que prover maior ganho será escolhido para retransmitir a mensagem de dados.

Os nós, ao receberem o alerta, devem verificar se são, ou não, o nó retransmissor. Caso o nó seja o retransmissor, este irá retransmitir

a mensagem aos seus vizinhos. Segundo Paula, Oliveira e Nogueira (2010), existem casos nos quais a disseminação direcionada pode trazer maiores benefícios para aplicações voltadas à segurança no trânsito, desta forma, o protocolo proposto também permite que a disseminação de uma mensagem seja tanto, omnidirecional, quanto direcional. Para diminuir a quantidade de mensagens de dados retransmitidas pela rede, o protocolo proposto implementa a operação lógica XOR. Em cenários com mais de uma mensagem de dados na rede, o protocolo realiza a operação XOR entre as mensagens existentes e faz uso de apenas uma retransmissão, ao invés de uma retransmissão para cada mensagem da rede. Todos estes processos e mecanismos serão detalhados no decorrer deste capítulo.

4.2 MÓDULO DE SELEÇÃO DO RETRANSMISSOR

Este módulo é responsável por determinar qual será o nó retransmissor da mensagem disseminada na rede. A seleção é realizada por meio de um mecanismo de seleção que consiste no calculo do ganho de cada nó W_j.

4.2.1 Mecanismo de Seleção

A troca de mensagens de controle permite que os nós compartilhem informações sobre a vizinhança dentro de um salto de distância e também os identificadores de mensagens já recebidas. Quando o nó i tem um alerta para transmitir, este irá selecionar o vizinho com a maior ganho W_j. O nó j selecionado fará a retransmissão do alerta imediatamente, assim que realizar os processos de verificação do alerta. Outros nós vizinhos, que não foram selecionados, irão receber e armazenar a mensagem e definir um tempo limite de espera com o objetivo de retransmitir o alerta caso o nó retransmissor não o faça. Este tempo aleatório é definido a partir do intervalo $[TeCM_{max}, Te_{max}]$ com

$$Te_{max} = TeCM_{max} + \frac{C}{Tp_k} + Random[0, 0.002] \tag{4.1}$$

em que Tp_k é o parâmetro usado para indicar o tipo da mensagem, com isso pode-se definir a urgência da mensagem. A constante $TeCM_{max}$ é definida por meio de estudos feitos do cenário.

A componente $Random[0, 0.002]$ tem papel de gerar um *offset*

com valor entre 0 e 2 ms no tempo de espera. C é parâmetro de configuração do protocolo e influencia na fórmula. Quando os nós detectarem que algum nó já começou a retransmitir a mensagem, estes cancelarão o tempo limite de espera (contagem regressiva).

A seleção do nó retransmissor ocorre quando um nó deseja transmitir ou retransmitir uma mensagem de dados na rede. Assim que um nó transmissor reconhece seu vizinhos, este calcula o peso W_j de cada vizinho pertencente em sua lista que contém as informações dos vizinhos a um salto de comunicação. Este peso W_j é utilizado para determinar qual a qualificação que cada nó tem para ocupar a função de retransmissor da mensagem. Assume o estado de retransmissor, o nó que possui o maior ganho. O nó i no estado transmissor calcula o ganho de cada vizinho, de acordo com:

$$W_j = w.\frac{B_j}{Th_B} + (w-1).\frac{D_j}{Th_D} \tag{4.2}$$

em que a componente B_j indica a distância de um veículo j em relação ao veículo transmissor i. O protocolo prioriza os nós mais próximos das bordas do raio de comunicação. A componente D_j indica a densidade local de cada nó. Tem-se que, quanto maior a densidade local de um nó, maior é a chance de que este nó difunda a mensagem ao maior número de nós da rede. As componentes Th_B e Th_D determinam o limiar para cada uma das componentes B_j e D_j, respectivamente.

A constante w determina a influência de cada uma das componentes no cálculo do peso W_j, de modo que, é possível priorizar um fator em relação ao outro. Em cenários com grande densidade, por exemplo, é interessante priorizar a distância entre o transmissor e o retransmissor, assim a mensagem atinge as bordas do raio de comunicação e é difundida o mais distante possível.

Para calcular a distância B_j de um nó j em relação ao nó i, utiliza-se a equação da distância euclidiana bidimensional, que leva em consideração as coordenadas x e y de cada veículo, conforme:

$$B_j = \sqrt{(x_i - x_j)^2 - (y_i - y_j)^2} \tag{4.3}$$

na qual, x_i e y_i representam as coordenadas do veiculo i, e as componentes x_j e y_j representam as coordenadas do veiculo j.

De posse da função B_j, cada veículo calcula sua distância em relação a cada vizinho presente em sua lista, sendo que, quanto maior valor de B_j, mais próximo à borda do círculo de comunicação o veículo está. Portanto, melhor será sua difusão da mensagem de dados aos

demais nós da rede. Para B_j, define-se um limiar referente à distância, neste caso, este limiar é definido pelo raio de cobertura do nó i.

A componente D_j da Equação 4.2 determina a densidade local do nó j. Quanto maior a densidade, maior será seu valor. Para o valor D_j, também é definido um limiar. Por meio do estudo do cenário a ser utilizado, pode-se definir o valor máximo de veículos ao redor de i que irão realmente auxiliar na retransmissão da mensagem.

Este protocolo também apresenta a possibilidade de retransmitir a mensagem em uma única direção. Segundo Paula, Oliveira e Nogueira (2010), em cenários rodoviários, muitas vezes ocorrem acidentes e o mais certo a se fazer é informar os nós que vem em direção ao acidente, no caso, deve-se direcionar a retransmissão da mensagem, assim atendendo todos os nós que vão de encontro ao acidente. Para realizar esta função, a Equação 4.2 sofre a seguinte mudança:

$$W_j = (w.\frac{B_j}{Th_B} + (w-1).\frac{D_j}{Th_D}).Dr_j \tag{4.4}$$

sendo que Dr_j define o sentido de direção do nó j e pode ter o valor +1 ou -1. Para definir o senso de direção, primeiro é obtido o sentido do veículo j em relação ao veículo i. St_j é definida por,

$$St_j = dA_{(i,j)} - dI_{(i,j)} \tag{4.5}$$

que é formada pela subtração das componentes $dA_{(i,j)}$ e $dI_{(i,j)}$. A primeira componente $dA_{(i,j)}$ determina a distância anterior ao envio da mensagem de controle por parte do nó j e é representada pela Equação 4.6.

$$dA_{(i,j)} = \sqrt{(x_i - xA_j)^2 - (y_i - yA_j)^2} \tag{4.6}$$

Já a segunda componente determina a distância de i e j no instante do envio da mensagem de controle, sendo dada por:

$$dI_{(i,j)} = \sqrt{(x_i - xI_j)^2 - (y_i - yI_j)^2} \tag{4.7}$$

Desta forma St_j poderá assumir um valor positivo ou negativo. Assim, pode-se definir a direção que j tem em relação ao nó i. Valores negativos determinam que o nó j está se distanciando do nó i, já valores positivos determinam que o nó j está se aproximando do nó transmissor i. As componentes xI e yI representam a posição do nó no instante t^k, no qual foi realizado o envio da mensagem de controle, já as componentes xA e yA representam a posição do nó no instante

$t^k - 1$, que é o instante anterior ao envio da mensagem de controle.

Ao descobrir qual é o sentido do nó j, pode-se definir Dr_j por meio do Algoritmo 1. No Algoritmo 1, pode-se perceber as componentes pI_j e pI_i que representam a posição dos nós i e j no instante t^k e a componente St_j que é calculada através da Equação 4.5. A Figura 13 exemplifica a definição de $Dr_j = +1$, ou seja, apenas os veículos que trafegam na via contrária ao acidente irão obter W positivo.

Algorithm 1: Obtenção do valor de Dr_j

```
1 inicio
2     pI_j ← Recupera posição no instante t^k do nó j;
3     pI_i ← Recupera posição no instante t^k do nó i;
4     St_j ← Recupera o sentido de direção do nó j;
5     se ((pI_j > pI_i) e (St_j < 0)) ou ((pI_j < pI_i) e (St_j ≥ 0)) então
6         retorna Dr_j = +1;
7     senão
8         retorna Dr_j = -1;
```

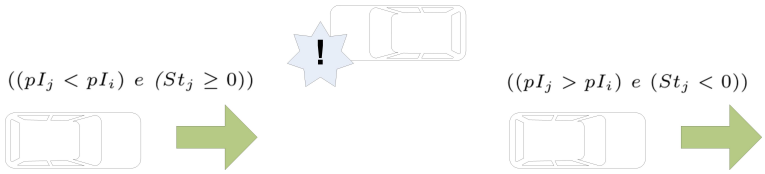

Figura 13: Situações nas quais Dr_j retorna valor positivo.

Após obter o valor de W_j, o nó com maior peso W será selecionado para ser o retransmissor. Este processo se repete, sempre que for necessário transmitir ou retransmitir uma mensagem de dado na rede.

4.3 MÓDULO DE COMUNICAÇÃO

Para permitir que dois nós se comuniquem, assume-se que cada um deles tem capacidade de comunicação e processamento embarcado. A comunicação entre os nós da rede veicular ocorre por difusão de mensagens. Dois nós que estejam dentro do raio de comunicação um do outro podem se comunicar diretamente, ou seja, receber e enviar mensagens um ao outro.

O raio de comunicação de um nó i é denominado r_i e define uma área de cobertura de comunicação descrita por um círculo, no

qual i encontra-se no centro e todos os nós que estejam dentro deste círculo são denominados vizinhos ou membros da vizinhança do nó i. Os vizinhos dentro do raio de comunicação de um nó são ditos vizinhos a um salto de comunicação deste nó; e aqueles que estão dentro $2r_i$ são denominados vizinhos a dois saltos e assim sucessivamente. Neste trabalho são utilizadas apenas as informações dos vizinhos a um salto de distância, com o objetivo de diminuir a quantidade de mensagens de controle utilizadas para obtenção de informações sobre a vizinhança.

Conforme mencionado, assume-se que cada nó está equipado com um dispositivo de localização (GPS). Este dispositivo provê ao nó i um relógio local, no qual, um instante de tempo t^k é um elemento de T e t_i^k indica o instante em que a *k-ésima* mensagem foi gerada pelo nó i.

As mensagens do protocolo são difundidas utilizando canais de comunicação não confiáveis, ou seja, uma mensagem difundida por um nó pode não ser recebida por algum dos seus vizinhos. Diante disto são utilizadas as mensagens de controle *CM*, para que os nós que não receberam certa mensagem possam avisar seus vizinhos do não recebimento da mensagem. Porém, assume-se que uma mensagem quando recebida, sempre é correta. Os tipos de mensagens e premissas adotadas em sua difusão são apresentados nas próximas seções.

4.3.1 Envio e Recepção de Mensagens de Controle e de Dados

O módulo de comunicação é responsável pela difusão e recepção de dois tipos distintos de mensagens: mensagens de controle (*beacons*) e mensagens de dados que representam os alertas. Cada nó difunde mensagens de controle de forma aperiódica, através da função *Enviar()*. O tipo de mensagem de controle a ser enviada depende do recebimento de outras mensagens de controle ou da necessidade de enviar uma mensagem de alerta. Toda mensagem de controle é composta por uma tupla de dados e contém informações do nó que a está difundindo e/ou sobre sua vizinhança. Esta mensagem é utilizada pelos nós para determinar suas próprias ações, por exemplo, definir o nó responsável pela retransmissão de uma mensagem a ser difundida. Os alertas são difundidos pelo nó que tem a necessidade de gerar um alerta e esta mensagem é retransmitida somente pelo nó escolhido pelo transmissor.

A função *Receber(m)* permanece continuamente recebendo as mensagens difundidas pelos vizinhos de um nó. Assim que uma mensagem é recebida, esta é encaminhada para o módulo de determinação da vizinhança ou para o módulo de comunicação.

As mensagens de controle são encaminhadas e tratadas no módulo de determinação de vizinhança, no qual, os dados de cada vizinho são armazenados em uma lista de vizinhos. No entanto, as mensagens de dados são encaminhadas para o módulo de comunicação que decide se irá tratá-la, retransmiti-la ou descartá-la.

As mensagens de controle são utilizadas pelos nós fixos e móveis para reconhecerem suas respectivas vizinhanças e eventualmente excluir uma mensagem de dados da rede. Estes *beacons* são muito menores comparados as mensagens de dados (alertas). Os nós móveis usam esta vizinhança para determinar quais são os nós mais aptos para retransmitir um alerta.

Neste protocolo são utilizadas três mensagens de controle, *CM*, *RQ* e *MR*. A mensagem de controle *CM* encapsula informações do nó e permite que sejam criadas listas de vizinhos, a mensagem *CM* é trocada de forma aperiódica e, de acordo com a densidade da rede, as trocas de *CM*s acontecem em menor quantidade quando a lista de vizinho não é atualizada com frequência, assim evitando mensagens de controle desnecessárias. Uma mensagem de controle *CM* é composta pelos campos presentes na Tabela 3.

Tabela 3: Mensagem de Controle *CM*

Campo	**Descrição**
Em_i	Endereço MAC do nó
D_i	Densidade local do nó
pA_i	Posição anterior ao instante t^k do nó i
pI_i	Posição no instante t^k do nó i
V_i	Velocidade do nó i no instante t^k
Id_k	Identificador único da última mensagem recebida pelo nó
Tp_k	Tipo da mensagem (CM)

Na Tabela 3, o campo Em_i é utilizado na lista de vizinhos e representa a identificação única do nó. O campo D_i armazena o total de nós que estão a um salto de distância do nó i, pA_i a posição anterior ao instante t^k do nó i, pI_i armazena a posição no instante t^k do nó i, já o campo V_i contém a velocidade instantânea do nó i. Por fim, o campo Id_k tem o papel de informar aos nós receptores a última mensagem recebida pelo nó i, assim o nó receptor poderá verificar se o nó i deixou de receber algum alerta, ao verificar esta situação o nó (receptor) j

difunde o alerta, assim o nó i é atendido.

No Algoritmo 2 são apresentados os passos para que a mensagem CM seja gerada. Caso o período α_i expire e o tamanho da lista de vizinhos N_i seja menor que ThD, a mensagens CM será enviada. O processo de recebimento da mensagem de controle CM será explicado em detalhes no Algoritmo 8.

Algorithm 2: Envio CM

```
1  inicio
2      α_i ← Período definido de acordo com a densidade local de i;
3      se ((α_i = 0) e (sizeof(N_i) < ThD)) então
4          Em_i ← Endereço MAC do nó;
5          D_j ← Densidade local do nó;
6          pA_i ← Posição anterior ao instante t^k do nó j;
7          pI_i ← Posição no instante t^k do nó j;
8          V_i ← Velocidade do nó i no instante t^k;
9          Id_k ← Identificador único da última mensagem recebida pelo nó;
10         Tp_k ← Tipo da mensagem (CM)
11         CM ← GeraCM(Em_i, D_i, Tp_k, pA_i, pI_i, V_i, Id_k);
12         Enviar(CM);
```

A mensagem de controle RQ é utilizada para forçar a troca de informações entre os nós próximos a um nó que pretende difundir um alerta na rodovia pela primeira vez. O nó i ao perceber que deve enviar um alerta, gera a mensagem de controle RQ e a difunde na rede. Ao receber essa mensagem, o nó j é forçado a difundir a mensagem de controle CM, desta forma, o nó i recebe novas informações sobre sua vizinhança e pode definir o nó que será o retransmissor do alerta em um segundo momento. Os campos presentes na mensagem de controle RQ são apresentados na Tabela 4 e o Algoritmo 3 mostra os passos para que a mensagem RQ seja gerada. Já o Algoritmo 4 mostra o processo executado por um nó que recebe uma mensagem de controle RQ.

Algorithm 3: Envio RQ

```
1  inicio
2      /* Sensor do veículo detectou evento e alerta foi gerado */
3      se (Existe alerta a ser enviado) então
4          Em_i ← Endereço MAC do nó;
5          Tp_k ← Tipo da mensagem RQ;
6          RQ ← GeraRQ(Em_i, Tp);
7          Enviar(RQ);
```

A mensagem de controle MR é utilizada para sinalizar os nós de que um alerta difundido teve seu tempo de vida expirado. O nó

Algorithm 4: Recebimento RQ

```
1  inicio
2      Tarefa: T1 /* Recepção RQ */
3      ao receber mensagem de controle RQ
4      se (i recebeu RQ) então
5          Em_i ← Endereço MAC do nó;
6          D_j ← Densidade local do nó;
7          pA_i ← Posição anterior ao instante t^k do nó j;
8          pI_i ← Posição no instante t^k do nó j;
9          V_i ← Velocidade do nó i no instante t^k;
10         Id_k ← Identificador único da última mensagem recebida pelo nó;
11         Tp_k ← Tipo da mensagem (CM)
12         CM ← GeraCM(Em_i, D_i, Tp_k, pA_i, pI_i, V_i, Id_k);
13         Enviar(CM);
```

Tabela 4: Mensagem de Controle RQ

Campo	**Descrição**
Em_i	Endereço MAC do nó i
Tp_k	Tipo da mensagem (RQ)

transmissor, ao perceber que o tempo de vida do alerta k expirou, difunde essa mensagem pela rede para que os nós presentes na rede retirem de circulação o alerta k. Os nós, ao receberem essa sinalização, prontamente retiram o alerta k da lista de alertas, assim evitando que a mesma seja difundida novamente. A mensagem MR é composta pela tupla: $< Id_k, t_i^k, Tp_k >$ conforme a Tabela 5, o campo Id_k armazena o identificador único do alerta a ser revogado, já o campo t_i^k armazena o *timestamp* referente ao momento que a mensagem foi revogada. No Algoritmo 5 são apresentados os passos realizados para que a mensagem MR seja gerada.

Tabela 5: Mensagem de Controle MR

Campo	**Descrição**
Id_k	Identificador único do alerta k
t_i^k	*Timestamp*
Tp_k	Tipo da mensagem (MR)

Algorithm 5: Envio MR

```
1  inicio
2      MA_l ← Conjunto de mensagens de alertas recebidos pelo nó l;
3      l ← Nó responsável por gerar mensagens MR;
4      para cada Alerta ∈ MA_l hacer
5          Status.Evento ← verifica(Alerta);
6          /* l verifica se o evento ainda é verdadeiro */
7          se (Status.Evento = falso) então
8              Id_k ← Alerta.Id_k;
9              t_i^k ← Alerta.t_i^k;
10             MR ← GeraMR(Id_k, t_i^k, Tp);
11             Enviar(MR);
```

A mensagem de dados existente neste protocolo é chamada de alerta e é utilizada para sinalizar problemas presentes na rodovia, como acidentes, congestionamentos, etc. Esta mensagem é composta pela tupla representada na Tabela 6.

Tabela 6: Mensagem de Dados - Alerta

Campo	**Descrição**
Id_k	Identificador único do alerta
Em_i	Endereço MAC do nó
Tp_k	Tipo do alerta
Ds_k	Descrição
x_i, y_i	Coordenadas
Tv_k	Tempo de vida na rede da mensagem k
t_i^k	*Timestamp*
Tag	Armazena 0 ou 1, 1 determina que a mensagem é um XOR
Em_j	Endereço MAC do nó escolhido (Retransmissor)

Cada alerta gerado tem um identificador único definido pela aplicação. Este identificador é armazenado no campo Id_k e é gerado através da utilização de uma função *hash* (o algoritmo SHA1 - Secure Hash Algorithm). Esta função produz uma sequência de bits de tamanho fixo a partir do mapeamento dos bits pertencentes às informações armazenadas nos campos Em_i, t_i^k e Ds_k, conforme descrito na equação

$$Id_k = hash(Em_i + t_i^k + Ds_k) \tag{4.8}$$

na qual Em_i é a sequência de bits que representa o endereço MAC da máquina que criou o alerta; t_i^k é a sequência de bits que representa a data e hora em que o alerta foi enviado; e Ds_k é a sequência de bits que representa as informações adicionais sobre o alerta.

O identificador único da mensagem é utilizado na comparação de alertas. Esta comparação é feita pela aplicação com o objetivo de evitar o envio de alertas já emitidos e a repetição de alertas disponibilizados aos condutores. O segundo campo da mensagem de dados, chamado de Em_i, é responsável por armazenar o endereço MAC no nó que criou o alerta e tem seu tamanho estipulado em 48 bits[1].

Já o campo Tp_k armazena o código referente ao tipo de alerta a ser emitido, com um tamanho de 10 bits. Os tipos de alertas dependerão dos tipos de sensores instalados no veículo e estão fora do escopo deste trabalho. Este campo tem capacidade de armazenar 10 bits, suficiente para representar um código de três dígitos. A descrição do alerta a ser enviado é armazenada no campo Ds_k, esse campo é capaz de armazenar 1.600 bits, ou seja, duzentos caracteres ASCII. A utilização desse campo permite aumentar o nível de detalhamento do alerta a ser enviado.

Para armazenar a longitude e a latitude do local onde houve a ocorrência, foi criado o campo x_i, y_i, com tamanho estipulado em 256 bits, suficiente para armazenar as informações obtidas pelo GPS. O campo t_i^k da mensagem é responsável por armazenar a data e hora na qual o sensor detectou o evento. Possui o tamanho de 32 bits. Tv_k armazena o tempo de vida que a mensagem k deve ter na rede. O campo t_i^k deve ser verificado no recebimento da mensagem de alerta, sendo utilizado como meio para garantir que a mensagem de alerta foi recentemente criada (*freshness*). Desta forma, é possível evitar que mensagens antigas que não refletem mais a situação atual da rodovia sejam retransmitidas. O campo Tag_k é utilizado para armazenar o valor *0* ou *1* e serve para determinar se a mensagem é derivada da operação lógica XOR entre duas mensagens de dados (*Alerta 1* $\oplus$ *Alerta 2*). O último campo presente no alerta é o campo Em_j. Este campo é responsável por armazenar o endereço MAC do nó escolhido para ser o retransmissor do alerta.

Como pode ser observado no Algoritmo 6, o qual apresenta os passos para a criação e disseminação da mensagem de alerta na rede, se o sensor localizado no veículo detectar algum evento e (linha 6), a aplicação irá obter as coordenadas do GPS e o tipo de alerta emitido, conforme demonstrados nas linhas (7 a 8). Caso o evento detectado

[1]Tamanho suficiente para representar um endereço MAC que é composto por doze dígitos hexadecimais.

seja um evento ainda não reportado (linha 14), a aplicação irá obter a data e hora (linha 15) e criará um ID único da mensagem (linha 16). Por fim, será gerada a mensagem (linha 21), a qual será repassada aos vizinhos (linha 22) que estão no seu raio de cobertura, para alertá-los sobre o perigo relatado.

Algorithm 6: Envio Alerta

```
1  inicio
2      MA_i ← Conjunto de mensagens de alertas recebidos pelo nó i;
3      Em_i ← Identificador único do veículo;
4      N_i^j ← Conjunto de nós vizinhos j no raio de cobertura do nó i;
5      e^i ← Eventos detectados pelos sensores do veículo i;
6      se (i detectar e) então
7          x_i, y_i ← Obter coordenadas;
8          Tp_k ← Obter tipo do alerta(e)
9          Tag_k ← 0; /* Define Tv_k de acordo com Tp_k
10         /* Veículo i verifica se já recebeu uma mensagem (Alerta)
               reportando evento e */
11         para cada Alerta ∈ MA_i hacer
12             Tp_old ← Alerta.Tp;
13             x_i, y_i old ← Alerta.x_i, y_i;
14             /* Evento ainda não reportado. Alerta é criado e disseminado
                   na rede */
15             se (Tp_old ≠ Tp) e (x_i, y_i old ≠ x_i, y_i) então
16                 t_i^k ← Obter Data/Hora;
17                 Id_k ← Calcula Hash(Em_i, t_i^k, Ds);
18                 /* Gera a mensagem RQ */
19                 Enviar(RQ);
20                 /* Atualiza vizinhança de acordo com os dados obtidos
                       nas trocas de mensagens CM */
21                 /* Seleciona retransmissor */
22                 Alerta ← Gera(Id_k, Em_i, Tp_k, Ds, x_i, y_i, Tv_k, t_i^k,
                       Tag_k, Em_j);
23                 Enviar(Alerta);
```

4.3.2 Envio de Mensagens de Controle Adaptativo

Nesta proposta a mensagem de controle utilizada pelo nó i para obter informações de sua vizinhança é a mensagem *CM*. Em abordagens estudadas no Capítulo 3 esta mensagem também existe e funciona de forma periódica. Esta característica acaba por interferir no funcionamento da rede, já que em determinados cenários a troca de mensagens de controle de forma periódica pode causar uma quantidade elevada de colisões de pacotes, por exemplo, em cenários com alta densidade de veículos. Para diminuir a quantidade de mensagens de controle em cenários densos buscou-se uma nova abordagem, este trabalho utiliza

mensagens de controle aperiódicas. Estas mensagens têm como base um período minimo entre retransmissões, porém este período se adapta de acordo com a densidade local do nó (linha 2 nos Algoritmos 2 e 6). Quanto maior a densidade local do nó, maior será o período entre retransmissões da mensagem de controle, desta forma em cenários de congestionamento os nós deixarão o canal de comunicação livre mais tempo para que possa ser utilizado por uma transmissão de alerta.

Para que o nó i possa calcular este período a cada mudança de densidade local é utilizada a seguinte equação:

$$\alpha_i = (Pf + (D_i.TpV)) - Random[0, 0.002] \tag{4.9}$$

na qual, a componente Pf representa um período fixo minimo igual a todos os nós pertencentes na rede (ex. 150 ms), já a componente D_i determina a densidade local do nó j (veículos na vizinhança de j), TpV define o tempo que cada veículo acrescenta ao cenário e, por fim, a componente $Random[0, 0.002]$ tem papel de gerar um *offset* com valor entre 0 e 2 ms no período α_i. O *offset* é criado para diminuir a chance de dois ou mais nós terem o mesmo período entre retransmissões e acabar por gerar colisões de pacotes na rede.

O período α_i é calculado sempre que a densidade local do nó i for alterada. No Algoritmo 7 podemos observar como esse processo ocorre. A tarefa *T1* ao ser realizada define se foi ou não inserido novo vizinho na lista de vizinhos, caso tenha sido inserido novo vizinho, o nó i irá calcular seu período α_i por meio da Equação 4.9, caso contrário o nó i mantem seu período α_i anterior ao recebimento da mensagem de controle, já que não houve mudança em sua lista de vizinhos.

Algorithm 7: Calculo de α_i

```
1  inicio
2      α_i ← Período definido de acordo com a densidade local de i;
3      Pf ← Período minimo;
4      D_i ← Densidade local do nó;
5      NovoVizinho ← falso;
6      Tarefa: T1 /* Recepção de atualização de dados */
7      ao receber mensagem de controle
8      Atualizar(lista de vizinhos)
9      NovoVizinho ← Atualizar(lista de vizinhos);
10     se (NovoVizinho = verdadeiro)) então
11         retorna α_i ← Calculaα_i(Pf, D_i);
12     senão
13         retorna /* Mantem α_i anterior */;
```

4.3.3 Mecanismo de Codificação de Rede

Segundo Ahlswede et al. (2000), em uma rede *unicast*, o roteamento é suficiente para atingir o fluxo máximo da rede. Porém, em redes *broadcast*, a codificação de rede pode ser necessária. Trabalhos como (OLIVEIRA et al., 2011) e (CRUZ et al., 2012) mostram que a utilização da codificação de rede pode melhorar o roteamento de mensagens em redes veiculares. Seu funcionamento foi abordado anteriormente na Seção 2.6.

Neste trabalho a operação XOR é utilizada em cenários nos quais existem mais de uma mensagem de dados na rede. Desta forma, os nós podem armazenar estas mensagens em suas listas de alertas. Por exemplo, o nó i tem em sua posse duas mensagens existentes na rede *Alerta 1* e *Alerta 2*, em um determinando momento este nó i recebe uma primeira mensagem de controle CM de um nó j vizinho. Então o nó i dispara um tempo de espera relativamente pequeno, porém suficiente para receber mais mensagens de controle de outros vizinhos a sua volta. Este tempo de espera é chamado de $TeCM_{max}$. Durante este tempo de espera, o nó i recebe um conjunto de mensagens de controle (MC_i) de outros vizinhos e, ao expirar $TeCM_{max}$, i verifica que um grupo de nós vizinhos não recebeu a mensagem *Alerta 1* e um segundo grupo de vizinhos não recebeu a mensagem *Alerta 2*. Ao verificar esta situação, o nó i calcula a porcentagem de nós vizinhos que requisitaram o *Alerta 1*, por meio da seguinte equação:

$$Pxor = \frac{TotalAlerta1}{TamMC_i} \tag{4.10}$$

Ao verificar que a porcentagem de nós requerentes do *Alerta 1* está dentro do limiar definido por [$Int_{inicial}$, Int_{final}], o nó i realiza a operação lógica XOR entre as duas mensagens (*Alerta 1* $\oplus$ *Alerta 2*).

O limiar [$Int_{inicial}$, Int_{final}] é configurável. Ao calcular $Pxor$, é obtida a porcentagem de veículos que requisitaram *Alerta 1*. Por exemplo, caso o limiar definido seja [40 %, 60 %] e 50 % dos vizinhos tenham requisitado o *Alerta 1* será realizada a operação XOR entre as mensagens; caso contrário as mensagens serão difundidas separadamente. A operação XOR é realizada bit a bit em cada mensagem. O processo para definir se deve ser ou não realizada a operação XOR pode ser observado no Algoritmo 8.

No Algoritmo 8 pode-se observar que ao verificar a existência de mais de uma mensagem vigente na rede e que $Pxor$ está contido em [$Int_{inicial}$, Int_{final}], o nó i gera o XOR das mensagens e o envia. Ao

Algorithm 8: Recebimento CM e Operação XOR

```
1  inicio
2      MA_i ← Conjunto de mensagens de alertas recebidos pelo nó i;
3      MC_i ← Lista de mensagens de controle recebidas durante o
       TeCM_max;
4      LA_i ← Lista temporária de mensagens de controle CM;
5      Envioltima ← falso;
6      cont ← 0;
7      intervalo ← [Int_inicial, Int_final] /* intervalo de probabilidade */;
8      Tarefa: T1 /* Recepção de atualização de dados */
9      ao receber mensagem de controle
10     se (i recebeu CM) então
11         /* i aguarda o tempo de espera TeCM_max expirar */
12         /* O nó i armazena todas as mensagens de controle recebidas na
           lista MC_i até que o tempo de espera TeCM_max expire */
13         repita
14             se (CM.Id_k = 0) então
15                 se (EnvioÚltima = falso) então
16                     Alerta ← Recupera o último alerta em CM_i;
17                     Envioltima ← verdadeiro;
18                     Enviar(Alerta);
19                 senão
20                     /* Verifica a próxima mensagem de controle CM */
21             senão
22                 se (CM.Id_k ∈ MA_i) então
23                     se (CM.Id_k ∉ LA_i) então
24                         LA_i ← Recupera alerta de MA_i;
25                         cont++;
26                 senão
27                     CM ← GeraCM(Em_i, D_i, Tp_k, pA_i, pI_i, V_i, Id_k);
28                     Enviar(CM);
29         até fim de MC_i;
30         se (cont > 1) então
31             TamMC_i ← sizeof(MC_i);
32             TotalAlerta1 ← Recupera o total de vezes que o Alerta1
               aparece em MC_i;
33             Pxor ← CalculaPxor(TamMC_i, TotalAlerta1);
34             se (Pxor ∈ intervalo) então
35                 Alerta ← GeraXOR(LA_i);
36                 Enviar(Alerta);
37                 MA_i ← Alerta;
38             senão
39                 repita
40                     Alerta ← Recupera alerta de LA_i;
41                     Enviar(Alerta);
42                 até fim de LA_i;
43         senão
44             Alerta ← Recupera alerta de LA_i;
45             Enviar(Alerta);
```

gerar o XOR das duas mensagens, o alerta recebe em seu campo Tag_k, o valor *1*. Desta forma, fica sinalizado que a mensagem é um XOR de duas outras mensagens, e o nó receptor pode realizar o processo inverso, obtendo a mensagem que ainda não havia recebido. Com este mecanismo, a quantidade de retransmissões pode ser diminuída. Esta diminuição pode ocorrer pelo fato que i não terá que realizar duas vezes o processo de retransmissão de mensagens. Com a codificação de rede o protocolo proposto pode, em determinados cenários, atender nós vizinhos com menos retransmissões.

4.3.4 Lista de Mensagens

A lista de mensagens, denominada neste trabalho como MA_i, é responsável por armazenar as mensagens de dados (alertas) recebidas pelo nó i. Esta lista é atualizada cada vez que uma nova mensagem é recebida e/ou quando uma mensagem tem seu tempo de vida concluído, desta forma a mensagem é retirada na lista. O nó i ao receber uma mensagem de controle MR, verifica se $MR.Id_k$ existe em sua lista MA_i, caso exista, esta mensagem deve ser retirada da lista. O processo é descrito no Algoritmo 9.

Algorithm 9: Remoção de Mensagem da Lista MA_i

```
1  inicio
2      MA_l ← Conjunto de mensagens de alertas recebidos pelo nó l;
3      Timestamp_i ← Recupera Data/Hora no instante i;
4      retirada ← falso;
5      Tarefa: T1 /* Recepção de MR */
6      ao receber mensagem de controle
7      se (i recebeu MR) então
8          se (MR.Id_k ∈ MA_i) então
9              retirada ← retirar(MR.Id_k);
10     se ((Timestamp_i − Alerta.t_i^k) > Alerta.Tv_k) então
11         retirada ← retirar(MR.Id_k);
12         Id_k ← Alerta.Id_k;
13         t_i^k ← Alerta.t_i^k;
14         MR ← GeraMR(Id_k, t_i^k, Tp);
15         Enviar(MR);
```

4.4 MÓDULO DE DETERMINAÇÃO DA VIZINHANÇA

O módulo de Determinação da Vizinhança é responsável pela atualização da lista de vizinhos, na qual, cada nó i armazena os dados dos vizinhos j, de quem tenha recebido uma mensagem de controle *CM*. Uma vez que um nó j faz parte da lista de vizinhos de um nó i, esse permanece na lista até que uma das estratégias implementadas pelo mecanismo de determinação de vizinhança o remova.

As estratégias implementadas neste módulo procuram minimizar o impacto que a mobilidade e a comunicação têm sobre a manutenção da vizinhança de um nó. Isto é feito em duas fases: primeiro um mecanismo de detecção de conectividade avalia se os vizinhos de um nó i ainda estão dentro de sua da área de cobertura de comunicação; e segundo, um mecanismo de adaptação de tempo de espera (*adaptative timeout*) procura evitar que atrasos e perda de sinalizações levem a frequentes remoções e reinserções de nós na lista de vizinhos.

A correta determinação de quais vizinhos estão ativos dentro da área de cobertura de comunicação de um nó, reduz o número de atrasos e perda de mensagens entre os processos, além de auxiliar no processo da determinação do nó retransmissor. Para isso, o mecanismo de determinação de vizinhança é constituído pelo algoritmo de atualização de vizinhança. O algoritmo de atualização de vizinhança é representado em pseudocódigo no Algoritmo 10.

Algorithm 10: Remoção de Vizinho

```
1  inicio
2      Tarefa: T1 /* Difusão de Mensagens de Controle */
3      Montar a mensagem CM
4      Difunde uma mensagem CM a cada T_s segundos
5      Tarefa: T2 /* Recepção de atualização de dados */
6      ao receber mensagem de controle
7      Atualizar(lista de vizinhos)
8      Tarefa: T3 /* Remoção do nó j da vizinhança de i */
9      repita
10         Quando β_j expira /* timeout do vizinho j expirou */
11         se (DC_(i,j)) = verdadeiro então
12             retorna β_(i,j) ← Calcular novo tempo de espera
13         senão
14             retorna Remover nó j da lista de vizinhos;
15     até sempre;
```

O Algoritmo 10 é composto por três tarefas executadas simultaneamente. A primeira tarefa, (linhas 2 a 4), realiza a geração e recepção de mensagens de controle *CM*, cujo campos foram descritos na Subse-

ção 4.3.1. Na segunda tarefa, atualiza-se a lista de vizinhos N_i a partir dos dados das mensagens recebidas (linhas 5 a 7). A última tarefa é responsável pela recuperação ou pela eliminação de um nó da lista de vizinhos (linhas 8 a 15). Nesta tarefa, quando o tempo de espera β_j expira, o nó i avalia através da estimativa de validade do enlace $DC_{(i,j)}$, a permanência do nó j em sua lista de vizinhos. As premissas avaliadas na tarefa *T3*, são apresentadas nas subseções a seguir.

4.4.1 Lista de Vizinhos

Toda vez que um nó i receber uma mensagem de controle *CM* de um vizinho *j*, deverá atualizar a sua lista de vizinhos *Ni*. A lista de vizinhos tem papel importante no funcionamento do protocolo, pois armazena informações pertinentes para a escolha do nó que deverá ser o retransmissor do alerta em um segundo momento. O nó i, ao receber uma mensagem de controle *CM*, obtém as informações e as adiciona na lista de vizinhos. No momento em que o nó precise gerar ou retransmitir um alerta, caso seja um nó escolhido para retransmitir, este nó i irá percorrer sua lista de vizinhos e obter os valores necessários para realizar, por exemplo, a escolha de um nó retransmissor.

4.4.2 Mecanismo de Adaptação dos Tempos de Espera

A comunicação nas redes VANETs é normalmente realizada pela difusão periódica de mensagens. Entretanto, nesta proposta a difusão passa a ser aperiódica e adaptativa de acordo com a densidade existente ao redor do nó transmissor. O *timeout* β_j, calculado em cada nó i, define um tempo de espera para que cada um de seus vizinhos j entregue a próxima mensagem de controle. Assume-se inicialmente que existe um período fixo entre as retransmissões da mensagem de controle *CM* e este período é modificado de acordo com a Equação 4.9. Por meio da obtenção da densidade local D_j de j é possível determinar o tempo de espera de uma mensagem de controle que será enviada por *j*. Para determinar este tempo é utilizada uma variação da Equação 4.9, dada por:

$$\beta_j = Pf + (D_j.TpV), \tag{4.11}$$

no qual, Pf é o período entre retransmissões inicial fixo e igual a todos os nós pertencentes a rede. Já a componente D_j determina a densi-

dade local do nó j e TpV define o tempo que cada veículo representa no cenário. Quando um nó adapta seu tempo de espera por uma sinalização de um vizinho, este lida melhor com as mudanças nas condições de comunicação da rede e reduz o número de enlaces perdidos.

4.4.3 Detector de Conectividade

Além de adaptar o tempo de espera as condições do meio físico das redes veiculares, o protocolo desenvolvido propõe um mecanismo para detectar a conectividade entre os nós. O detector de conectividade busca estimar a posição dos vizinhos, dos quais se tenha perdido alguma mensagem de controle e determinar se o nó vizinho ainda se encontra em sua área de cobertura de comunicação. A estimativa de conectividade é realizada pelo algoritmo a seguir. Para estimar se um enlace de comunicação permanece válido entre dois vizinhos, o nó i utiliza informações deste e as que já estão armazenadas na lista N_i. As informações utilizadas são: a última posição e velocidade conhecidas do vizinho j, além de sua posição anterior no instante $t^k - 1$, o raio de comunicação r_i e o *timestamp* da última sinalização deste vizinho que foi recebido pelo nó i (linhas 1 a 8). Caso o *timestamp* das informações do nó j respeite o limite de tempo *NSth*, no qual se considera as informações deste válida, realiza-se o processo que define a posição estimada de j.

Antes de obter Pe_j deve-se descobrir se o nó j está se aproximando ou se distanciando do nó i. Para obter esta informação é usada a Equação 4.5 (linhas 10 e 11). O resultado obtido por esta equação é submetido ao Algoritmo 12.

St_j poderá assumir dois valores +1 ou -1. O valor positivo determina que o nó j está se distanciando do nó i e o valor negativo define que o nó j está se aproximando de i. Desta forma, é possível determinar a posição estimada de j por meio da Equação 4.13. Após definir St_j, o Algoritmo 11 busca obter a distância percorrida por j (linhas 12 e 13) dentro do espaço de tempo delimitado por t_j^{last} e t_i^k, para definir Dp_j é utilizada a seguinte equação:

$$Dp_j = (t_i^k - t_j^{last}).V_j, \tag{4.12}$$

A estimava da posição do nó j (linha 14) é mensurada através da função *CalculaPosicaoE*() (linha 15) e esta função faz uso da seguinte equação:

Algorithm 11: Detector de Conectividade

```
1  inicio
2      enlace ← Inválido;
3      t_i^k ← Tempo atual em i;
4      t_j^last ← Último timestamp recebido do vizinho j;
5      V_j ← Último velocidade conhecida de j;
6      pI_i ← Posição atual do nó i;
7      pI_j ← Última posição conhecida do nó j;
8      pA_j ← Posição anterior conhecida do nó j;
9      se (t_i^k − t_j^last) ≤ NSth então
10         /* Sentido do nó j */
11         St_j ← CalculaSt(pI_i, pI_j, pA_j);
12         /* Calcula distância percorrida de j */
13         Dp_j ← CalculaDp(t_j^last, t_i^k, V_j);
14         /* Calcula posição estimada j */
15         Pe_j ← CalculaPosicaoE(pI_j, pI_i, Dp_j, St_j);
16         se ( Pe_j ≤ r_i ) então
17             retorna enlace ← válido;
18         senão
19             retorna enlace ← inválido;
```

Algorithm 12: Obtenção do valor de St_j

```
1  inicio
2      St_j ← Recupera o sentido de direção do nó j;
3      se (St_j ≥ 0)) então
4          retorna St_j = -1;
5      senão
6          retorna St_j = +1;
```

$$Pe_j = \left| dI_{(i,j)} + (Dp_j.St_j) \right|, \tag{4.13}$$

na qual, a componente $dI_{i,j}$ é definida pela Equação 4.7, já as componentes Dp_j e St_j são definidas respectivamente pelas Equações 4.12 e 4.5.

Se a diferença entre as posições de i e j for menor que o raio de comunicação de i, este considera o enlace válido, caso contrário o enlace será inválido (linhas 17 e 19).

4.5 CONSIDERAÇÕES FINAIS

A utilização das redes veiculares inclui aplicações para prover segurança aos condutores dos veículos. Estas aplicações visam minimizar acidentes e melhorar as condições do tráfego concedendo informações úteis por meio de mensagens de dados, como por exemplo, problemas na pista, avisos de colisão, ponto de congestionamento, entre outros.

No entanto, é necessário prover confiabilidade na entrega destas mensagens de dados. O protocolo proposto foi desenvolvido com o objetivo de aumentar esta confiabilidade, através de um misto de mecanismos, além de prover confiabilidade na entrega das mensagens. Este busca minimizar o impacto que mensagens de controle provocam em cenários com alta densidade, por meio de um protocolo adaptativo.

Este capítulo descreveu o protocolo proposto que visa prover confiabilidade na entrega de mensagens da rede que faz uso de uma aplicação voltada a disseminação de alertas. As premissas a serem adotadas, o detalhamento das mensagens do protocolo e da aplicação foram definidos e especificados. Todos os mecanismos empregados no protocolo proposto também foram apresentados, juntamente com seus algoritmos e equações necessárias para o funcionamento dos mecanismos implementados.

5 SIMULAÇÃO E ANALISE DOS RESULTADOS

Este capítulo tem como objetivo descrever o projeto de experimentos executado para avaliar o protocolo proposto e apresentar os resultados das simulações com suas respectivas análises. A confiabilidade do protocolo é avaliada por meio da taxa do sucesso da entrega dos alertas, número de colisões de pacotes, da mobilidade e densidade dos nós da rede e latência da rede. Desta forma foi possível definir o impacto do uso deste protocolo na rede veicular. Os experimentos simulados serviram para avaliar se utilização dos mecanismos para prover confiabilidade ao protocolo não prejudica a entrega dos alertas pela aplicação.

Este capítulo, primeiramente, apresenta o ambiente de simulação com uma breve descrição dos simuladores de rede e de tráfego veicular escolhido para os experimentos, bem como uma descrição dos parâmetros desses simuladores. Os parâmetros adotados na aplicação desenvolvida e no protocolo proposto também são descritos. Em seguida, o projeto de experimentos utilizados para a avaliação com suas métricas é apresentado. Por fim, os resultados obtidos nos experimentos e uma análise destes são descritos.

5.1 AMBIENTE DE SIMULAÇÃO

O funcionamento de um protocolo pode ser verificado de diversas formas, dentre estas se destacam as simulações, que tem como objetivo reproduzir o comportamento do protocolo e da aplicação implementada, visto que às vezes os custos dos testes em ambientes reais podem ser bastante elevados. Além disso, a utilização de simuladores permite um controle melhor sobre o ambiente como a repetição dos experimentos considerando diferentes cenários (por exemplo, a densidade de veículos).

5.1.1 Simulador de Rede Escolhido

O OMNeT++ (Objective Modular Network Testbed in C++) é um simulador de eventos discretos para modelagem de redes de comunicação, que baseia-se, fundamentalmente, no conceito de módulos, facilitando deste maneira a criação de diferente protocolos, modelos ou topologia de redes. Neste simulador, as simulações podem ser execu-

tadas via linha de comando ou com interface gráfica interativa, que facilita as simulações complexas e em grande escala (VARGA, 2013).

No que diz respeito aos protocolos e padrões de comunicação de rede, estes não são implementados pelo OMNeT, ficando isso a cargo de módulos adicionais. O INET *framework* é um destes módulos adicionais, sendo um pacote *open source* no qual há vários protocolos de redes cabeadas e sem fio já implementados, tais como, UDP, TCP, IP, OSPF, 802.11 entre outros. O INET *framework* é também o módulo mais utilizado na comunicação sem fio, além de possuir uma vasta documentação relacionada a este, o que colabora para o desenvolvimento rápido de novos módulos.

A escolha pelo simulador OMNeT++/INET foi devido a este ter uma interface clara que facilita o desenvolvimento das aplicações, permitindo também o uso de *frameworks* específicos para redes veiculares, além de sua ampla utilização no meio acadêmico. Outro fator importante para a escolha, é que este simulador pode trabalhar bidirecionalmente acoplado com geradores de tráfegos, como por exemplo, a ferramenta SUMO (Simulation of Urban Mobility), o que facilita as simulações mais detalhadas sobre os efeitos de determinados parâmetros sobre o tráfego na rede.

5.1.2 Simulador de Tráfego

Com o objetivo de tornar as simulações mais realistas, foi utilizada a ferramenta geradora de cenários de mobilidade SUMO (Simulation of Urban Mobility). Esta ferramenta destaca-se por poder ser integrada ao simulador OMNET++ (acoplamento bidirecional), além de ser amplamente utilizada em pesquisas acadêmicas na área de redes veiculares (VANETs). Conforme Dressler et al. (2008), a ferramenta possibilita a criação manual de mapas, a importação de mapas, e a criação de várias classes de veículos (ônibus, carros e motos), caracterizadas pelo seu comprimento, valores de aceleração e desaceleração, velocidade máxima e imperfeição do condutor. O SUMO destaca-se ainda por permitir a realização de ultrapassagens, sempre que a via da esquerda esteja livre, retornando a sua faixa logo após a ultrapassagem.

A facilidade de configuração dos cenários de mobilidade, a facilidade de implementação dos experimentos e a possibilidade, em tempo real, da integração com o simulador de rede OMNeT, foram os principais fatores que justificaram a escolha deste como ferramenta de simulação de tráfego adotada.

5.1.3 Parâmetros do Simulador de Redes

Os parâmetros do simulador de redes (OMNeT++/INET) foram definidos de forma que todas as comunicações na rede fossem realizadas conforme o padrão IEEE 802.11g. Embora exista o padrão 802.11p (DSCR/WAVE) desenvolvido especialmente para as redes veiculares, este não foi adotado, pois a implementação deste no OMNeT++/INET é bem recente e pouco difundida (nenhum trabalho acadêmico que utiliza este simulador fez uso dessa implementação). Apesar disto, procurou-se usar parâmetros que emulem algumas características do padrão 802.11p.

A Tabela 7 lista os parâmetros de configuração do simulador de rede OMNeT++/INET, para atender os requisitos desejados. Tais parâmetros foram configurados de forma a seguir as características apresentadas do *datasheet* do *Acess Point* Cisco Aironet 1260. As configurações feitas também tiveram como objetivo, manter a integridade dos pacotes enviados, prevenindo que estes se transformem em ruído. Como as transmissões são feitas por meio de *broadcast*, foram desabilitados o RTS e o CTS. Para simular a propagação das ondas de rádio, o modelo de espaço livre simples foi utilizado.

Tabela 7: Parâmetros da rede configurados no INET Framework.

Parâmetros	Valores
wlan.mac.address	auto
wlan.mac.maxQueueSize	14
wlan.mac.bitrate	12 Mbps
wlan.radio.channelNumber	0
wlan.radio.transmitterPower	25 mW
wlan.radio.bitrate	12 Mbps
wlan.radio.thermalNoise	-95 dBm
wlan.radio.pathLossAlpha	1,9
wlan.radio.snirThreshold	3 dB
wlan.radio.sensitivity	-83 dBm
channelcontrol.carrierFrequency	2,4 GHz
channelcontrol.pMax	50 mW

5.1.4 Cenário de Mobilidade

Neste trabalho, o modelo de mobilidade a ser utilizado foi o acoplamento bidirecional entre um simulador de rede e um gerador de tráfego. Este modelo permite movimentos realistas, a obtenção de informações sobre o comportamento dos nós e facilita a analise dos resultados. Este modelo de mobilidade também permite a parametrização da rede e das aplicações desenvolvidas. Nas simulações que utilizam esse modelo de mobilidade, dois processos interdependentes são executados simultaneamente, ou seja, o simulador de rede e o simulador de tráfego. Ambos os processos compartilham dados como a posição e a velocidade dos veículos simulados. Informações atualizadas sobre o movimento de veículos simulados são trocadas em intervalos regulares. Segundo Dressler et al. (2008), a simulação bidirecional acoplada geralmente consiste de duas fases alternadas. Na primeira fase a simulação da rede envia as alterações de parâmetros para a simulação do tráfego, alterando o comportamento do condutor ou atributos referentes à estrada e que influenciam as decisões dos veículos. Já na segunda fase, em intervalos regulares, a simulação do tráfego executa cálculos de tráfego com base nesses novos parâmetros e envia atualizações dos movimentos dos veículos para a simulação da rede.

A modelagem em simulações bidirecionalmente acopladas depende da intercomunicação intensa das ferramentas de simulação usando diferentes interfaces. Já na modelagem de simulações de traços artificiais, o gerador de tráfego cria estes traços para que posteriormente sejam utilizados na simulação da rede. Em simulações que utilizam movimentos aleatórios, o modelo de mobilidade pode ser implementado no próprio simulador de rede, dispensando ferramentas geradoras de tráfego, como pode-se observar na Figura 14.

5.1.4.1 Cenário de Mobilidade Desenvolvido

O desenvolvimento do cenário de mobilidade utilizado nos experimentos pode ser dividido em três fases: inicialmente, criou-se a via de circulação dos veículos, recorrendo ao gerador de tráfego SUMO; em seguida, foram criadas e caracterizadas as diferentes classes de veículos utilizadas na simulação; finalmente, na última fase, utilizando novamente o gerador de tráfego SUMO, foram gerados os movimentos dos veículos, obtendo-se assim o cenário de mobilidade necessário para as simulações.

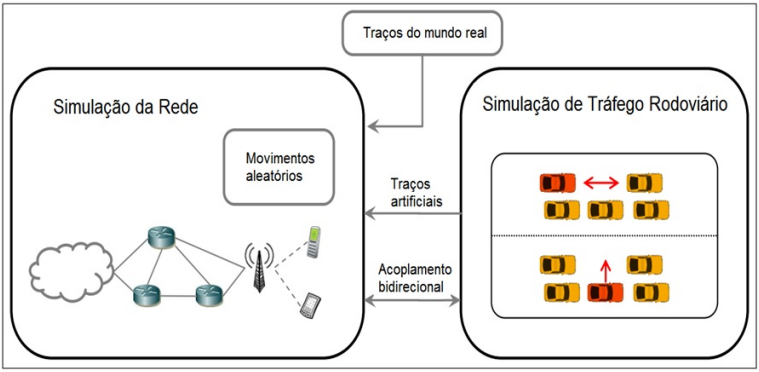

Figura 14: Técnicas de modelagem de mobilidade para a simulação de protocolos e aplicações para VANETs.

Recorrendo ao comando *netconvert* da ferramenta SUMO, foi implementado um trecho real da rodovia BR-101 entre os municípios de Itapema e Porto Belo no estado de Santa Catarina, que se encontra a aproximadamente 50 km de distância de Florianópolis. Este trecho de 5 km pode ser observado na Figura 15. O trecho é composto por dois sentidos e duas faixas para cada sentido, tendo quatro faixas de rodagem no total, com uma velocidade máxima estipulada em 110 km/h. O tráfego diário normal neste trecho segundo o Posto Policial Rodoviário Federal[1] do município de Itapema é de 60 mil veículos, sendo constituído por veículos de passeio de 2 eixos, veículos destinados ao transporte de carga, com até 6 eixos, veículos destinados ao transporte de passageiros, com até 3 eixos e, por fim, de motocicletas.

De modo a tentar recriar o conjunto de veículos que circulam no trecho entre os municípios de Itapema e Porto Belo, foram definidas quatro classes de veículos, sendo distinguíveis no seu comprimento, velocidade máxima, probabilidade, imperfeição do condutor[2], taxa de aceleração e desaceleração (ver Tabela 8):

- **Classe 1:** os veículos desta classe representam os carros que

[1]Por meio de contato telefônico com o Posto da Policia Rodoviária Federal localizado no km 143 da rodovia BR-101, foram obtidos os dados referentes ao fluxo de veículos no trecho. Contato: (47) 33682055.

[2]O parâmetro imperfeição do condutor, pode assumir valores entre 0 e 1 e determina como o condutor reage a certas situações, por exemplo, em que momento tomar a decisão de ultrapassar outro veiculo.

Figura 15: Trecho real entre os municípios de Itapema e Porto Belo.

trafegam na via e são caracterizados por uma velocidade máxima de 30,6 m/s (110 km/h), valores de aceleração e desaceleração são de 3 m/s^2 e 6 m/s^2 respectivamente, um comprimento de 5 m. Esta classe representa aproximadamente 65% dos veículos que compõem o cenário. Seu parâmetro de comportamento do condutor é de 0,5;

- **Classe 2:** os veículos que pertencem a esta classe caracterizam-se por serem mais lentos que os da classe anterior, atingido apenas os 22,3 m/s (80 km/h), sendo parametrizados com valores de aceleração e desaceleração de 1 m/s^2 e 4 m/s^2 respectivamente, um comprimento de 15 m e seu parâmetro para o comportamento do condutor está em 0,75. Esta classe corresponde aproximadamente a 26% dos veículos que circulam na rede e representam caminhões;

- **Classe 3:** os veículos que pertencem a esta classe caracterizam-se por se aproximar das características da classe anterior, atingem

um velocidade máxima de 22,3 m/s (80 km/h), sendo parametrizados com valores de aceleração e desaceleração de 1 m/s^2 e 4 m/s^2 respectivamente, um comprimento de 15 m e seu parâmetro para o comportamento do condutor está em 0,5. Esta classe corresponde aproximadamente a 8% dos veículos que circulam na rede e representam ônibus; e

- **Classe 4:** por fim, 1% dos veículos que restam no cenário de mobilidade fazem parte da Classe 4, que representam motocicletas. Nesta classe, os veículos atingem uma velocidade máxima de 30,6 m/s (110 km/h), parametrizados com aceleração de 3 m/s^2 e uma taxa de desaceleração de 6 m/s^2, apresentando 3 m de comprimento e comportamento do condutor em 0,5.

Após realizar a definição da via de circulação e caracterizar as quatro classes de veículos, definiu-se a quantidade e a distribuição dos veículos que fazem parte da simulação. Foi definido um alcance de rádio para os veículos de 300 m, ou seja, sempre que um veículo estiver a uma distância igual ou inferior a 300 m de outro, considera-se que existe uma ligação física entre ambos. Foram implementados alguns cenários de simulação de modo a representar cinco valores de densidade diferentes para a vizinhança dos veículos. Em todos os cenários, o comprimento da auto-estrada é mantido em 5 km.

Tabela 8: Características dos veículos.

Parâmetros	Classe 1	Classe 2	Classe 3	Classe 4
Tamanho (m)	5	15	15	3
Vel. Máxima (m/s)	30,6	22,3	22,3	30,6
Aceleração (m/s^2)	3	1	1	3
Desaceleração (m/s^2)	6	4	4	6
Probabilidade (%)	65	26	8	1
Imperfeição do Condutor (σ)	0,5	0,75	0,5	0,5

Após a definição das quatro classes de veículos e suas características, definiu-se a quantidade e a distribuição dos veículos que fazem parte da simulação. Para observar o comportamento do protocolo proposto diante de diferentes quantidades de veículos na rodovia, nas simulações, foram consideradas diferentes densidades de veículos. As densidades de veículos foram definidas a partir de uma quantidade máxima

de veículos repassados pela Polícia Rodoviária Federal que foi de 2500 veículos/hora ou 250 veículos em 360 segundos (tempo da simulação), sendo o valor médio de veículos/hora aqui considerado de 3000 veículos. Nas simulações, foram considerados os seguintes valores de densidade de veículo: 1000, 2000, 3000, 4000 e 5000 veículos/hora, considerando os dois sentidos da rodovia. Estes fluxos simulam os tráfegos esparso (1000 e 2000), médio (3000 e 4000) e denso (5000). Cabe ressaltar que em todos os cenários, o tamanho da autoestrada é mantido em 5 km.

Na Tabela 9 são apresentados os cenários de densidades de veículos na rede que foram simulados, considerando os dois sentidos da rodovia. Os elementos C1, C2, C3 e C4, presentes na Tabela 9, representam as classes de veículos 1, 2, 3 e 4, respectivamente. Estes cenários diferem apenas na quantidade de veículos que circulam na rodovia, respeitando a proporção apresentada na Tabela 8.

Tabela 9: Quantidade de veículos existentes em cada um dos cenários simulados.

Cenário	C1	C2	C3	C4	Nós/360 s^2	Nós/Hora
Cenário 1	65	26	8	1	100	1000
Cenário 2	130	52	16	2	200	2000
Cenário 3	195	78	24	3	300	3000
Cenário 4	260	104	32	4	400	4000
Cenário 5	325	130	40	5	500	5000

5.1.5 Parâmetros da Aplicação Desenvolvida

Em todos os cenários simulados, conforme descrito na Tabela 10, existem duas unidades de acostamento (RSUs) responsáveis pela propagação de alertas aos veículos que não receberam sinalizações pela forma convencional, desta forma buscou-se mitigar o problema do nó oculto. Uma foi posicionada no início do quilômetro um e a outra no início do quilômetro três.

Foi considerado, para fins de simulação, um evento dentro da área simulada. Este evento indica a existência de um acidente na pista e está localizado no quilômetro dois e meio da área de simulação, de um total de cinco quilômetros.

Tabela 10: Parâmetros Aplicação.

Parâmetros	Valores
Dimensão da Rede	5000 metros
Quantidade de veículos/hora	1000 - 2000 - 3000 - 4000 - 5000
Quantidade de RSUs	2
Posição RSU 1	1000 metros
Posição RSU 2	3000 metros
Posição do evento	2500 metros

5.1.6 Parâmetros do Protocolo

Para a simulação do protocolo, a fim de avaliar a confiabilidade, foi necessário configurar diversos parâmetros. Os parâmetros utilizados e seus valores podem ser vistos na Tabela 11.

Tabela 11: Parâmetros do Protocolo.

Parâmetros	Valores
Th_B	300 metros
Th_D	50 veículos
$TeCM_{max}$	150 milisegundos
C	1
Pf	300 milisegundos
TpV	20 milisegundos

5.1.7 Parâmetros do Ambiente Computacional

Todas as simulações realizadas durante o desenvolvimento deste trabalho foram feitas numa máquina com processador Intel Core I5 com dois núcleos, cada qual com frequência de clock de 3,2 GHz, 4GB de memória RAM e sistema operacional Microsoft Windows 7 de 64 bits.

5.2 PROJETO DE EXPERIMENTOS

Com o objetivo de avaliar (1) a confiabilidade do protocolo desenvolvido perante outras abordagens e (2) o impacto dos mecanismos implementados no desempenho da rede em diferentes condições de tráfego. O objetivo dos experimentos foi de avaliar a confiabilidade do protocolo ao entregar um alerta aos nós da rede e também avaliar os impactos decorrentes do uso dos mecanismos implementados na eficácia e eficiência da protocolo e da rede veicular. A seguir, tem-se uma descrição do projeto de experimentos.

5.2.1 Projeto para Avaliar a Eficácia do Protocolo Proposto

Estes experimentos visam avaliar os impactos decorrentes do uso dos mecanismos implementados na eficácia e na eficiência da Protocolo Proposto. Para isto quatro diferentes métricas são avaliadas.

As métricas utilizadas para avaliar os impactos são:

- Total de veículos que recebem a mensagem de alerta (eficácia): Para cada cenário de variação de densidade de veículos simulado, deve ser obtido o total de veículos que recebem a mensagem de alerta. Esta métrica tem como objetivo verificar se a mensagem foi recebida pela maioria dos veículos, desta forma determinar a confiabilidade do Protocolo Proposto;

- Total de pacotes gerados: Para avaliar se os mecanismos desenvolvidos para diminuir a quantidade de mensagens desnecessárias na rede surtem efeito perante cenários com densidades diferentes;

- Colisões de pacotes: Para avaliar o impacto na eficiência do Protocolo Proposto é importante verificar a quantidade de colisões de pacotes na rede. A colisão de pacotes acontece toda a vez que dois ou mais veículos tentam transmitir dados ao mesmo tempo, tendo como consequência a diminuição do desempenho na rede e podendo até prejudicar a eficácia do protocolo; e

- Tempo e distância do recebimento do alerta: Representa o tempo após a criação do alerta até o recebimento deste pelos veículos participantes da rede e a distância do local do evento. Desta forma, é possível verificar se os condutores terão tempo hábil para reagir com segurança a uma situação inesperada.

5.3 RESULTADO E ANÁLISE DOS EXPERIMENTOS

Para obtenção destes resultados, foram realizadas cinco simulações para cada cenário de densidade (1000, 2000, 3000, 4000 e 5000 veículos/hora) e uma média aritmética simples dos resultados de cada cenário foi calculada. Todos os resultados apresentados dos experimentos possuem 95 % de intervalo de confiança. E, conforme já descrito anteriormente, foi considerado um tempo de simulação de 6 minutos (360 segundos). Também nesta seção são avaliados e discutidos os resultados obtidos através dos experimentos das simulações.

5.3.1 Resultado e Análise da Quantidade de Nós Atendidos

Ao analisar os dados gerados pela ferramenta OMNeT++, pôde-se verificar qual foi a quantidade de nós atendidos em cada um dos cenários simulados. A premissa do Protocolo Proposto é atender a todos os nós existentes na rede para que todos os condutores tenham tempo de reagir a esta situação com segurança. A Tabela 12 apresenta o número de veículos que receberam a mensagem de alerta considerado o Protocolo Proposto em comparação com a abordagem de Broadcast Puro e o impacto provocado pelo uso do protocolo nesta métrica de eficácia.

Tabela 12: Quantidade de Veículos - Porcentagem de Mensagens de Alertas Recebidas

Densidade (veículos/hora)	Broadcast Puro	Protocolo Proposto
1000	93 %	100 %
2000	92,5 %	100 %
3000	92,3 %	100 %
4000	92 %	100 %
5000	91,2 %	100 %

Conforme apresentado na Tabela 12, o Protocolo Proposto diante da abordagem Broadcast Puro, obteve bom desempenho, o qual mostrou que o Protocolo Proposto pode prover confiabilidade em todos os cenários simulados. O Protocolo Proposto entregou o alerta a todos os nós presentes na rede. O impacto provocado pelo uso do Protocolo

Proposto para disseminar informações a todos os nós da rede fica claro em cenários com alta densidade, no qual o impacto chegou a 8,8 %, ao comparar o Protocolo Proposto com a abordagem Broadcast Puro.

Diante dos resultados obtidos na comparação entre o Protocolo Proposto e a abordagem de Broadcast Puro, buscou-se comparar o Protocolo Proposto com as seguintes abordagens estudadas neste trabalho: Asynchronous Fixed Repetition (AFR), Asynchronous p-persistent Repetition (APR) e Density-aware Reliable Broadcasting Protocol (DECA). O gráfico da Figura 16 apresenta a taxa de veículos que receberam a mensagem de alerta em relação ao número total de veículos na rodovia para cada uma das abordagens e em cada um dos cenários.

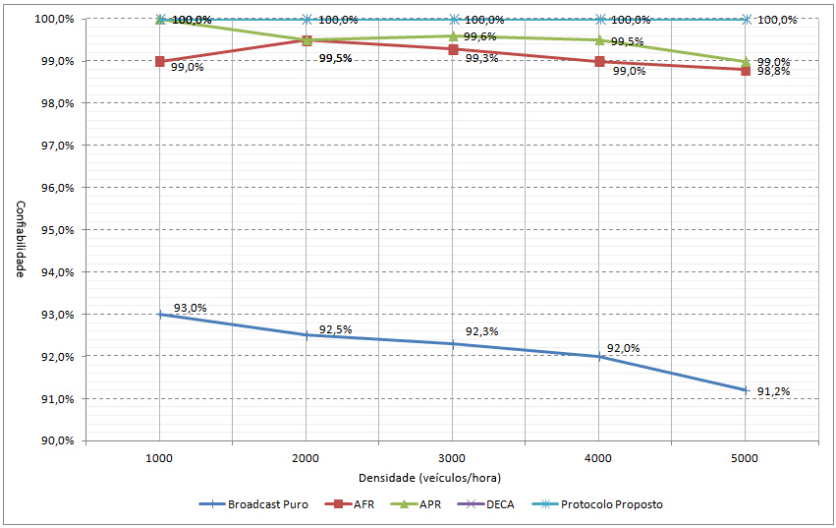

Figura 16: Porcentagem de Veículos que receberam a mensagem de dados (Alerta) - Broadcast Puro, AFR, APR, DECA e Protocolo Proposto

Após obter todos os resultados referentes a confiabilidade de cada uma das abordagens, pode-se verificar que as abordagens DECA e Protocolo Proposto mantêm a entrega das mensagens de dados em 100 % em todos os cenários simulados. Para efeito de comparação, buscou-se um cenário específico com uma configuração de carga na qual as abordagens deixam de entregar 100 % das mensagens. Estes cenários podem

ser observados na Figura 17.

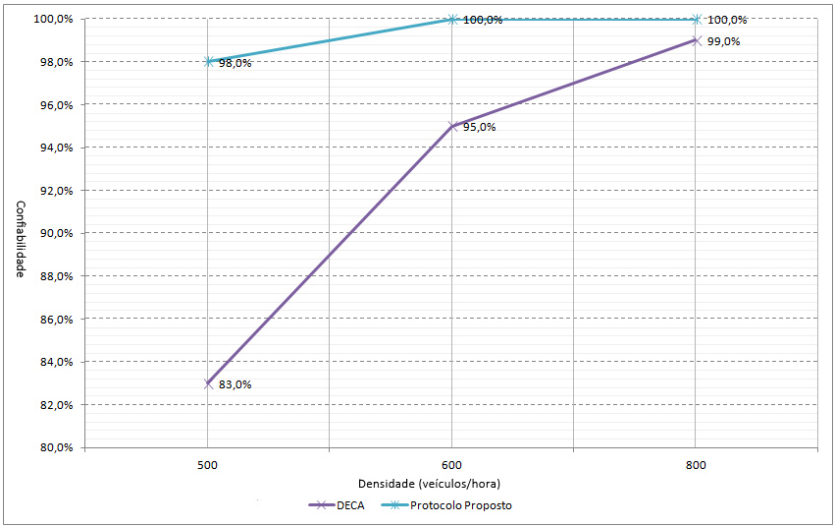

Figura 17: Porcentagem de Veículos que receberam a mensagem de dados (Alerta) - DECA e Protocolo Proposto

Na Figura 17 pode-se observar que a abordagem DECA deixa de entregar 100 % das mensagens de dados já no cenário com 800 veículos/hora, neste cenário o Protocolo Proposto ainda consegue manter a confiabilidade, porém o Protocolo Proposto chega ao seu limite no cenário com densidade de 500 veículos/hora, o Protocolo Proposto degrada sua confiabilidade em 2 %, já o protocolo DECA degrada ainda mais sua confiabilidade ao compararmos com o Protocolo Proposto. Estes cenários são improváveis de ocorrer no cenário real estudado neste trabalho. O Protocolo Proposto faz uso de RSUs e por este motivo consegue manter sua confiabilidade por mais cenários que o protocolo DECA. Em cenários com densidades muito baixas, a possibilidade de que esses cenários gerem situações como, por exemplo o nó oculto, é alta. Desta forma ao utilizar os nós fixos (RSU) ao longo da via o Protocolo Proposto mitiga este problema em boa parte dos cenários com baixa densidade, ao contrário das outras abordagens que não fazem uso deste mecanismo.

Em todas as densidades de veículos simuladas neste trabalho, que podem ocorrer no cenário real, os nós que trafegavam em ambos os

sentidos receberam o alerta por meio da utilização do Protocolo Proposto. Logo, o Protocolo Proposto mostrou-se 100 % eficaz ao atender a todos os nós que trafegavam na via, mesmo em situações extremas, por exemplo, densidade de 5000 veículos a cada uma hora, ou um número muito inferior de veículos que de fato trafegam no trecho, 600 veículos/hora.

5.3.2 Resultado e Análise da Quantidade de Colisões e Perdas de Pacotes

Uma colisão de pacotes acontece sempre que dois ou mais veículos tentam enviar dados ao mesmo tempo. Como pode ser observado através das simulações, quanto maior o número de veículos na rodovia, consequentemente, será maior a quantidade de mensagens enviadas e maiores serão as colisões de pacotes. Nas Tabelas 13 e 14 podem ser observados o total de pacotes gerados, (*Alertas + Beacons*) no caso do Protocolo Proposto, total de colisões geradas e a proporção de colisões diante o total de pacotes gerados em cada um dos cenários para as abordagens Protocolo Proposto e Broadcast Puro.

Tabela 13: Quantidade de Pacotes Gerados e Colisões geradas por cenários - Broadcast Puro

Densidade (veículos/hora)	Pacotes Gerados	Colisões	Proporção de Colisões
1000	985	89	9,1 %
2000	2346	356	15,2 %
3000	5020	943	18,8 %
4000	7292	1545	21,2 %
5000	9684	2692	27,8 %

Ao observar a Tabela 15, pode-se verificar a proporção de colisões geradas pelas abordagens estudadas em cada um dos cenários. Já a Figura 18, ilustra a comparação entre as abordagens, a qual apresenta o número de pacotes colididos na rede para cinco diferentes densidades de veículos.

Ao analisar os dados gerados pelo simulador, pôde-se observar que quanto maior a densidade de veículos na rodovia, maior a quantidade de pacotes colididos na rede (Figura 18); isto é consequência

Tabela 14: Quantidade de Pacotes Gerados e Colisões Geradas Por Cenários - Protocolo Proposto

Densidade (veículos/hora)	Pacotes Gerados	Colisões	Proporção de Colisões
1000	9863	828	8,4 %
2000	10103	1333	13,2 %
3000	18890	3060	16,2 %
4000	20239	3784	18,7 %
5000	28446	6059	21,3 %

Tabela 15: Proporção de Colisões - Broadcast Puro, AFR, APR, DECA e Protocolo Proposto

Densidade (v/h)	B. Puro	APR	AFR	P. Proposto	DECA
1000	9,1 %	10,2 %	11,5 %	8,4 %	9,8 %
2000	15,2 %	16,5 %	17,4 %	13,2 %	16,2 %
3000	18,8 %	19,7 %	20,1 %	16,2 %	19,1 %
4000	21,2 %	21,2 %	23,4 %	18,7 %	20,5 %
5000	27,8 %	30,8 %	31,1 %	21,3 %	24,9 %

do maior número de mensagens geradas por cada veículo. Observa-se também, conforme Figura 18, que o Protocolo Proposto gera uma quantidade maior de pacotes e consequentemente uma quantidade maior de colisões, frente as abordagens Broadcast Puro, AFR e APR. Isso ocorre, pois o Protocolo Proposto faz uso da troca de *beacons* para obter informações sobre os nós vigentes na rede.

A troca de informações que ocorre no Protocolo Proposto por meio da mensagem *CM* que é enviada de forma adaptativa, quanto maior for a densidade, maior será o período e caso essa densidade seja maior que o limiar, a mensagem *CM* deixa de ser propagada. O envio da mensagem *CM* acontece de forma aperiódica e também utiliza-se um *offset* para evitar que dois ou mais nós enviem mensagens de controle ao mesmo tempo. Assim, medidas como as citadas anteriormente contribuem para que a proporção de colisões frente à quantidade de mensagens geradas seja menor que a existente nas abordagens simula-

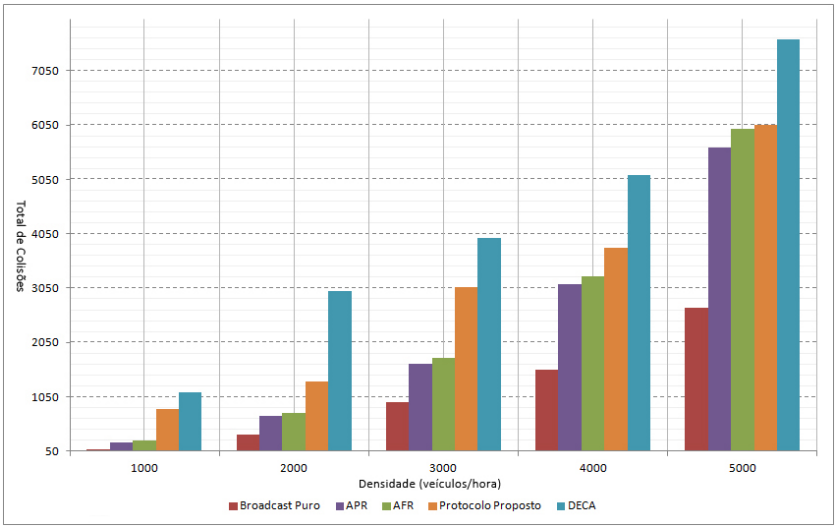

Figura 18: Total de colisões - Broadcast Puro, AFR, APR, DECA e Protocolo Proposto

das.

Dentre todas as abordagens comparadas, apenas o protocolo DECA utiliza *beacons* e fica claro que a utilização de *beacons* periódicos por parte da abordagem DECA acaba por degradar a rede, gera uma quantidade alta de mensagens de controle na rede, consequentemente uma quantidade maior de colisões. Ainda sim, o DECA obteve uma proporção menor de colisões que outras abordagens que buscam prover confiabilidade como, por exemplo AFR e APR.

Nas simulações do Protocolo Proposto no cenário com densidade de 5000 veículos/hora, apenas 21,3 % das mensagens geradas sofrem colisão, ao comparar com a abordagem AFR, pode-se verificar que a proporção de colisões diminui 9,8 % em um ambiente com alta densidade de veículos. Os mecanismos implementados no Protocolo Proposto tinham como objetivo diminuir as mensagens de controle em cenários com alta densidade, por meio da adaptabilidade, isso fica claro quando são analisados os cenários simulados, quanto maior a densidade, maior é a diferença na proporção de colisões quando comparadas as abordagens Protocolo Proposto, Broadcast Puro, AFR, APR e DECA.

Todavia, mesmo com o acréscimo de mensagens geradas e coli-

sões, os mecanismos implementados no Protocolo Proposto não prejudicam significativamente o desempenho do protocolo, visto que os veículos recebem a mensagem de alerta independentemente da densidade existente no cenário.

5.3.3 Resultado e Análise do Tempo da Entrega do Alerta Disseminado

As Tabelas 16, 17, 18 e 19 apresentam o tempo, em segundos, do atraso máximo e a distância (metros) em que um veículo recebeu pela primeira vez a mensagem de alerta sobre o evento ocorrido. Este experimento foi realizado para determinar se o atraso gerado pelos mecanismos implementados no Protocolo Proposto podem ou não influenciar no tempo para que o condutor possa tomar uma decisão com segurança. Foram simuladas as abordagens DECA, Broadcast Puro, AFR e APR afim de comparar com o Protocolo Proposto.

Tabela 16: Tempo de recebimento Mensagem de Dados (Atraso Máximo x Distância) - Cenário 5000 veículos/hora

Protocolo	**Atraso Máximo (s)**	**Distância (m)**
Broadcast Puro	2,57	2810
DECA	2,62	2886
Protocolo Proposto	2,66	2903
AFR	3,28	1650
APR	4,02	822

Neste experimento o objetivo é analisar o tempo decorrido após a criação do alerta até o recebimento deste pelos veículos participantes da rede. Pode-se perceber que o maior atraso proporcionado pelo Protocolo Proposto em todos os cenários foi 2,73 segundos e o veículo que recebeu a mensagem estava a 2891 metros da ocorrência, caso o veículo represente a Classe 1, a velocidade máxima é de 110 km/h, então o condutor do veículo terá até um minuto e meio para realizar uma mudança em sua trajetória ou frear o veículo. Ao comparar o Protocolo Proposto com as abordagens simuladas, o atraso máximo gerado pelo Protocolo Proposto é igual ao atraso máximo gerado pela abordagem DECA e superior apenas à abordagem Broadcast Puro, as abordagens AFR e APR obtiveram atrasos maiores em todos os cenários simulados.

Tabela 17: Tempo de recebimento Mensagem de Dados (Atraso Máximo x Distância) - Cenário 4000 veículos/hora

Protocolo	Atraso Máximo (s)	Distância (m)
Broadcast Puro	2,58	2809
DECA	2,67	2872
Protocolo Proposto	2,71	2899
AFR	3,32	1648
APR	4,05	819

Tabela 18: Tempo de recebimento Mensagem de Dados (Atraso Máximo x Distância) - Cenário 2000 veículos/hora

Protocolo	Atraso Máximo (s)	Distância (m)
Broadcast Puro	2,59	2809
DECA	2,71	2869
Protocolo Proposto	2,72	2893
AFR	3,37	1641
APR	4,11	817

Também fica claro que quanto maior a quantidade de veículos, menor é o atraso, isso corre, pois em cenários mais densos existem menos espaços livres nas vias, desta maneira, é formado um canal de comunicação mais estável, já em cenários mais esparsos, a comunicação fica dependente da técnica *store-and-forward* que consiste em armazenar as mensagens para uma retransmissão posterior, assim aumentando o atraso em cenários com pouca densidade.

Pode-se concluir que o Protocolo Proposto gera atraso na retransmissão das mensagens de sinalização, porém este atraso não prejudica a tomada de decisão do condutor, tendo em vista que o protocolo desenvolvido obteve o segundo menor atraso e a maior distância entre todas as abordagens estudadas.

Tabela 19: Tempo de recebimento Mensagem de Dados (Atraso Máximo x Distância) - Cenário 1000 veículos/hora

Protocolo	**Atraso Máximo (s)**	**Distância (m)**
Broadcast Puro	2,58	2808
DECA	2,73	2867
Protocolo Proposto	2,73	2891
AFR	3,41	1635
APR	4,13	815

5.3.4 Resultado e Análise do Mecanismos de Codificação de Rede

Para verificar o funcionamento do Protocolo Proposto utilizando o mecanismo de codificação de rede, a operação lógica XOR, foi definido um novo cenário, no qual foi utilizada a densidade de 3000 veículos/hora, foram mantidas as estruturas das vias e parâmetros de simulação. A principal função deste mecanismo é diminuir a quantidade de retransmissões das mensagens de dados existentes na rede veicular sem degradar a confiabilidade do protocolo. Na Tabela 20 são apresentados os cenários simulados. As simulações são iniciadas com o povoamento das listas de mensagens dos nós, na Tabela 20, por exemplo, no Cenário 1 45 % dos nós foram inicializados com o *Alerta 1* em suas listas de mensagens, 45 % dos nós foram inicializados com o *Alerta 2* em suas listas e por fim, 10 % dos nós foram inicializados com ambas as mensagens em suas listas.

Tabela 20: Cenários Simulados - Codificação de Rede

Cenários	Alerta 1	Alerta 2	Alertas 1 e 2
Cenário 1	45 %	45 %	10 %
Cenário 2	30 %	30 %	30 %
Cenário 3	20 %	20 %	60 %
Cenário 4	5 %	5 %	90 %
Cenário 5	0 %	0 %	100 %

Com as simulações buscou-se obter a quantidade de mensagens

geradas durante os 360 segundos, tanto na abordagem com o mecanismo de codificação de rede, quanto sem o mecanismo. Neste cenário não foi definido um incidente gatilho, desta forma as retransmissões tiveram inicio no momento que os nós começaram a trocar informações por meio de *beacons CM*. Na Tabela 21 é demostrada a quantidade total de retransmissões das mensagens que representam os alertas 1 e 2 e o impacto que o mecanismo gera em cada um dos cenários.

Tabela 21: Quantidade de retransmissões de Mensagens de Dados (Alerta) - Sem e Com Codificação de Rede

Cenários	S/ XOR	C/ XOR	Redução de Mensagens
Cenário 1	735	452	38,5 %
Cenário 2	512	301	41,2 %
Cenário 3	351	191	45,5 %
Cenário 4	93	41	55,9 %
Cenário 5	0	0	0 %

Na Tabela 21 pode ser observada a comparação entre o Protocolo Proposto com, e sem o mecanismo. Também pode-se observar que o mecanismo de codificação de rede prove menor quantidade de retransmissões de mensagens em comparação ao Protocolo Proposto sem o mecanismo: ao gerar o XOR de duas mensagens, o nó não precisou retransmitir os alertas *1* e *2* separadamente ao receber solicitações de ambas as mensagens no mesmo período de tempo. No Cenário 4, o mecanismo obteve melhor resultado. Isso acontece porque a porcentagem de nós com as duas mensagens em suas listas é de 90 %, desta forma serão realizadas mais operações lógicas XOR neste cenário, assim diminuindo a quantidade de retransmissões. Fica claro que, quanto maior for o número de nós com as duas mensagens em suas listas, menor será a quantidade de retransmissões no cenário. No Cenário 5 não há retransmissões de mensagens, já que todos os nós possuem ambas as mensagens, desta forma não há necessidade de retransmissões.

Por tanto, ao analisar a Tabela 21 pode-se verificar que a abordagem sem o mecanismo realiza mais que o dobro (55,9 %) de retransmissões que a abordagem com o mecanismo. Desta forma, o mecanismo atendeu seu objetivo, que é diminuir a quantidade de retransmissões geradas na rede em cenários que possuem mais de um alerta a serem disseminados.

5.4 CONSIDERAÇÕES DO CAPÍTULO

Este capítulo apresentou os resultados obtidos nos experimentos, os quais serviram para avaliar o desempenho do protocolo proposto. Os resultados dos experimentos demonstram que os impactos decorrentes das colisões, o tempo para o recebimento das mensagens e os mecanismos implementados não prejudicam o desempenho da aplicação, mesmo diante de cenários com densidades diferentes. Além disso, a eficácia do sistema pôde ser comprovada pelas simulações, uma vez que o protocolo proposto atendeu a todos os nós da rede, desta maneira é possível comprovar sua confiabilidade. Também ficou clara a eficiência do protocolo proposto diante dos cenários simulados, já que o protocolo proposto proveu a menor proporção de perdas de pacotes comparado aos outros protocolos simulados.

6 CONCLUSÕES

Um dos desafios em redes veiculares é a inserção de novos mecanismos que possam torná-las mais seguras e confiáveis, sem adicionar riscos no comprometimento de seu desempenho. Com a necessidade de prover confiabilidade às redes veiculares surgem os protocolos confiáveis que buscam oferecer um serviço de entrega de mensagens garantida, através de implementações de mecanismos de controle para que seu comportamento possa dinamicamente adaptar-se às condições observadas na rede.

O objetivo deste trabalho foi prover confiabilidade na entrega de mensagens de dados em redes veiculares, por meio de um protocolo adaptativo e eficiente que, agregado a uma arquitetura de comunicação em redes veiculares, contribui para a confiabilidade na transmissão de mensagens em cenários rodoviários. Este protocolo teve por objetivo aumentar a confiabilidade nas transmissões, mitigar problemas encontrados em abordagens que buscaram gerar confiabilidade para este cenário, a fim de proporcionar uma melhora no desempenho para as aplicações que têm como requisito crítico a entrega das mensagens em um cenário veicular. Os métodos de pesquisa utilizados foram distribuídos em três fases.

Na primeira fase, foi executado um procedimento técnico de pesquisa bibliográfica para realizar a fundamentação teórica, que abordou a área de redes veiculares, protocolos confiáveis, aplicações que utilizam redes veiculares e codificação de rede. Ainda nessa fase, foi realizada a revisão sistemática, selecionando-se e analisando-se trabalhos correlatos. Na segunda fase, o protocolo proposto foi definido e seus algoritmos, equações e mensagens foram detalhadamente descritos. Na terceira fase, o protocolo proposto e a aplicação que faz uso do protocolo foram implementados utilizando dois simuladores (rede e de tráfego) bidirecionalmente acoplados. Diferentes experimentos simulados foram realizados com o objetivo de avaliar o protocolo proposto. A análise dos resultados obtidos nas simulações juntamente com a comparação entre o protocolo proposto e outras abordagens foram realizadas nesta fase.

Com a identificação das principais características presentes nos protocolos confiáveis, com a definição do protocolo proposto e pela análise feita dos impactos do protocolo proposto e da sua eficácia, pode-se afirmar que os objetivos específicos desse trabalho foram atingidos. O protocolo proposto nesta dissertação inova em relação aos trabalhos

relacionados por ser um protocolo adaptativo que busca diminuir a quantidade de mensagens desnecessárias na rede, atrasos na entrega de mensagens e também problemas presentes em outras abordagens como, por exemplo, nó oculto.

O protocolo proposto seleciona o nó retransmissor por meio do calculo do ganho, este calculo leva em consideração a densidade local do nó e a sua proximidade da borda de comunicação. O nó com maior ganho retransmite a mensagem e também escolhe o próximo retransmissor. Na abordagem proposta neste trabalho faz-se uso de mecanismos que tornam o protocolo proposto adaptável ao cenário veicular, desta forma, a quantidade de mensagens de controle é diminuída. Em cenários com mais de uma mensagens de dados (alerta) vigente na rede, o protocolo proposto realiza a técnica de codificação de rede, a operação XOR, para diminuir a quantidade de retransmissões desnecessárias.

Com os resultados obtidos nas simulações foi possível comprovar a eficácia do protocolo proposto. A métrica utilizada para avaliar a eficácia do uso do protocolo por uma aplicação foi a taxa de mensagens entregues aos nós pertencentes a rede em diversos cenários. Os resultados demonstram também que os impactos na eficácia do protocolo proposto provenientes da implementação dos mecanismos não prejudicam os objetivos. Uma vez que todos dos veículos, independente da densidade, receberam a mensagem de alerta. Com as simulações, foi possível também comprovar a eficiência da protocolo, uma vez que mesmo com o acréscimo das colisões com o uso das mensagens de controle, todos os veículos receberam o alerta em tempo hábil para tomar decisões. Os atrasos no recebimento do alerta não prejudicaram os condutores, visto que os veículos receberam o alerta a uma distancia segura e suficiente. Apesar dos impactos e degradações provocadas pelo uso das mensagens de controle, os resultados foram superiores as abordagens correlatas estudadas e simuladas neste trabalho. Entretanto, cabe ressaltar que como em qualquer simulação as análises da eficiência e eficácia devem ser interpretadas de maneira cuidadosa, pois na prática pode haver fatores externos como interferência eletromagnética, clima, sombreamento que podem ocasionar problemas na rede veicular.

Por fim, os resultados obtidos permitiram confirmar as hipóteses de pesquisa, dado que o protocolo prove confiabilidade na entrega das mensagens, mas aumenta o tempo de processamento das mensagens e por fim, aumenta o atraso na entrega das mensagens. Também foi possível verificar que o protocolo adiciona sobrecarga de mensagens de controle em cenários com alta densidade veicular, mesmo com esta degradação todos os veículos receberam o alerta e que os atrasos para o

recebimento do alerta (impacto sobre o tempo) identificados não prejudicaram a ação dos motoristas. Contudo, de formal geral, a atuação do protocolo proposto nesta dissertação contribuí para o aumento da robustez e da eficácia na comunicação em cenários rodoviários. Estas contribuições fornecidas pela utilização dos mecanismos podem ser úteis a aplicações voltadas a segurança no transito.

6.1 CONTRIBUIÇÕES DA DISSERTAÇÃO

Dentre as principais contribuições desta dissertação podem ser destacadas as seguintes:

- Análise de mecanismos utilizados para prover confiabilidade na entrega de mensagens de dados em redes veiculares;
- Desenvolvimento de um protocolo para aplicações de segurança em rodovias que:
  - prove confiabilidade na entrega de mensagens de dados em redes veiculares;
  - diminui a quantidade de mensagens de controle em cenários com alta densidade de veículos;
  - diminui a proporção de colisões e perdas de pacotes frente a quantidade de pacotes gerados;
  - adapta o período entre transmissões de mensagens de controle de acordo com a densidade da rede; e
  - diminui a quantidade de retransmissões das mensagens de dados, tanto em cenários com apenas uma mensagem de sinalização, quanto em cenários com mais de uma mensagem de sinalização.
- Aprimoramento da aplicação desenvolvida que visa disseminar alertas em rodovias e que está integrada ao protocolo proposto.

6.2 TRABALHOS FUTUROS

Quanto a trabalhos futuros, sugere-se:

- Continuar a avaliação do protocolo proposto, através de simulações, de forma a analisar a sua eficácia diante de cenários e

densidades diferentes. A partir desta análise, desenvolver novas técnicas que possam prover confiabilidade ao protocolo em diversos cenários.

- Estender o protocolo proposto para que este possa ser adaptado (configurável) para outros tipos de aplicações de segurança no trânsito e cenários (urbano, por exemplo), através de uma interface, e com isso poder avaliar a sua integração a outras aplicações.

- Implantação de mecanismos de segurança para garantir a integridade e autenticidade das mensagens trocadas entre os nós que compõem a rede.

- Buscar novos mecanismos que possam ser empregados para que o protocolo proposto melhore seu desempenho nos cenários estudados neste trabalho.

REFERÊNCIAS

AHLSWEDE, R. et al. Network information flow. *IEEE Transactions on Information Theory*, v. 46, n. 4, p. 1204?1216, 2000.

ALSHAER, H.; HORLAIT, E. An optimized adaptive broadcast scheme for inter-vehicle communication. In: *Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st.* [S.l.: s.n.], 2005. v. 5, p. 2840 – 2844 Vol. 5. ISSN 1550-2252.

ARNOULD, G. et al. A transport based clearing system for dynamic carpooling business services. In: *ITS Telecommunications (ITST), 2011 11th International Conference on.* [S.l.: s.n.], 2011. p. 527 –533.

AUGUSTO C. H. P.; REZENDE, J. F. Escalonamento distribuído de inundações em redes ad hoc móveis. In: *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos.* Gramado, RS, Brazil: [s.n.], 2010. (SBRC '10), p. 857–870.

BALON, N.; GUO, J. Increasing broadcast reliability in vehicular ad hoc networks. In: *Proceedings of the 3rd international workshop on Vehicular ad hoc networks.* New York, NY, USA: ACM, 2006. (VANET '06), p. 104–105. ISBN 1-59593-540-1. <http://doi.acm.org/10.1145/1161064.1161088>.

BECHLER, M. et al. Efficient discovery of internet gateways in future vehicular communication systems. In: *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual.* [S.l.: s.n.], 2003. v. 2, p. 965 – 969 vol.2. ISSN 1090-3038.

BENSLIMANE, A. Localization in vehicular ad hoc networks. In: *Systems Communications, 2005. Proceedings.* [S.l.: s.n.], 2005. p. 19 –25.

BERNSEN, J.; MANIVANNAN, D. Review: Unicast routing protocols for vehicular ad hoc networks: A critical comparison and classification. *Pervasive Mob. Comput.*, v. 5, n. 1, p. 1 –18, feb. 2009. ISSN 1574-1192.

BISWAS, S.; TATCHIKOU, R.; DION, F. Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. *Communications Magazine, IEEE*, v. 44, n. 1, p. 74 –82, jan. 2006. ISSN 0163-6804.

CALISKAN, M.; GRAUPNER, D.; MAUVE, M. Decentralized discovery of free parking places. In: *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM, 2006. (VANET '06), p. 30–39. ISBN 1-59593-540-1. <http://doi.acm.org/10.1145/1161064.1161070>.

CAMBRUZZI, E. et al. Uma abordagem adaptativa para detecção de falhas em redes veiculares ad hoc. In: *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Gramado, RS, Brazil: [s.n.], 2010. (SBRC '10), p. 569–583.

CARVALHO, C. B.; REZENDE, J. F. Roteamento em redes em malha sem fio ieee 802.11 com adaptação de largura de canal. In: *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Gramado, RS, Brazil: [s.n.], 2010. (SBRC '10), p. 161–174.

CHANG, J.-M.; MAXEMCHUK, N. F. Reliable broadcast protocols. *ACM Trans. Comput. Syst.*, ACM, New York, NY, USA, v. 2, n. 3, p. 251–273, ago. 1984. ISSN 0734-2071. <http://doi.acm.org/10.1145/989.357400>.

CHEN, W.; CAI, S. Ad hoc peer-to-peer network architecture for vehicle safety communications. *Communications Magazine, IEEE*, v. 43, n. 4, p. 100 – 107, april 2005. ISSN 0163-6804.

CHISALITA, L.; SHAHMEHRI, N. A peer-to-peer approach to vehicular communication for the support of traffic safety applications. In: *Intelligent Transportation Systems, 2002. Proceedings. The IEEE 5th International Conference on*. [S.l.: s.n.], 2002. p. 336 – 341.

CHUAN, D.; JIAN, W. A reliable and efficient highway multihop vehicular broadcast model. *Communications and Networking, ISRN*, v. 2012, n. 185472, p. 8, quarter 2012.

CONSORTIUM, C. A. M. P. V. S. C. *Vehicle Safety Communications Project: Task 3 Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC*. National Highway Traffic Safety Administration, Office of Research and Development, Washington, D.C., 2005. <http://books.google.com.br/books?id=BwmMNwAACAAJ>.

CRUZ, E. et al. Performance analysis of xor-based routing in urban vehicular ad hoc networks. In: *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*. [S.l.: s.n.], 2012. p. 2521 –2525. ISSN 1525-3511.

DOEFEXI, A. et al. An evaluation of the performance of ieee 802.11a and 802.11g wireless local area networks in a corporate office environment. In: *Communications, 2003. ICC '03. IEEE International Conference on*. [S.l.: s.n.], 2003. v. 2, p. 1196 –1200 vol.2.

DOTZER, F.; FISCHER, L.; MAGIERA, P. Vars: a vehicle ad-hoc network reputation system. In: *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*. [S.l.: s.n.], 2005. p. 454–456.

DRESSLER, F. et al. Requirements and objectives for secure traffic information systems. In: *Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on*. [S.l.: s.n.], 2008. p. 808 –814.

DURRESI, M.; DURRESI, A.; BAROLLI, L. Emergency broadcast protocol for inter-vehicle communications. In: *Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference on*. [S.l.: s.n.], 2005. v. 2, p. 402 –406. ISSN 1521-9097.

ECKHOFF, D. et al. Simulative performance evaluation of the simtd self organizing traffic information system. In: *Ad Hoc Networking Workshop (Med-Hoc-Net), 2011 The 10th IFIP Annual Mediterranean*. [S.l.: s.n.], 2011. p. 79 –86.

EVANS, L. *Traffic safety and the driver*. New York, USA: Van Nostrand Reinhold, 1991. 428 p.

FASOLO, E.; ZANELLA, A.; ZORZI, M. An effective broadcast scheme for alert message propagation in vehicular ad hoc networks. In: *Communications, 2006. ICC '06. IEEE International Conference on*. [S.l.: s.n.], 2006. v. 9, p. 3960 –3965. ISSN 8164-9547.

FRAGOULI, C.; SOLJANIN, E. Network coding fundamentals. foundations and trends. *Networking*, Now Publishers Inc, 2007.

GASS, R.; SCOTT, J.; DIOT, C. Measurements of in-motion 802.11 networking. In: *Mobile Computing Systems and Applications, 2006. WMCSA '06. Proceedings. 7th IEEE Workshop on*. [S.l.: s.n.], 2006. p. 69 –74. ISSN 1550-6193.

GEISSLER, T.; SCHINDHELM, R.; LUEDEKE, A. Socio-economic assessment of the safespot cooperative systems - methodology, final assessment results and deployment conclusions. In: *Intelligent Vehicles*

Symposium (IV), 2011 IEEE. [S.l.: s.n.], 2011. p. 368 –374. ISSN 1931-0587.

GIL, A. C. *Como elaborar projetos de pesquisa*. São Paulo, Brazil: Ed. Atlas, 2002.

GOMES, P. H. et al. A queue management mechanism for improving tcp fairness in wireless access networks. In: *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Gramado, RS, Brazil: [s.n.], 2010. (SBRC '10), p. 871–884.

HARRI, J.; FILALI, F.; BONNET, C. Mobility models for vehicular ad hoc networks: a survey and taxonomy. *Communications Surveys Tutorials, IEEE*, v. 11, n. 4, p. 19–41, quarter 2009. ISSN 1553-877X.

HARTENSTEIN, H.; LABERTEAUX, K. *Vehicular Applications and Inter-Networking Technologies*. United Kingdom: Ed. Wiley, 2010. 466 p. ISBN 978-0-470-74056-9.

HEISSENBUTTEL, M. et al. Optimized stateless broadcasting in wireless multi-hop networks. In: *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*. [S.l.: s.n.], 2006. p. 1 –12. ISSN 0743-166X.

HERON, M. et al. Deaths: Preliminary data for 2006. *Division of vital statistics, National Vital Statistics Reports*, v. 56, n. 16, 2008.

IPEA. Ipea diz que gastos com acidentes de trânsito nas rodovias é de 22 bilhões de reais ao ano. *Agência Brasil*, v. 27, may 2008.

IPEA. Ipea estima custo anual com acidentes no brasil em r$ 40 bilhões. *Congresso Internacional de Trânsito*, jul 2012.

JACOBSSON, M.; GUO, C.; NIEMEGEERS, I. A flooding protocol for manets with self-pruning and prioritized retransmissions. In: *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on*. [S.l.: s.n.], 2005. p. 9 pp. –49.

JAKUBIAK, J.; KOUCHERYAVY, Y. State of the art and research challenges for vanets. In: *Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE*. [S.l.: s.n.], 2008. p. 912 –916.

KAMOLTHAM, N.; NAKORN, K.; ROJVIBOONCHAI, K. Improving reliable broadcast over asymmetric vanets based on a rssi-voting

algorithm. In: *Intelligent Signal Processing and Communications Systems (ISPACS), 2011 International Symposium on*. [S.l.: s.n.], 2011. p. 1 –6.

KARGL, F.; PAPADIMITRATOS, P. Acm wisec 2011 poster and demo session. *ACM SIGMOBILE Mobile Computing and Communications Review*, ACM, New York, NY, USA, v. 15, p. 34–34, 07/2011 2011. ISSN 1559-1662. <http://doi.acm.org/10.1145/2073290.2073296>.

KHAN, A.; STOJMENOVIC, I.; ZAGUIA, N. Parameterless broadcasting in static to highly mobile wireless ad hoc, sensor and actuator networks. In: *Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on*. [S.l.: s.n.], 2008. p. 620–627. ISSN 1550-445X.

KORKMAZ, G. et al. Urban multi-hop broadcast protocol for inter-vehicle communication systems. In: *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM, 2004. (VANET '04), p. 76–85. ISBN 1-58113-922-5. <http://doi.acm.org/10.1145/1023875.1023887>.

KOSCH, T. Local danger warning based on vehicle ad-hoc networks: Prototype and simulation. In: *Proceedings of 1st International Workshop on Intelligent Transportation (WIT),2004*. [S.l.: s.n.], 2004.

KOSCH, T. Technical Concept and Prerequisites of Car-to-Car Communication. In: *ITS Europe*. Hannover: [s.n.], 2005.

KOUBEK, M.; REA, S.; PESCH, D. Reliable broadcasting for active safety applications in vehicular highway networks. In: *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st*. [S.l.: s.n.], 2010. p. 1 –5. ISSN 1550-2252.

LAKATOS, E. M.; MARCONI, M. A. *Fundamentos de Metodologia Científica*. São Paulo, Brazil: Ed. Atlas, 2000.

LAOUITI, A.; MUHLETHALER, P.; TOOR, Y. Reliable opportunistic broadcast in vanets (r-ob-van). In: *Intelligent Transport Systems Telecommunications,(ITST),2009 9th International Conference on*. [S.l.: s.n.], 2009. p. 382 –387.

LI, F.; WANG, Y. Routing in vehicular ad hoc networks: A survey. *Vehicular Technology Magazine, IEEE*, v. 2, n. 2, p. 12 –22, june 2007. ISSN 1556-6072.

LIN, X. et al. Gsis: A secure and privacy-preserving protocol for vehicular communications. *Vehicular Technology, IEEE Transactions on*, v. 56, n. 6, p. 3442 –3456, nov. 2007. ISSN 0018-9545.

LIU, P.; XU, Z. Temporal diversity assisted blind channel estimation for downlink long-code cdma systems. In: *Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04). IEEE International Conference on*. [S.l.: s.n.], 2004. v. 4, p. iv – 953–6 vol.4. ISSN 1520-6149.

LUNDGREN, H.; NORDSTRö, E.; TSCHUDIN, C. Coping with communication gray zones in ieee 802.11b based ad hoc networks. In: *Proceedings of the 5th ACM international workshop on Wireless mobile multimedia*. New York, NY, USA: ACM, 2002. (WOWMOM '02), p. 49–55. ISBN 1-58113-474-6. <http://doi.acm.org/10.1145/570790.570799>.

MITROPOULOS, G. et al. Wireless local danger warning: Cooperative foresighted driving using intervehicle communication. *Intelligent Transportation Systems, IEEE Transactions on*, v. 11, n. 3, p. 539 –553, sept. 2010. ISSN 1524-9050.

NADEEM, T. et al. Trafficview: traffic data dissemination using car-to-car communication. *SIGMOBILE Mob. Comput. Commun. Rev.*, ACM, New York, NY, USA, v. 8, n. 3, p. 6–19, jul. 2004. ISSN 1559-1662. <http://doi.acm.org/10.1145/1031483.1031487>.

NAGARAJ, U.; DHAMAL, P. Broadcasting routing protocols in vanet. *Network and Complex Systems, IISTE*, v. 1, n. 2, p. 13 – 19, 2011. ISSN 2225-0603.

NAKORN, K. N.; ROJVIBOONCHAI, K. Comparison of reliable broadcasting protocols for vehicular ad-hoc networks. In: *Communication Technology (ICCT), 2010 12th IEEE International Conference on*. [S.l.: s.n.], 2010. p. 1168 –1171.

NAUMOV, V.; BAUMANN, R.; GROSS, T. An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces. In: *Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing*. New York, NY, USA: ACM, 2006. (MobiHoc '06), p. 108–119. ISBN 1-59593-368-9. <http://doi.acm.org/10.1145/1132905.1132918>.

NAUMOV, V.; GROSS, T. Connectivity-aware routing (car) in vehicular ad-hoc networks. In: *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. [S.l.: s.n.], 2007. p. 1919 –1927. ISSN 0743-166X.

NEKOVEE, M.; BOGASON, B. Reliable and effcient information dissemination in intermittently connected vehicular adhoc networks. In: *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*. [S.l.: s.n.], 2007. p. 2486 –2490. ISSN 1550-2252.

NI, S.-Y. et al. The broadcast storm problem in a mobile ad hoc network. In: *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*. New York, NY, USA: ACM, 1999. (MobiCom '99), p. 151–162. ISBN 1-58113-142-9. <http://doi.acm.org/10.1145/313451.313525>.

OHTA, T.; INOUE, S.; KAKUDA, Y. An adaptive multihop clustering scheme for highly mobile ad hoc networks. In: *Autonomous Decentralized Systems, 2003. ISADS 2003. The Sixth International Symposium on*. [S.l.: s.n.], 2003. p. 293 – 300.

OLIVEIRA, R. et al. Towards the use of xor-based routing protocols in vehicular ad hoc networks. In: *Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd*. [S.l.: s.n.], 2011. p. 1 –6. ISSN 1550-2252.

OSAFUNE, T.; LIN, L.; LENARDI, M. Multi-hop vehicular broadcast (mhvb). In: *ITS Telecommunications Proceedings, 2006 6th International Conference on*. [S.l.: s.n.], 2006. p. 757 –760.

OSTERMAIER, B.; DOTZER, F.; STRASSBERGER, M. Enhancing the security of local dangerwarnings in vanets - a simulative analysis of voting schemes. In: *Proceedings of the The Second International Conference on Availability, Reliability and Security*. Washington, DC, USA: IEEE Computer Society, 2007. (ARES '07), p. 422–431. ISBN 0-7695-2775-2. <http://dx.doi.org/10.1109/ARES.2007.79>.

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

PANAYAPPAN, R. et al. Vanet-based approach for parking space availability. In: *Proceedings of the fourth ACM international*

workshop on Vehicular ad hoc networks. New York, NY, USA: ACM, 2007. (VANET '07), p. 75–76. ISBN 978-1-59593-739-1. <http://doi.acm.org/10.1145/1287748.1287763>.

PANDAZIS, J.-C. ecomove: Cooperative its for green mobility. *European Wireless, 2012. EW. 18th European Wireless Conference*, p. 1 –5, april 2012.

PAPADIMITRATOS, P. et al. Secure vehicular communication systems: design and architecture. *Communications Magazine, IEEE*, v. 46, n. 11, p. 100 –109, november 2008. ISSN 0163-6804.

PASSOS, D.; ALBUQUERQUE, C. Implementação e análise prática de desempenho do mecanismo mara em redes em malha sem fio. In: *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Gramado, RS, Brazil: [s.n.], 2010. (SBRC '10), p. 885–898.

PAULA, W.; OLIVEIRA, S.; NOGUEIRA, J. Um mecanismo de reputação para redes veiculares tolerantes a atrasos e desconexões. In: *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Gramado, RS, Brazil: [s.n.], 2010. (SBRC '10), p. 545–550.

PUNZO, V.; CIUFFO, B. Integration of driving and traffic simulation: Issues and first solutions. *Intelligent Transportation Systems, IEEE Transactions on*, v. 12, n. 2, p. 354–363, june 2011. ISSN 1524-9050.

RAYA, M.; HUBAUX, J.-P. The security of vehicular ad hoc networks. In: *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*. New York, NY, USA: ACM, 2005. (SASN '05), p. 11–21. ISBN 1-59593-227-5. <http://doi.acm.org/10.1145/1102219.1102223>.

REICHARDT, D. et al. Cartalk 2000: safe and comfortable driving based upon inter-vehicle-communication. In: *Intelligent Vehicle Symposium, 2002. IEEE*. [S.l.: s.n.], 2002. v. 2, p. 545 – 550 vol.2.

REUMERMAN, H.-J.; ROGGERO, M.; RUFFINI, M. The application-based clustering concept and requirements for intervehicle networks. *Communications Magazine, IEEE*, v. 43, n. 4, p. 108 – 113, april 2005. ISSN 0163-6804.

RIZVI, S. et al. A novel approach to reduce traffic chaos in emergency and evacuation scenarios. In: *Vehicular Technology Conference, 2007.*

VTC-2007 Fall. 2007 IEEE 66th. [S.l.: s.n.], 2007. p. 1937 –1941. ISSN 1090-3038.

ROS, F.; RUIZ, P.; STOJMENOVIC, I. Reliable and efficient broadcasting in vehicular ad hoc networks. In: *Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th.* [S.l.: s.n.], 2009. p. 1 –5. ISSN 1550-2252.

SARAVANAN, K.; THANGAVELU, A.; RAMESHBABU, K. A middleware architectural framework for vehicular safety over vanet (invanet). In: *Networks and Communications, 2009. NETCOM '09. First International Conference on.* [S.l.: s.n.], 2009. p. 277 –282.

SICHITIU, M.; KIHL, M. Inter-vehicle communication systems: a survey. *Communications Surveys Tutorials, IEEE*, v. 10, n. 2, p. 88 –105, quarter 2008. ISSN 1553-877X.

SOMMER, C.; DRESSLER, F. Progressing toward realistic mobility models in vanet simulations. *Communications Magazine, IEEE*, v. 46, n. 11, p. 132 –137, november 2008. ISSN 0163-6804.

TAHA, M.; HASAN, Y. M. Y. Vanet-dsrc protocol for reliable broadcasting of life safety messages. In: *Signal Processing and Information Technology, 2007 IEEE International Symposium on.* [S.l.: s.n.], 2007. p. 104–109.

TAMPERE, C.; AREM, B. van. Traffic flow theory and its applications in automated vehicle control: a review. In: *Intelligent Transportation Systems, 2001. Proceedings. 2001 IEEE.* [S.l.: s.n.], 2001. p. 391–397.

TANG, K.; GERLA, M. Mac reliable broadcast in ad hoc networks. In: *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE.* [S.l.: s.n.], 2001. v. 2, p. 1008 – 1013 vol.2.

TONGUZ, O. et al. Broadcasting in vanet. In: *2007 Mobile Networking for Vehicular Environments.* [S.l.: s.n.], 2007. p. 7 –12.

TOULMINET, G.; BOUSSUGE, J.; LAURGEAU, C. Comparative synthesis of the 3 main european projects dealing with cooperative systems (cvis, safespot and coopers) and description of coopers demonstration site 4. In: *Intelligent Transportation Systems, 2008. ITSC 2008. 11th International IEEE Conference on.* [S.l.: s.n.], 2008. p. 809 –814.

VARGA, A. *The OMNeT++ discrete event simulation system*. Junho 2013. <http://www.omnetpp.org>. Acessado em 11 mar. 2013.

WEI, M.-H.; WANG, K.; HSIEH, Y.-L. A reliable routing scheme based on vehicle moving similarity for vanets. In: *TENCON 2011 - 2011 IEEE Region 10 Conference*. [S.l.: s.n.], 2011. p. 426 –430. ISSN 2159-3442.

WEIL, T. Service management for its using wave (1609.3) networking. In: *GLOBECOM Workshops, 2009 IEEE*. [S.l.: s.n.], 2009. p. 1 –6.

WILLKE, T.; TIENTRAKOOL, P.; MAXEMCHUK, N. A survey of inter-vehicle communication protocols and their applications. *Communications Surveys Tutorials, IEEE*, v. 11, n. 2, p. 3 –20, quarter 2009. ISSN 1553-877X.

XIE, J. et al. Improving the reliability of ieee 802.11 broadcast scheme for multicasting in mobile ad hoc networks. In: *Wireless Communications and Networking Conference, 2005 IEEE*. [S.l.: s.n.], 2005. v. 1, p. 126 – 131 Vol. 1. ISSN 1525-3511.

XU, K.; GERLA, M. A heterogeneous routing protocol based on a new stable clustering scheme. In: *MILCOM 2002. Proceedings*. [S.l.: s.n.], 2002. v. 2, p. 838 – 843 vol.2.

XU, Q. et al. Vehicle-to-vehicle safety messaging in dsrc. In: *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM, 2004. (VANET '04), p. 19–28. ISBN 1-58113-922-5. <http://doi.acm.org/10.1145/1023875.1023879>.

YEUNG, R. W.; CAI, N. Network error correction, part i: Basic concepts and upper bounds. *Commun. in Inf. and Systems*, v. 6, n. 1, p. 19?36, 2006. ISSN 1018-4864.

YI, C.-W. et al. Streetcast: An urban broadcast protocol for vehicular ad-hoc networks. In: *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st*. [S.l.: s.n.], 2010. p. 1 –5. ISSN 1550-2252.

ZANELLA, A.; PIEROBON, P.; MERLIN, S. On the limiting performance of broadcast algorithms over unidimensional ad-hoc radio networks. In: *WPMC 2004. Proceedings*. [S.l.: s.n.], 2004. v. 2, p. 165 – 169 vol.2.

ZEADALLY, S. et al. Vehicular ad hoc networks (vanets): status, results, and challenges. *Telecommunication Systems*, Springer US, p. 1–25, 2010. <http://dx.doi.org/10.1007/s11235-010-9400-5>.

ZHANG, J.; ZHANG, Q.; JIA, W. A novel mac protocol for cooperative downloading in vehicular networks. In: *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*. [S.l.: s.n.], 2007. p. 4974 –4978.

ZHANG, Z. et al. Dual xor in the air: A network coding based retransmission scheme for wireless broadcasting. In: *Communications (ICC), 2011 IEEE International Conference on*. [S.l.: s.n.], 2011. p. 1 –6. ISSN 1550-3607.

ZHAO, J.; CAO, G. Vadd: Vehicle-assisted data delivery in vehicular ad hoc networks. *Vehicular Technology, IEEE Transactions on*, v. 57, n. 3, p. 1910 –1922, may 2008. ISSN 0018-9545.

APÊNDICE A – Revisão Sistemática

Uma revisão sistemática de literatura é um meio para identificar, interpretar e avaliar todos os resultados relevantes de uma pesquisa acerca de uma questão, área ou fenômeno em particular. Utilizando uma metodologia rigorosa e que possa ser reproduzida posteriormente. A revisão sistemática tem por objetivo apresentar uma avaliação concisa a respeito de um tópico (KITCHENHAN, 2009).

A primeira atividade desta revisão sistemática será a definição de um protocolo, que visa levantar a literatura relevante acerca do tema sobre protocolos confiáveis para redes veiculares. O escopo da pesquisa é voltado para a identificação de técnicas utilizadas para prover confiabilidade na disseminação de informação em redes veiculares.

A.1 OBJETIVO

Executar uma revisão sistemática tendo como objetivo identificar, analisar e avaliar os trabalhos encontrados na literatura que utilizam mecanismos para prover confiabilidade na disseminação de informação em redes móveis *ad hoc*, entre estas as redes veiculares.

A.1.1 Formulação da Questão de Pesquisa

- Questão Principal: Quais mecanismos podem prover confiabilidade a protocolos voltados a disseminação de informação em redes veiculares?
- Questão Adicional 1: Quais os impactos decorrentes do uso destes mecanismos na entrega das mensagens (eficácia) e no tempo para entrega dos alertas (eficiência)?

A.1.2 Intervenção (O que será investigado?)

- Questão Principal: A utilização do protocolo proposto é capaz de prover confiabilidade na entrega das mensagens?
- Questão Adicional 1: Confiabilidade na entrega dos pacotes, número de colisões e impacto na eficácia e eficiência do protocolo.
- Resultados: (1) Definir e implementar um protocolo para prover confiabilidade na entrega de mensagens para aplicações voltadas

à rodovias com simuladores de redes e de tráfego bidirecionalmente acoplados. (2) avaliação da eficácia do protocolo proposto e dos impactos decorrentes dos mecanismos implementados através de simulações realizadas em diferentes cenários de densidade de veículos, e (3) as análises dos resultados experimentais obtidos.

•Contexto: Protocolo confiável para redes veiculares.

A.2 ESTRATÉGIA DE BUSCA

A.2.1 Termos de Busca

•Em português: (Protocolo confiável OR Vanets) AND (Disseminação confiável OR Vanets)

•Em inglês: (*Reliable Protocol* OR Vanets) AND (*Reliable Broadcast* OR Vanets)

A.2.2 Fontes

•Google acadêmico: http://scholar.google.com.br

•IEEEExplore: http://ieeexplore.ieee.org

•SpringerLink: http://springerlink.com

•CAPES: http://www.periodicos.capes.gov.br

A.3 CRITÉRIOS E PROCEDIMENTOS PARA A SELEÇÃO

A.3.1 Critérios de seleção de fontes

•Artigos publicados entre 01/01/2000 e 30/10/2013;

•Disponibilidade de consultas de artigos através da WEB;

•Presença de mecanismos de busca através de palavras chaves;

A.3.2 Métodos de busca de fontes

As fontes serão acessadas via web.

A.3.3 Idiomas dos artigos

Inglês e português.

A.3.4 Critérios de Inclusão e Exclusão

Os trabalhos serão filtrados a partir dos seguintes critérios:

- Análise do título do trabalho;
- Pela análise do resumo e conclusões do trabalho;
- Pela data de publicação do trabalho;

A.3.5 Critérios para a inclusão de estudos

- Para a questão primária: Serão incluídos no estudo trabalhos nos quais títulos e resumos contenham informações referentes a obtenção de confiabilidade na disseminação de informação em redes veiculares por meio de mecanismos implementados. A conclusão será analisada para verificar a contribuição do trabalho. A data de publicação do trabalho deve ser superior ou igual ao ano de 20XX.
- Para a questão secundária: Os mesmos critérios utilizados na questão primária, porém o título e resumo devem conter a informação sobre confiabilidade na disseminação de informação em redes veiculares.

A.3.6 Critérios para a exclusão de estudos

- Para a questão primária: Serão excluídos do estudo trabalhos cujos títulos e resumos sejam conflitantes, ou seja, o título remete a um assunto enquanto o resumo remete a outro assunto.

- Para a questão secundária: Os mesmos critérios adotados na questão primária além de que o título e o resumo não estiverem informando sobre confiabilidade na disseminação de informação em redes veiculares.

A.3.7 Processo de seleção dos estudos primários

- Processo de seleção preliminar: As estratégias de pesquisa serão aplicadas para identificar os estudos primários potenciais. Caso um trabalho não atenda aos critérios de inclusão e também não atenda aos critérios de exclusão, este será incluído.

- Processo de seleção final: Cópias dos trabalhos incluídos como resultados da pesquisa inicial serão revisados. Esta revisão conclui a seleção de trabalhos a serem incluídos no processo de extração de dados.

A.3.8 Critérios de Qualidade e Avaliação da Qualidade dos Estudos

Os estudos foram avaliados em sua qualidade abordando os seguintes aspectos:

- Objetivos: Os trabalhos devem ter como objetivos o desenvolvimento de protocolo com a finalidade de prover confiabilidade na entrega de mensagens em cenários veiculares.

- Condução: O sistema deve, preferencialmente, possuir uma etapa experimental e ser bem referenciado.

- Experimentos: Que possua resultados obtidos através de implementação.

A.3.9 Estratégia para a extração de informação

Para cada artigo aprovado pelo processo de seleção completo, tanto para a questão primária quanto para a questão secundária, foram extraídos os seguintes dados:

- Informação para referência bibliográfica;

- Tipo de artigo: teórico, experimental ou ambos;
- Problema alvo;
- Solução proposta;
- Metodologia ou materiais utilizados;
- Resultados obtidos;
- Métricas de avaliação;
- Problemas em aberto;

A.3.10 Síntese dos dados extraídos

Os resultados foram organizados em tabelas. A partir da tabulação dos dados, foram extraídos os dados.

APÊNDICE B – Aplicações que utilizam redes veiculares

- **CCA (*Cooperative Collision Avoidance*)**: aplicação desenvolvida para evitar colisões utilizando uma abordagem cooperativa. Seu funcionamento consiste no envio de mensagens em múltiplos saltos, alertando aos condutores da ocorrência de uma situação de emergência. Pode ser utilizada também nas situações em que o motorista não possui visão dos veículos à sua frente, como nos casos de neblina ou chuva intensa (BISWAS; TATCHIKOU; DION, 2006).

- **CarTALK 2000**: projeto inicializado em agosto de 2001 com o objetivo de projetar, testar e avaliar sistemas para segurança no trânsito, utilizando comunicação entre veículos e entre os veículos e a infraestrutura. As aplicações desenvolvidas neste projeto foram divididas em três grupos: as direcionadas a prover informações e alertas aos condutores, as focadas em comunicação baseada em controle longitudinal e as voltadas à assistência cooperativa (REICHARDT et al., 2002).

- **TrafficView**: nesta aplicação, os veículos guardam informações sobre sua posição e velocidade, além das informações enviadas de outros nós da rede. Cada nó espalha todas as informações conhecidas apenas aos nós vizinhos, que de forma periódica repetem a mesma operação. Estas informações são enviadas e quando um automóvel recebe, este verifica e grava estas informações em uma base de dados, mas antes de armazenar estas informações a aplicação verifica se estas informações já existem, caso as informações recebidas já estejam armazenadas, estas são descartadas. As informações armazenadas passam por um módulo de interface de usuário (NADEEM et al., 2004).

- **VSC (*Vehicle Safety Communications*)**: desenvolvido nos Estados Unidos em 2005, uniu montadoras como a Toyota, General Motors (GM), Honda, Mercedes-Benz, Ford, além de instituições governamentais para identificar aplicações de segurança e levantar seus requisitos. O projeto pretende usar estas aplicações para aumentar a segurança das rodovias, diminuir congestionamentos, diminuir a poluição do ar e consumo de energia. Esse projeto utiliza a frequência 5,9 Ghz DSRC e o padrão 802.11p para a comunicação entre veículos (CONSORTIUM, 2005).

- **eCoMove:** de acordo com Pandazis (2012), esse projeto prevê a redução de consumo de combustível no transporte rodoviário

em 20% através da aplicação de tecnologias de informação e comunicação. Sua comunicação cooperativa é baseada nas mais recentes normas internacionais utilizadas para suportar aplicações inovadoras de mobilidade verde. A plataforma de comunicação eCoMove é baseada em resultados de projetos anteriores como o SAFESPOT (TOULMINET; BOUSSUGE; LAURGEAU, 2008) descrito a seguir.

- **InVANET (*Intelligent vehicular ad-hoc networks*):** projeto destinado ao desenvolvimento de aplicações voltadas a segurança no trânsito. O InVANET é baseado na cooperação entre ECUs, sensores e dispositivos de comunicação sem fio (WiFi/WiMax) (SARAVANAN; THANGAVELU; RAMESHBABU, 2009).

- **SAFESPOT:** projeto destinado a desenvolver e avaliar aplicações classificadas como Assistentes de Margem de Segurança (do inglês *Safety Margin Assistant* - SMA), que estende as informações de segurança à disposição dos condutores em termos de tempo e espaço. O SMA leva em conta situações potencialmente perigosas que ocorrem em um segmento especifico da rodovia, capacidades dinâmicas do veículo e o estado da via, bem como a capacidade do condutor em gerenciar manobras de emergência. O SMA visa aumentar a percepção do condutor em relação ao perigo próximo e também tornar a condução mais segura (GEISSLER; SCHINDHELM; LUEDEKE, 2011).

- **PRESERVE (*Preparing Secure Vehicle-to-X Communication Systems*)**: o objetivo do projeto PRESERVE é trazer segurança e privacidade a comunicação veicular, fornecendo segurança e privacidade para subsistemas voltados as redes veiculares. o projeto PRESERVE combina e estende os resultados de projetos de pesquisas anteriores, integrando-os e os desenvolvendo para que sejam implementados em maior escala, reduzindo os custos e os problemas enfrentados para que estes projetos sejam comercializados (KARGL; PAPADIMITRATOS, 2011). Como resultado, o projeto pretende apresentar um completo subsistema de segurança escalável e de baixo custo para redes veiculares. Segundo Kargl e Papadimitratos (2011) PRESERVE está próximo de ser comercializado e já existem outros projetos interessados em colaborar.