UM MECANISMO DE REPUTAÇÃO PARA REDES VEICULARES TOLERANTES A ATRASOS E DESCONEXÕES

WELLINGTON PASSOS DE PAULA

Orientador: José Marcos Silva Nogueira

UM MECANISMO DE REPUTAÇÃO PARA REDES VEICULARES TOLERANTES A ATRASOS E DESCONEXÕES

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Minas Gerais como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação.

Belo Horizonte

Dezembro de 2009

Paula, Wellington Passos de
P324m Um mecanismo de reputação para redes veiculares tolerantes a atrasos e desconexões / Wellington Passos de Paula. — Belo Horizonte, 2009
xx, 72 f. : il. ; 29cm

Dissertação (mestrado) — Universidade Federal de Minas Gerais
Orientador: José Marcos Silva Nogueira

1. Redes de computação - segurança - teses. 2. Redes de computação - medidas de segurança - teses. 3. VANETs - teses. 4. DTN - teses. I. Título.

CDU 519.6*22(043)

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

FOLHA DE APROVAÇÃO

Um mecanismo de reputação para redes veiculares tolerantes a atrasos e desconexões

WELLINGTON PASSOS DE PAULA

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

PROF. JOSÉ MARCOS SILVA NOGUEIRA - Orientador
Departamento de Ciência da Computação - UFMG

PROF. SÉRGIO DE OLIVEIRA - Co-orientador
Universidade Federal de São João - UFSJ

PROF. ANTONIO ALFREDO FERREIRA LOUREIRO
Departamento de Ciência da Computação - UFMG

DRA. MICHELE NOGUEIRA LIMA
Pesquisadora associada - LIP6/UPMC - França

Belo Horizonte, 22 de dezembro de 2009.

Dedico este trabalho àquela que sempre foi meu maior exemplo e fonte de inspiração, minha mãe Maria Cecília.

Agradecimentos

A Deus, por se fazer tão presente em minha vida, me iluminando e permitindo que eu alcance coisas jamais sonhadas.

À minha mãe, por me ensinar que valores como trabalho, esforço, humildade e perseverança sempre serão recompensados, por todo o amor que sempre me dedicou e por abrir mão de muitos de seus sonhos para que os meus se tornassem realidade.

À Amanda, por entender minha ausência, pelo apoio nos momentos de fraqueza, pela presença nos momentos de alegria, mas, sobretudo, por ser alguém tão especial em minha vida e me dar a honra de fazer parte da sua.

Aos meus orientadores José Marcos e Sérgio, pela compressão com o fato de eu trabalhar durante o mestrado e principalmente por todo o comprometimento e atenção que sempre tiveram com meu trabalho, possibilitando assim que ele se tornasse realidade.

Ao pessoal do ATM, pela amizade e pelos divertidos almoços na Química e no CDTN, além é claro das inúmeras soluções simples e diretas que me economizaram horas e horas de trabalho.

Ao Thiago, por ser meu "representante" em BH, meu companheiro em longas e variadas conversas, mas, sobretudo, por ser um quase irmão pra mim.

A todos os meus amigos que, mesmo cansados da recorrente desculpa: "Hoje não posso, preciso trabalhar no mestrado!", nunca desistiram de mim.

À Gerdau Açominas, por me apoiar durante a realização do mestrado, fato determinante para que esse dia se tornasse realidade.

A todos vocês, meu Muito Obrigado!

"Seja você quem for, seja qual for a posição social que você tenha na vida,
a mais alta ou a mais baixa, tenha sempre como meta muita força,
muita determinação e sempre faça tudo com muito amor
e com muita fé em Deus, que um dia você chega lá.
De alguma maneira você chega lá."
(Ayrton Senna da Silva)

Resumo

Redes *Ad Hoc* Veiculares (VANETs) constituem um novo paradigma na computação móvel, com muitas aplicações em potencial. Dentre as possibilidades, destacam-se aplicações nas quais usuários da rede trocam informações sobre as condições de tráfego e a ocorrência de eventos de risco nas vias, como por exemplo, o acúmulo de óleo em determinado ponto de uma pista. Todavia, em cenários cooperativos como esses, existe sempre o risco de algum membro condicionar seu comportamento aos seus objetivos pessoais, em detrimento do interesse geral, o que pode causar graves acidentes, uma vez que informações erradas podem ser utilizadas nos processos de decisão executados pelos veículos. Logo, surge a necessidade de desenvolvimento de mecanismos de segurança capazes de permitir aos participantes da rede validar a confiabilidade de dados recebidos. Este trabalho apresenta um mecanismo de reputação para VANETs, denominado RMDTV (*Reputation Mechanism for Delay Tolerant Vehicular Networks*), no qual membros da rede qualificam outros membros responsáveis pelo envio de informações corretas. As qualificações emitidas são enviadas pela rede em direção ao seu destino. Todavia, como os veículos em uma VANET podem ser submetidos a momentos de desconexão total, ocasionados, por exemplo, por sua alta mobilidade, optou-se pelo uso dos conceitos de Redes Tolerantes a Atrasos e Interrupções (DTNs) para o suporte a essas situações. Uma vez recebidas, elas são adicionadas por seus portadores a todas as mensagens geradas, com o intuito de atestar sua confiabilidade. Assim, membros da rede podem verificar previamente a confiabilidade de novos vizinhos, antes mesmo da troca de dados. Resultados de simulações mostram que o RMDTV aumenta consideravelmente a qualidade das decisões tomadas pelos membros de uma VANET na qual são trocadas informações sobre o estado do tráfego na via de deslocamento, mesmo com a presença de uma grande quantidade de nós maliciosos.

Abstract

Vehicular Ad Hoc Networks (VANETs) constitute a new paradigm on mobile computing with many potential applications. Among the possibilities, we can highlight security applications in which network users can exchange information about the traffic conditions and the occurrence of risk events in the roads such as the oil accumulation in determined point of a track. However, in cooperative scenarios like those, there is always the risk of user's behavior be conditioned by their personal objectives instead of the general interest. Because of this, serious accidents may happen once wrong information can be used in the decision process executed by the vehicles. Therefore, the development of security mechanisms is necessary to validate data's reliability received by network participants. This work presents a reputation mechanism for VANETs, called RMDTV (Reputation Mechanism for Delay Tolerant Vehicular Networks). Through this mechanism, network members qualify other members responsible for sending correct information. The emitted qualifications are sent towards their destiny by the network. However, as the VANET's vehicles can be exposed to total connectionless moments, caused, for example, by their high mobility, we have chosen the Delay Tolerant Networks (DTNs) concepts to support such situations. Once received, they are added to all generated messages by their carriers in intention of attesting their reliability. Thus, network users can previously verify the new neighbors' reliability, even before data is exchanged. Simulation results show that RMDTV considerably increases the quality of taken decisions by members of a VANET exchanging information about the traffic conditions on the road, even in the presence of a great amount of malicious nodes.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Nos últimos anos, redes de computadores com e sem fio têm possibilitado a conexão de diversos tipos de dispositivos como PC's, PDA's e celulares, mesmo existindo uma grande distância entre eles. Nos cenários de comunicação sem fio, as redes *ad hoc* móveis (*Mobile Ad Hoc Networks* - MANETs) têm sido foco de muitos estudos. As redes *ad hoc* veiculares (*Vehicular Ad Hoc Networks* - VANETs) são um dos tipos de redes MANETs mais estudados, devido aos seus desafios e às suas inúmeras aplicações, como por exemplo, a troca de mensagens informando condições de tráfego ou outras situações de risco possivelmente existentes na via de deslocamento.

Embora em VANETs sejam empregados dispositivos mais poderosos que aqueles comumente utilizados nas MANETs, os quais possuem grande capacidade de comunicação e, geralmente, energia ilimitada, membros de VANETs podem ser submetidos a momentos de desconexão total, ocasionados, por exemplo, por sua alta mobilidade ou mesmo pelas variações do meio físico sem fio. Assim, soluções propostas para essas redes precisam levar em consideração a existência dessas situações. O conceito de redes tolerantes a falhas e desconexões (*Delay and Disruption Tolerant Networks* - DTN's) [Fall, 2003] surge então como uma solução para possibilitar a comunicação em cenários nos quais a conectividade entre os membros é intermitente ou existem grandes atrasos.

Além de considerar possíveis momentos de desconexão na rede, outro fator crítico para o sucesso de aplicações em VANETs é o comportamento de membros da rede. Nesses tipos de cenários, nos quais existem trocas de informações entre tais membros, existe sempre o risco de algum deles agir de modo egoísta, ou seja, condicionar seu comportamento de acordo com seus interesses pessoais, em detrimento do interesse geral.

Logo, visando minimizar as consequências de comportamentos desse tipo e consequentemente, aumentar a segurança das redes como um todo, soluções que motivem a cooperação e honestidade de seus membros tornam-se necessárias [Dotzer et al., 2005].

Mecanismos de reputação contribuem com esse objetivo na medida em que permitem aos membros da rede decidir em quem confiar antes mesmo do início da troca de dados [Swamynathan et al., 2007]. Esses sistemas assumem que o comportamento antigo de um membro indica de forma bem confiável seu comportamento futuro.

Porém, nas redes veiculares, a constante mobilidade de seus membros em altas velocidades diminui muito as oportunidades de conexão por eles experimentadas. Assim, tais oportunidades devem ser usadas, majoritariamente, para a troca de dados, o que dificulta a troca de informações de reputação entre eles. Dessa forma, a melhor maneira de definir a reputação de um membro seria ele próprio guardar seus dados de reputação, desde que a integridade dessas informações possa ser garantida.

Neste trabalho é proposto um mecanismo de reputação que faz uso de qualificações emitidas por terceiros. Dessa maneira, toda vez que um membro tem uma experiência de comunicação positiva com outro membro, uma qualificação é emitida e assinada pelo primeiro, dificultando assim alterações posteriores. Tal qualificação é encaminhada pela rede, mesmo sob condições de desconectividade, até encontrar seu destino. As qualificações recebidas são então adicionadas por seus portadores às mensagens de dados por eles geradas, com o objetivo de atestar sua confiabilidade.

1.1 Objetivos

Este trabalho tem como objetivo a proposição e análise de um mecanismo de reputação que permita aos membros da rede avaliar previamente a confiabilidade de novos vizinhos, antes mesmo da realização de uma transação. Isso é feito através do uso de qualificações emitidas por terceiros confiáveis, atestando a confiabilidade de seu portador. Como cada qualificação emitida deve ser encaminhada pela rede em direção a seu destino, objetivamos também que o mecanismo proposto seja capaz de suportar os possíveis períodos de desconexão experimentados pelos nós intermediários no caminho percorrido por essas qualificações entre origem e destino.

1.2 Contribuições

O estudo do problema de confiabilidade das informações recebidas em aplicações de segurança em redes veiculares, o desenvolvimento e a avaliação de mecanismo de reputação resiliente a interrupções de comunicação trazem as seguintes contribuições:

- Concepção de um mecanismo de reputação para redes veiculares tolerantes a atrasos e desconexões, denominado RMDTV, que permite aos membros de rede

tomar decisões sobre eventos existentes na via, com base nas mensagens recebidas informando as condições dos referidos eventos, de forma mais segura. Esse protocolo faz uso de qualificações anexadas às mensagens geradas, as quais atestam a confiabilidade da origem dos dados.

- Implementação do mecanismo proposto utilizando o simulador Opportunistic Network Environment (ONE) que permite simular redes nas quais a conectividade é intermitente.

- Avaliação do desempenho do mecanismo proposto, em relação a parâmetros como quantidade de intrusos e diferentes extensões das regiões geográficas de um evento. Foi analisada também a escalabilidade do mecanismo e a sobrecarga adicionada por ele à rede veicular na qual ele é utilizado.

1.3 Organização do Texto

Esta dissertação está organizada em seis capítulos. No Capítulo 2, apresentamos os conceitos básicos das redes *ad hoc* veiculares (VANETs). Em seguida discutimos sobre os tipos aplicações propostas para essas redes, com destaque para as aplicações de segurança. Apresentamos então as características dos modelos de mobilidade existentes para as VANETs. Por fim, mostramos o problema de desconexões no roteamento dessas redes, relacionado às constantes mudanças em suas topologias, e como aplicação dos conceitos de redes tolerantes a atrasos e desconexões (DTNs) pode ajudar a mitigá-lo.

No Capítulo 3 apresentamos os principais conceitos de segurança relacionados às redes veiculares, como perfis de intrusos, possíveis ataques executados e soluções de criptografia. Discutimos também sobre a aplicabilidade de alguns mecanismos de segurança disponíveis na literatura no contexto de aplicações de segurança em redes veiculares.

No Capítulo 4 apresentamos o mecanismo proposto, denominado RMDTV, e descrevemos o funcionamento de cada fase do mesmo, bem como especificamos o formato das mensagens utilizadas.

No Capítulo 5 é feita uma avaliação do desempenho da solução de reputação proposta. Avaliamos o RMDTV, por meio de simulações, comparando seu desempenho com o de uma rede na qual não é utilizado nenhum mecanismo de reputação. Em seguida, avaliamos o impacto da extensão das regiões geográficas ao redor dos eventos simulados. Discutimos também sobre a escalabilidade do melanismo proposto, bem como a necessidade da aplicação do conceito das redes DTN à rede veicular simulada. Por fim, avaliamos a sobrecarga adicionada pelo RMDTV à rede simulada.

Por fim, apresentamos no Capítulo 6 as conclusões da análise do RMDTV. Vislumbramos também a possibilidade de trabalhos futuros para mecanismos de reputação em redes veiculares tolerantes a atrasos e desconexões.

Capítulo 2

Redes Móveis Veiculares

Neste capítulo apresentamos e descrevemos os principais conceitos, a arquitetura, os tipos de aplicações existentes, os modelos de mobilidade e os problemas de desconexão relacionados às redes *ad hoc* veiculares (VANETs). A Seção 2.1 descreve as principais características de uma VANET. A Seção 2.2 apresenta a arquitetura básica de uma VANET. A Seção 2.3 lista alguns tipos de aplicações já propostas para as VANETs, com destaque para a descrição completa de uma aplicação de segurança para essas redes. A Seção 2.4 discute as características dos modelos de mobilidade existentes para as VANETs e apresenta o modelo de mobilidade adotado neste trabalho. Por fim, na Seção 2.5 é mostrado o problema de desconexões no roteamento das VANETs e como o uso dos conceitos de redes tolerantes a atrasos e desconexões (DTN) permite às redes veiculares suportar tais situações sem maiores prejuízos ao seu desempenho.

2.1 VANETs

Nos últimos anos, as redes *ad hoc* móveis (*Mobile Ad Hoc Netwoks* - MANETs) têm recebido muita atenção da comunidade acadêmica. Inicialmente direcionadas apenas para ambientes militares e de emergência, essas redes passaram a ser foco de grande interesse comercial, uma vez que o aumento do uso de aparelhos móveis, como celulares e PDAs, criou uma forte demanda por aplicações capazes de dar suporte a esses dispositivos. Dessa forma, uma MANET é assim definida pela [Manet, 2009]:

> Uma MANET é um sistema autônomo de roteadores móveis (e hosts associados) conectados por enlaces sem fio - a união desses dispositivos forma um gráfico arbitrário. Os roteadores são livres para se mover aleatoriamente e se organizar arbitrariamente assim, a topologia da rede sem fio pode se alterar de forma rápida e imprevisível. Tal rede pode ainda operar

isoladamente ou estar conectada à Internet.

Dentre os tipos de MANETs mais estudados atualmente estão as redes *ad hoc* veiculares (*Vehicular Ad hoc Networks* - VANETs), redes nas quais os veículos atuam como dispositivos móveis. Um dos principais objetivos dessas redes é criar condições seguras de circulação para os veículos que trafegam em uma via. Isso é feito através da troca de mensagens entre esses veículos informando as condições do trânsito, ocorrência de acidentes, obstruções, etc. De acordo com [Raya e Hubaux, 2005], podemos destacar como principais características das VANETs:

- **Banda disponível:** as tecnologias sem fio disponíveis atualmente possuem capacidades de transmissão significativamente menores 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 veículos, o sentido desse deslocamento e o raio de alcance dos dispositivos móveis instalados nesses veículos. Assim, da mesma forma que podem existir áreas nas quais um veículo mantém um grande número de conexões, também é possível a formação de ilhas de conexão em certos pontos da rede.
- **Cooperação:** a funcionalidade da rede recai totalmente sobre a cooperação dos veículos que a compõem. 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 a maior rede *ad hoc* móvel existente no futuro.
- **Mobilidade organizada:** diferentemente das MANETs tradicionais, os membros 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 que definem, por exemplo, o sentido de circulação e a velocidade máxima permitida.
- **Topologia dinâmica da rede:** graças à alta mobilidade aliada a grandes velocidades, a topologia das VANETs pode mudar rápida e frequentemente.
- **Recursos energéticos e computacionais:** considera-se que VANETs possuem recursos energéticos e computacionais suficientes para as aplicações desenvolvidas, ao contrário das MANETs tradicionais;
- **Segurança:** com o acesso compartilhado ao meio, essas redes são muito mais suscetíveis a ataques que as redes cabeadas convencionais.

2.2 Arquitetura das VANETs

A arquitetura de uma VANET consiste basicamente de veículos comunicando entre si, através de conexões sem fio, como também com estações base fixas existentes ao longo da via. Embora existam diversas aplicações visionadas para as VANETs (Seção 2.3) essa comunicação visa principalmente a troca de informações de forma aumentar a segurança e a eficiência do tráfego na via. A Figura 2.1 apresenta uma visão em alto nível dessa arquitetura. Nela, os componentes da rede trocam mensagens sobre um evento de emergência existente na via (uma colisão entre dois carros) de forma que os veículos se aproximando dessa região, ao serem informados dessa situação, possam tomar ações, como por exemplo, a redução gradativa da velocidade de deslocamento, evitando assim novos acidentes.

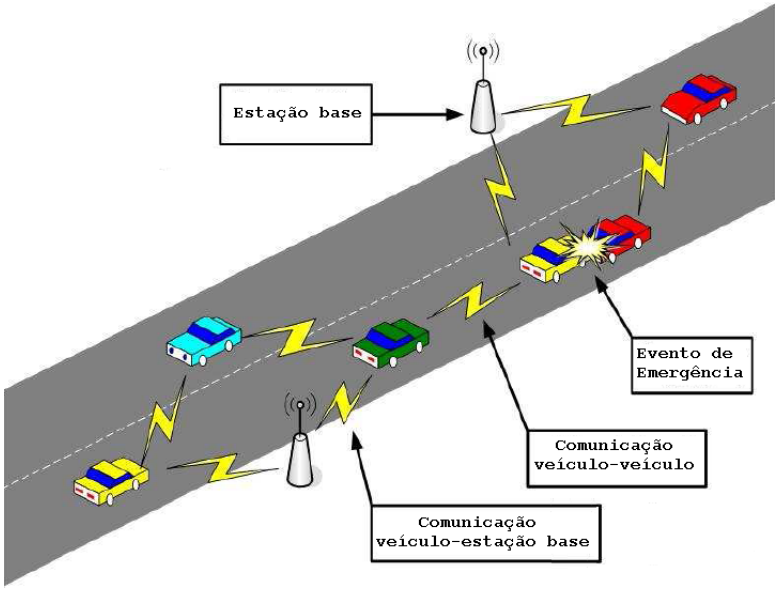

Figura 2.1. Arquitetura básica de uma VANET [Raya e Hubaux, 2005].

2.2.1 Estações base

As estações base são dispositivos geralmente localizados ao lado das vias de tráfego, responsáveis por prover comunicação entre a rede veicular e outros tipos de redes, como a Internet. Além disso, podem atuar tanto na geração de novas informações quanto no roteamento de dados gerados por terceiros. De maneira geral, essas estações são controladas por agências governamentais, o que garante sua idoneidade. Todavia, também podem pertencer a provedores de serviço, para atender a fins comerciais.

2.2.2 Veículos

Os veículos são os principais membros da VANET, pois graças a sua mobilidade, informações geradas em um ponto da rede são transportadas até pontos distantes de sua posição inicial. Além disso, atuam como os principais observadores de eventos ocorridos na via, uma vez que acidentes, congestionamentos e outros problemas de tráfego podem ocorrer fora do raio de alcance das estações base.

Os veículos participantes podem ser tanto particulares (carros, caminhões, etc), públicos (ônibus) ou até mesmo oficiais (viaturas policiais e ambulâncias). Entretanto, os chamados *veículos inteligentes*, como são conhecidos os membros móveis de uma VANET, necessitam de alguns componentes que possibilitem a comunicação e a execução dos aplicativos distribuídos. Os principais componentes, conforme [Hubaux et al., 2004], são descritos abaixo:

- **Sensores:** são os responsáveis pelo monitoramento dos eventos ocorridos com o veículo e ao seu redor. Variam desde um simples sensor de temperatura até um radar capaz de determinar a velocidade dos outros veículos trafegando na via.

- **Unidade de computação:** unidade central de processamento do veículo, é responsável, por exemplo, por transformar os dados obtidos pelos sensores em informações relevantes para o motorista e para toda a rede. É o único componente que se comunica com todos os outros.

- **Unidade de armazenamento:** guarda os dados utilizados pela unidade de computação e também as informações geradas por ela, para possíveis consultas futuras ou envio pela rede.

- **Unidade de comunicação:** habilita a comunicação sem fio com outros veículos e com as estações base. Essa comunicação pode fazer uso de uma versão customizada do padrão IEEE 802.11, proposta em [DSRC, 2009].

- **Sistema de posicionamento:** um *Global Position System* (GPS) permite ao veículo informar com maior segurança o local onde foram observados os eventos por ele detectados. Da mesma forma, esse sistema permite à unidade de computação calcular, por exemplo, a distância em relação a um evento relatado por outro veículo da rede, de forma que as ações sugeridas por ela ao motorista sejam as melhores possíveis.

- **Interface com o usuário:** mostra ao motorista, de forma amigável e intuitiva, os resultados obtidos pela unidade de computação. Considera-se que essa

unidade faça uso de mapas digitais para mostrar a localização dos eventos relatados, ou para exibir uma rota de desvio, possivelmente calculada pela unidade de computação.

2.3 Aplicações em VANETs

Existem muitos tipos de aplicações propostas para as VANETs [Car2Car, 2009]. Essas aplicações podem ser divididas em dois grandes grupos:

1. **Segurança e controle de tráfego**

   - **Informação de perigos:** ao identificar um perigo na via, como acúmulo de óleo na pista, ou mesmo um acidente, o veículo gera uma mensagem e a distribui informando a situação aos outros veículos.
   - **Otimização do tráfego:** são geradas mensagens com informações sobre a intensidade do tráfego nas vias. A partir do recebimento desses dados, os motoristas podem definir rotas otimizadas para seus trajetos evitando, por exemplo, trafegar em regiões onde foi reportada a existência de congestionamentos.

2. **Entretenimento e outras**

   - **Acesso à Internet:** veículos utilizam a infraestrutura criada pela VANET para acesso à Internet.
   - **Marketing:** veículos recebem informações sobre possíveis pontos de interesse, como postos de gasolina, oficinas mecânicas, bancos e outros.

Dentre as aplicações relacionadas à segurança, a troca de Mensagens de Perigo Local (*Local Danger Warnings* - LDWs), que são informações baseadas nas leituras obtidas pelos sensores locais dos veículos, mostra-se como uma das mais promissoras, dado o significativo benefício coletivo trazido pela disseminação de mensagens informando situações de risco na via. Definida inicialmente em [Kosch, 2004], essa aplicação foi alvo de estudos também em [Ostermaier, 2005] e [Adler e Strassberger, 2006].

Este trabalho tem como objetivo final aumentar o nível de segurança de uma VANET na qual esteja executando um sistema LDW. Assim, torna-se necessária uma discussão maior sobre esse tipo de aplicação, o que é feito na subseção seguinte.

2.3.1 Aplicação de mensagem de perigo local

Nos últimos tempos, o tráfego nas grandes cidades tem aumentado continuamente. Entre as conseqüências dessa situação, podemos citar o crescimento substancial do número de congestionamentos e acidentes nas ruas e estradas. Eventos como esses, além de representarem perda de tempo, uma vez que obstruem a fluidez normal do trânsito, representam também riscos reais à segurança dos motoristas. Logo, seria interessante se os motoristas fossem avisados o mais rápido sobre esses problemas, de forma que ações paliativas pudessem ser tomadas, diminuindo então as conseqüências geradas por tais situações.

Em uma Aplicação de Mensagem de Perigo Local (*Local Danger Warning Application*), eventos de risco detectados pelos sensores dos veículos geram mensagens de aviso que são disseminadas pela rede. A cada evento detectado é gerada uma nova mensagem informando sua condição. A Figura 2.2 exemplifica o processo de detecção de disseminação de informações sobre um evento de risco. Nela, o veículo 1, após detectar o acúmulo de óleo na pista, distribui na rede uma mensagem informando o problema aos outros veículos. Estes, por sua vez, atuarão como roteadores da mensagem, aumentando assim consideravelmente o alcance deste aviso. Ao receber uma mensagem, o aplicativo LDW avaliará seu conteúdo. Toda vez que esse aplicativo considerar suficiente as evidências de um evento, ele fará uso da interface com o usuário para comunicá-lo da existência do problema. Assim, o motorista terá tempo hábil para reagir àquela situação da maneira mais segura possível.

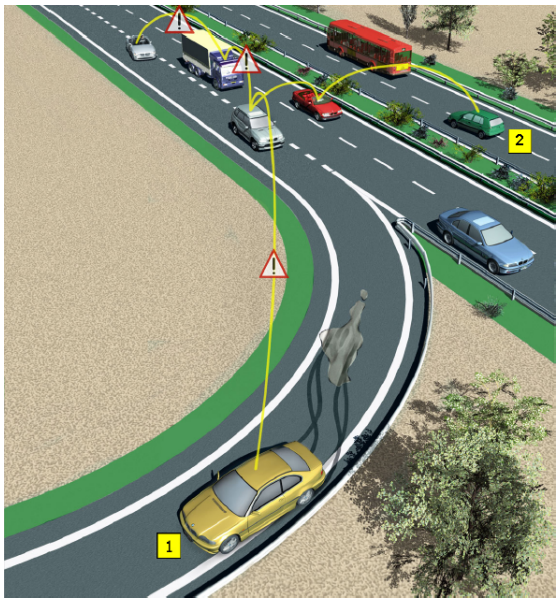

Figura 2.2. Disseminação de mensagem em cenário de perigo [Kosch, 2004].

Analisando a Figura 2.2, podemos perceber também que a referência geográfica tem

um papel importante em aplicações LDW. Na situação ilustrada, os dados disseminados sobre o acúmulo de óleo serão provavelmente considerados irrelevantes pelos veículos circulando no sentido contrário deste, como o carro 2, localizado na parte superior direita da figura, uma vez que este tende a não trafegar pela região de perigo informada nas mensagens. Assim, de forma a controlar a detecção de eventos, a distribuição de mensagens e o processo de tomada de decisões [Dotzer et al., 2005] definem que cada evento existente na rede é circundado por três regiões geográficas (Figura 2.3), definidas a seguir.

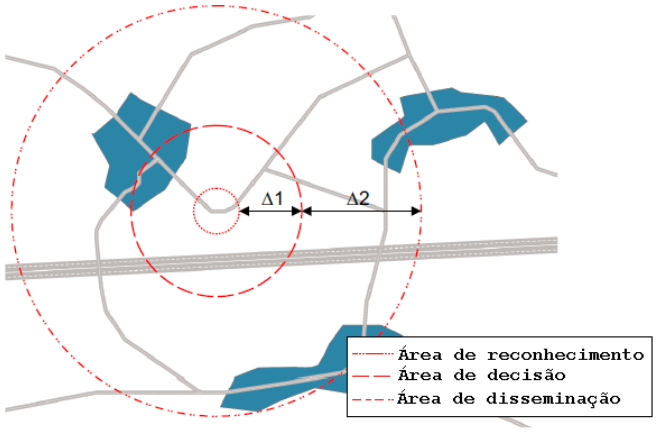

Figura 2.3. Áreas geográficas de um evento [Ostermaier, 2005].

A área mais externa é identificada como *área de disseminação*. Ao entrar nessa região, os veículos começam o processo de coleta e repasse das informações recebidas sobre o evento. Ao atingir a área intermediária, chamada de *área de decisão*, o veículo determina se alguma ação deve ser tomada acerca das informações recebidas sobre determinado evento. A área central, *área de reconhecimento*, é caracterizada por ser a única região onde um veículo é capaz de detectar, através da leitura de seus sensores locais, a presença de um evento na via, ou seja, somente veículos nessa área podem criar novas mensagens informando a ocorrência de eventos.

Neste trabalho as regiões geográficas assumiram formas circulares. Entretanto, tais regiões podem ser adaptadas para seguir o formato das vias. Além disso, o tamanho dessas áreas pode variar devido a fatores como a densidade da rede ou o tipo de evento ocorrido. A influência dessas variações será discutida adiante.

2.3.1.1 Fases de um sistema LDW

A partir das regiões que circundam um evento, um sistema LDW é constituído basicamente de três passos, segundo [Ostermaier et al., 2007]:

1. **Detecção de eventos**

   O processo de detecção de eventos na via deve acontecer de forma automática, sem a participação dos motoristas. Todavia esse processo não é simples e ainda é objeto de estudo [Adler e Strassberger, 2006]. Por exemplo, pode ser difícil calcular a dimensão exata de um congestionamento, haja vista que são necessários dados de velocidades dos veículos vizinhos para essa definição. Consideramos neste trabalho que os eventos podem ser captados pelos sensores dos veículos de forma simples e direta, sem a necessidade de análises mais complexas. Esse processo de detecção de eventos é conhecido como *experiência*.

2. **Disseminação de mensagens**

   Toda vez que um veículo tem uma experiência, uma mensagem é criada e disseminada pela rede. Todo receptor dessa mensagem determinará, a partir da sua relevância, se ela será simplesmente descartada ou guardada para ser utilizada no processo de decisão, sendo neste caso também encaminhada para outros veículos da rede. Com esse procedimento, experiências realizadas por veículos que já deixaram a área de disseminação ainda podem ser utilizadas por outros veículos em seu processo de decisão.

   A definição da relevância de uma mensagem pode levar em consideração vários aspectos, como o horário de geração da mensagem, sua origem ou até mesmo seu conteúdo. Como todos os veículos da rede executam os mesmos algoritmos, enquanto uma mensagem for relevante para um veículo, também o será para todos os outros. Quando o veículo deixa a área de disseminação a mensagem não é descartada, apenas seu envio é suspenso. Assim, caso ele retorne à área do evento, ela ainda pode ser usada no processo de decisão. Assim, reforçamos que o não atendimento aos critérios de relevância é o único motivo que leva ao descarte de uma mensagem.

   A disseminação das mensagens geradas é realizada através de um processo simples de difusão (*broadcast*). Embora existam algoritmos de propagação otimizados, como aqueles propostos em [Li e Lou, 2008] e [Sun e Garcia-Molina, 2004], estes estão além do escopo deste trabalho.

   A distância entre o limite exterior da área de disseminação e o limite exterior da área de decisão, representada na Figura 2.3 por $\Delta 2$, é diretamente proporcional à quantidade de mensagens recebidas pelo veículo durante o processo de coleta. Assim, caso $\Delta 2$ seja muito pequeno, o veículo pode receber uma quantidade insuficiente de mensagens antes do processo de decisão. Todavia, caso $\Delta 2$ seja muito grande, um carro estará sujeito a receber muitas mensagens desatualizadas,

graças aos intervalos de distância e tempo entre o ponto de origem e o ponto de recebimento desses dados.

3. **Processo de decisão**

   Imediatamente após entrar na área de decisão, um veículo, a partir das mensagens relevantes nele armazenadas, decide se avisa ou não ao motorista sobre uma possível situação de risco. Esse processo é executado somente uma vez a cada entrada do veículo nessa área. Nessa etapa existe o risco de erros nas decisões tomadas, causados por motivos como informações insuficientes, informações desatualizadas e até mesmo informações erradas enviadas por veículos com interesses escusos na rede. O objetivo do mecanismo de reputação proposto neste trabalho é atuar nessa etapa do processo de uma aplicação LDW, de forma a minimizar o número de decisões tomadas erroneamente.

   Podemos perceber que, da mesma maneira que $\Delta 2$, a distância entre o limite exterior da área de decisão e da área de reconhecimento, representada na Figura 2.3 por $\Delta 1$, também influi de forma decisiva na qualidade das decisões tomadas por um veículo. Com $\Delta 1$ pequeno, o tempo hábil de reação para o conjunto veículo-motorista torna-se muito curto, o que pode até mesmo inviabilizar uma atitude segura, como uma mudança de rota, ou uma frenagem de emergência. Já com $\Delta 1$ grande, um evento pode sofrer alterações ou até mesmo desaparecer no intervalo de tempo entre a tomada de decisão e a chegada do veículo ao local referido nas mensagens recebidas.

2.3.1.2 Conteúdo de uma mensagem LDW

Embora outros tipos de conteúdo possam ser adicionados, segundo [Ostermaier, 2005], a mensagem de uma aplicação LDW deve conter ao menos as seguintes informações:

- **Identidade da origem:** identifica o membro da rede responsável pela geração dos dados. No caso dos veículos, a identidade deve ser amarrada ao veículo, e não ao seu motorista. Essa identificação permite que várias mensagens informando um mesmo evento sejam consideradas por um veículo, devido às suas diferentes origens. Como veremos mais à frente, neste trabalho, a fonte de uma mensagem também será utilizada para definir a relevância dos dados por ela informados.

- **local da experiência:** O local de uma experiência permite ao receptor da mensagem definir se o evento está localizado em sua rota. Assim, é possível a definição das três áreas geográficas anteriormente definidas e a execução de seus respectivos processos.

- **horário da experiência:** O tempo de vida de uma mensagem é definido a partir do horário de sua criação. Logo, a inclusão do horário da experiência, permite ao veículo receptor definir localmente se a mensagem recebida está desatualizada e deve então ser descartada.

- **tipo de experiência:** Aqui é informado o tipo de evento observado pela fonte, como por exemplo, congestionamentos, acidentes, aquaplanagens ou outras situações de perigo que merecem a atenção do motorista.

2.4 Mobilidade em VANETs

Diferentemente das MANETs, nas quais o movimento dos membros da rede acontece, de maneira geral, em campo aberto, nas redes veiculares esses membros têm seu movimento restrito por vias pré-existentes, nas quais existem bloqueios como prédios e árvores, que influenciam na taxa de conectividade experimentada por um veículo. Além disso, o movimento dos membros é regulado por leis que definem, por exemplo, a velocidade máxima e mínima permitidas. Assim, o uso de modelos de mobilidade simplistas, como o *Random Waypoint* - (RWP) [Johnson e Maltz, 1996], em simulações de redes veiculares gera resultados sensivelmente diferentes daqueles conseguidos por modelos que respeitam as restrições citadas, como comprovado em [Choffnes e Bustamante, 2005].

Existem, na literatura, muitos modelos de mobilidade propostos para VANETs. De acordo com [Härri et al., 2007], que discute as características de vários modelos, tais propostas podem ser divididas em quatro grandes grupos:

- **Modelos sintéticos:** são modelos criados exclusivamente a partir de formulações matemáticas. Assim, os veículos desconsideram qualquer tipo de estímulo recebido do meio, fato que é visto como um problema grave, uma vez que tais perturbações poderiam causar variações consideráveis na modelagem do tráfego.

- **Modelos baseados em pesquisas:** são baseados em pesquisas realizadas sobre padrões de comportamento de grandes grupos. Modelam, por exemplo, o comportamento de pessoas que utilizam seus automóveis para atividades diárias como ir e voltar do trabalho, simulando seus horários de chegada e saída, almoço, etc.

- **Modelos baseados em traces reais:** são extraídos de grandes massas de dados reais. Com o auxílio de modelos matemáticos, padrões podem ser extraídos e

refinados a partir desses dados. Têm como maior problema o alto custo para obtenção desses *traces*.

- **Modelos baseados em simuladores de tráfego:** são complexos modelos sintéticos obtidos após um pesado processo de validação no qual são utilizados tanto *traces* reais como padrões de comportamento. Devido a sua natureza comercial, suas licenças têm custo da ordem de milhares de dólares, o que se torna o maior entrave à sua disseminação entre a comunidade acadêmica.

Neste trabalho, o modelo de mobilidade utilizado foi o Movimento em um Dia de Trabalho (*Working Day Movement* - WDM) [Ekman et al., 2008]. Proposto inicialmente para Redes Tolerantes a Atrasos e Desconexões (*Delay Tolerant Networks* - DTN) [Fall, 2003], este modelo, validado a partir de *traces* reais, simula um dia comum na vida de pessoas que acordam pela manhã, seguem para o trabalho, onde permanecem até o fim da tarde, quando então, retornam para casa. Essas pessoas levam consigo dispositivos portáteis capazes de realizar conexões, como celulares e PDAs. A partir de sua descrição geral, percebemos que o WDM simula o comportamento de um grupo de pessoas certamente interessado no estabelecimento de uma VANET na qual são trocadas mensagens sobre as condições de tráfego das vias, uma vez que tais informações, caso essas pessoas estivessem circulando de carro, permitiriam a elas a escolha de rotas melhores no intuito de reduzir o tempo gasto diariamente nos trajetos casa-trabalho e trabalho-casa. O funcionamento detalhado do WDM é descrito a seguir.

Primeiramente, cada pessoa tem seu horário de acordar definido. Essa definição pode ocorrer de forma aleatória ou seguir alguma distribuição estatística. Nesse horário, as pessoas saem de casa e seguem para o trabalho. Esse deslocamento pode ser feito com o uso de carro, ônibus ou mesmo a pé. A duração do período trabalhado é configurável e durante esse tempo o movimento das pessoas dentro do escritório é simulado, de forma que elas experimentem maiores oportunidades de conexão. Ao final do dia, elas escolhem, a partir de uma probabilidade pré-definida, se seguem direto para casa ou para algum ponto de atividades noturnas. Aqui novamente são utilizados os modelos de transporte anteriormente citados. Essas atividades podem ser entendidas como um passeio no shopping, um restaurante, um bar, etc. De forma análoga ao tempo de trabalho, a duração dessas atividades também é configurável e durante sua execução as pessoas se movimentam, o que permite o estabelecimento um número maior de conexões. Ao final, elas seguem para casa. Em casa, não há simulação de movimentos, como se o dispositivo fosse colocado em cima de uma mesa até o início de um novo dia, quando todo o ciclo se repete.

Todas as movimentações propostas pelo modelo acontecem dentro de um mapa.

Tal condição é de suma importância, haja vista que as restrições impostas pelas vias existentes influenciam o desempenho da rede.

A definição da localização da casa, escritório e local de atividades noturnas de cada pessoa é feita uma única vez no início da simulação. Essa definição pode ser totalmente aleatória ou pode ser restrita a determinadas áreas, o que simula, por exemplo, a existência de regiões residenciais e comerciais dentro de uma cidade. Os pontos escolhidos são conhecidos como *pontos de interesse* de uma pessoa. Da mesma forma, o meio de transporte utilizado também é definido no início da simulação. Pessoas que possuem carro utilizam somente esse meio de transporte durante todo o tempo simulado. Para o caso das demais pessoas, elas fazem o percurso de ônibus caso a distância Euclidiana entre o ponto de origem e o ponto de ônibus mais perto, somado com a distância Euclidiana entre o destino e o ponto de ônibus mais perto seja menor que a distância Euclidiana entre origem e destino. Caso contrário, elas decidem realizar o percurso caminhando.

Embora o WDM permita que as pessoas experimentem oportunidades de conexão a todo momento, nosso interesse, neste trabalho, restringiu-se aos contatos estabelecidos "sobre rodas". Dessa maneira, embora as movimentações e seus horários sigam exatamente o que propõe o modelo, somente as mensagens trocadas entre as pessoas trafegando de carro e os ônibus, que percorriam continuamente rotas previamente definidas no cenário simulado, foram consideradas.

2.5 Desconexão em VANETs

A mobilidade a altas velocidades, uma das principais características das VANETs, impõe grandes desafios aos protocolos de roteamento existentes. Essa mobilidade, restrita às ruas e estradas previamente definidas, é responsável por profundas alterações na topologia da rede. Assim, da mesma forma que a rede pode apresentar grandes densidades no centro de uma cidade ou durante um congestionamento, essa densidade pode cair a valores mínimos em bairros distantes, regiões rurais e vias de tráfego livre. Para o segundo tipo de situação, protocolos de roteamento comuns, que consideram a existência permanente de um caminho fim-a-fim entre um par qualquer de veículos, podem falhar na entrega de suas mensagens.

Segundo o teorema abaixo, cuja demonstração pode ser encontrada em [Xue e Kumar, 2004], para que o problema de desconexões em uma rede sem fio inexista, é necessário e suficiente que cada membro tenha $\Theta(\log n)$ vizinhos, sendo n o número total de membros dessa rede.

Teorema 1 *Seja $\mathcal{S}$ um quadrado em $\Re^2$, com n membros distribuídos de maneira uniforme e independente em $\mathcal{S}$. Seja $\mathcal{G}(n, \phi_n)$ a rede formada em $\mathcal{S}$ quando cada membro está conectado a seus ϕ_n vizinhos mais próximos. Para $\mathcal{G}(n, \phi_n)$ ser assintoticamente conectada, $\Theta(\log n)$ vizinhos são necessários e suficientes. Sendo $Pr\{A\}$ a probabilidade de ocorrência do evento A, existem, precisamente, duas constantes $0 < c_1 < c_2$ tais que:*

$\lim_{n\to\infty} Pr\{\mathcal{G}(n, c_1 \log n)$ *é desconectada*$\} = 1$ *e*

$\lim_{n\to\infty} Pr\{\mathcal{G}(n, c_2 \log n)$ *é conectada*$\} = 1$

Em uma VANET, existem outros fatores, além dos anteriormente citados, que influem na densidade da rede. Além disso, interferências no sinal de comunicação, causadas por construções e outras obstruções, podem afetar de forma significativa a conectividade nessa rede. Assim, é impossível garantir que cada veículo estará sempre conectado a $\Theta(\log n)$ vizinhos.

A Figura 2.4 exemplifica uma situação na qual um veículo tenta enviar dados para outro em uma rede particionada. Como não é possível estabelecer um caminho fim-a-fim entre origem e destino, o mecanismo utilizado para a comunicação deve suportar o atraso gerado pela interrupção, que pode ser de horas ou até mesmo dias.

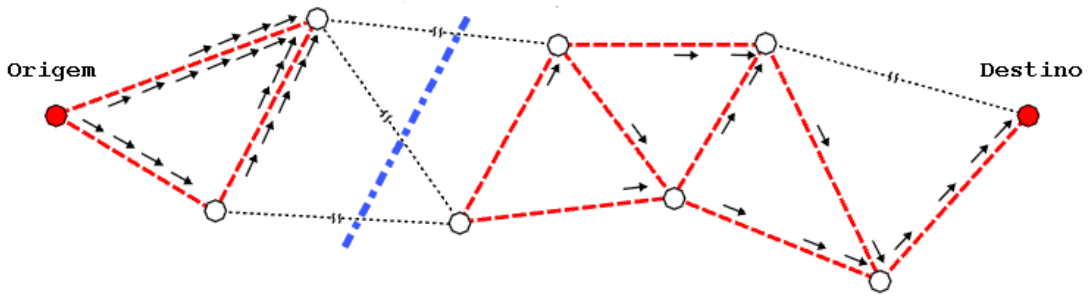

Figura 2.4. Particionamento em VANETs [Warthman, 2003].

Situações como a exemplificada acima geram novos desafios para os mecanismos de comunicação das redes veiculares. Nesses cenários, pode-se tentar continuamente o restabelecimento da conexão ou então adaptar-se a essa desconexão temporária. Uma opção para contornar esse tipo de problema é a utilização dos conceitos de redes tolerantes a atraso e desconexões no roteamento em redes veiculares [Burgess et al., 2006]. Nessas redes, a comunicação é feita no momento do estabelecimento de contatos agendados ou oportunísticos. Assim, os dados recebidos ou gerados por um veículo devem ser armazenados até que uma conexão esteja disponível, quando então são transmitidos. Logo, os veículos atuam como roteadores de dados quando existem conexões estabelecidas ou como armazenadores desses dados, quando a rede está particionada.

Os conceitos das redes tolerantes a atrasos e desconexões são discutidos de maneira aprofundada na subseção seguinte.

2.5.1 Redes tolerantes a atrasos e desconexões

Veículos em VANETs podem ser submetidos a períodos de desconexão na rede. Além disso, fatores como a mobilidade desses veículos a grandes velocidades podem gerar alterações significativas na topologia de tais redes, levando à formação das chamadas ilhas de conexão. Assim, diferentemente dos protocolos de comunicação atuais, que consideram a existência de conectividade contínua entre origem e destino, tais situações devem ser levadas em consideração na proposta de aplicações para VANETs, de forma a impactar o mínimo possível o desempenho da rede.

As *Challenge Networks* [Fall, 2003] são tipos redes caracterizadas pela comunicação intermitente, latências variáveis, taxas de dados assimétricas e grandes percentuais de erros. Dadas essas características especiais, aplicações nessas redes comportam-se de maneira diferente quando comparadas àquelas de redes convencionais.

De forma a possibilitar a comunicação nesses cenários desafiadores, foram criadas as redes tolerantes a atrasos e desconexões (*Delay Tolerant Networks* - DTN) [Fall, 2003]. DTNs contornam as questões existentes nas *Challenge Networks* utilizando o conceito de armazenagem-e-repasse para o encaminhamento de mensagens. Esse método define que um membro deve armazenar uma mensagem até que seja possível encaminhá-la a outro membro na rede, como mostra a Figura 2.5. O armazenagem-e-repasse é utilizado nos sistemas de e-mail atuais, nos quais fonte e destino contactam, de forma independente, um servidor localizado no caminho entre ambos, responsável por armazenar as mensagens trocadas.

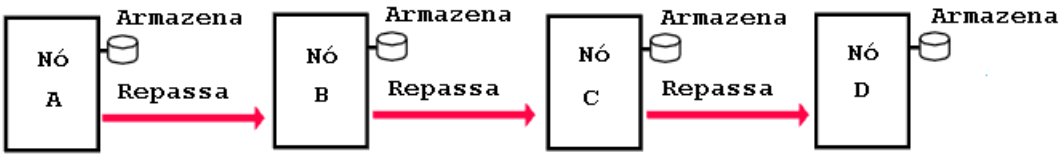

Figura 2.5. Modelo armazenagem-e-repasse de encaminhamento de mensagens [Warthman, 2003].

O modelo armazenagem-e-repasse é implementado pelas DTNs a partir da criação de uma nova camada sobrepondo toda a pilha definida pelo modelo OSI, a camada de agregação (camada *bundle*). Essa camada armazena e enfileira as mensagens agregadas

(os *bundles*) recebidas por um membro da rede DTN até que seja novamente estabelecida a conexão. Segundo [Warthman, 2003], esse armazenamento deve ser persistente, devido aos seguintes motivos:

- Um enlace de comunicação para o próximo salto pode ficar indisponível por um longo tempo.
- Um membro pode estabelecer conexão com outro capaz de enviar ou receber os dados mais rapidamente que ele. Assim, é necessário armazenamento temporário para acomodar diferenças de capacidade.
- Pode haver necessidade de retransmissão de mensagem, caso aconteça um erro no próximo salto, ou haja recusa no recebimento da mensagem encaminhada.

Os conceitos de DTN podem ser aplicados a vários tipos de redes, como as redes interplanetárias [Cerf et al., 2001], rurais [Seth et al., 2006], MANETs [Yang et al., 2006] e até mesmo em redes criadas para o rastreamento de animais selvagens, como a ZebraNet [Juang et al., 2002]. Além disso, como a camada *bundle* atua de maneira independente da tecnologia que dá suporte a comunicação, existe a possibilidade de interoperabilidade entre essas redes e a Internet, por exemplo.

Os protocolos de roteamento em uma rede DTN geralmente são escolhidos com base em características da aplicação e da rede, como o modelo de mobilidade utilizado. Em redes planetárias, por exemplo, o movimento dos planetas e satélites é previsível, de forma que são estabelecidos os chamados *contatos agendados*. Dessa maneira, nessas redes, os protocolos de roteamento utilizados são aqueles que realizam o roteamento determinístico, uma vez que é de conhecimento do membro quando existirão conexões disponíveis. Por outro lado, em redes veiculares, por exemplo, o movimento de seus veículos pode ser arbitrário, de forma que é difícil prever quando um novo contato será estabelecido. Por esse motivo, as conexões ativas em tais redes são definidas como *contatos oportunísticos*. Dada essa incerteza sobre novas possibilidades de conexão, veículos nessas redes tendem a repassar as mensagens por eles armazenadas de forma epidêmica para todos os seus vizinhos ativos, na esperança de que esses dados atinjam seu destino.

2.5.1.1 Arquitetura das redes DTN

O RFC 4838 [Cerf et al., 2007] define a arquitetura de uma rede DTN como uma composição da pilha de camadas definida para a Internet (modelo TCP/IP), acrescida de uma nova camada, chamada *bundle*, sobreposta à camada de transporte. A existência

dessa camada comum permite que redes DTN sejam compostas por várias subredes heterogêneas, nas quais os protocolos de comunicação das camadas inferiores podem ser inteiramente distintos. Assim, segundo [Warthman, 2003], uma DTN é uma rede de redes regionais, formando uma rede sobreposta (*overlay*) no topo dessas redes, incluindo a Internet.

A Figura 2.6 mostra uma comparação entre a pilha de protocolos da internet e das redes DTN. Podemos perceber que para o funcionamento da rede DTN é necessário apenas a existência da camada *bundle* em todas as subredes que a compõem, ficando então cada subrede livre para implementar os protocolos de comunicação específicos às suas características/necessidades particulares. A interface entre aplicações e as tecnologias de comunicação utilizadas fica a cargo da camada *bundle*.

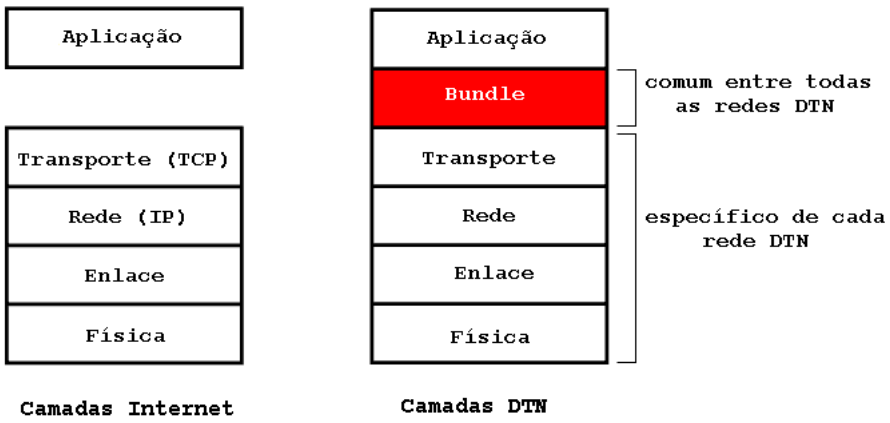

Figura 2.6. Arquitetura das redes DTN [Warthman, 2003].

Os *bundles* podem ser de tamanhos variados e consistem de três partes: dados da aplicação, informações de controle (dados fornecidos pela origem descrevendo ao destino como manusear as informações recebidas) e o cabeçalho, inserido pela camada *bundle*.

Em uma rede DTN, considera-se um membro como uma entidade na qual existe a camada *bundle*. Um membro pode ser um *host*, *roteador* ou *gateway*(podendo também assumir mais de um papel) atuando como fonte, destino ou repassador de *bundles*.

- **Hosts:** enviam e/ou recebem *bundles*, mas não os repassam. Caso sejam submetidos a enlaces intermitentes, necessitam de armazenamento persistente, de forma que seja possível a formação de filas de *bundles* até que esses enlaces estejam disponíveis novamente.

- **Roteadores:** repassam os *bundles* dentro de uma subrede, podendo atuar também como *hosts*. De maneira análoga aos *hosts*, também necessitam de arma-

zenamento persistente para possíveis formações de filas de *bundles*, caso sejam submetidos a enlaces intermitentes.

- **Gateway:** encaminham os *bundles* entre duas ou mais subredes DTN, além de poderem atuar também como *hosts*. Possuem, obrigatoriamente, armazenamento persistente para as mensagens recebidas. Devem ser capazes de realizar a conexão entre subredes utilizando tecnologias de comunicação distintas.

2.5.1.2 Segurança em redes DTN

Redes DTN normalmente são submetidas a severas condições de escassez de recursos, principalmente relacionadas à comunicação. Em redes planetárias, por exemplo, os membros são submetidos a longos períodos de desconexão. Cenários desse tipo tornam necessário o desenvolvimento de mecanismos de segurança capazes de conter ataques executados tanto por membros internos, quanto por aqueles externos à rede. Segundo o RFC 4838 [Cerf et al., 2007], mecanismos propostos para essas redes devem objetivar o atendimento dos seguintes requisitos:

- Prevenção contra o envio e armazenamento, pelos membros da rede, de dados de aplicações não autorizadas.
- Prevenção contra o envio de dados e a alocação de recursos maiores que os permitidos por aplicações autorizadas.
- Descarte de *bundles* modificados de maneira maliciosa durante seu roteamento.
- Detecção e remoção de membros maliciosos.

Soluções de segurança existentes para as redes tradicionais, como a publicação de listas de revogação ou a realização de consultas a servidores centrais em operações de autenticação e autorização de transações, podem não funcionar muito bem em redes DTN, dados os grandes atrasos experimentados entre o envio e o recebimento de dados por seus membros. Dessa maneira, mecanismos propostos para redes DTN tendem a utilizar dois tipos de mecanismos de autenticação e verificação de integridade: fim-a-fim e salto-a-salto. Enquanto o primeiro permite ao destino verificar a integridade e autenticidade dos dados recebidos, o segundo permite aos membros roteadores no caminho entre origem e destino a validação passo a passo, de forma que dados alterados ou fontes não confiáveis possam ser descobertas o mais rápido possível, evitando assim, problemas como a utilização de recursos de comunicação e armazenamento por aplicações não autorizadas ou até mesmo ataques de negação de serviço (DoS), nos

quais a rede é inundada por pacotes de dados enviados geralmente por entidades não autorizadas.

No Capítulo 4, veremos que o RMDTV, mecanismo de reputação proposto neste trabalho, faz uso de validações salto-a-salto a fim de detectar e descartar mensagens geradas por fontes não confiáveis o mais rápido possível, diminuindo assim, a eficiência dos ataques executados por esses intrusos.

2.6 Conclusão

Neste capítulo apresentamos os principais conceitos de VANETs. Começamos com a arquitetura da rede, passando pelas possíveis aplicações que podem ser executadas nesse ambiente. Além disso, discutimos os modelos de mobilidade e suas características terminando com o problema de conectividade ao quais tais redes estão expostas.

Apesar de existirem vários tipos de aplicações visionadas para redes veiculares, aquelas que fazem uso da troca de informações entre os veículos visando uma maior segurança não só das vias de tráfego, mas também dos motoristas que nelas circulam, despertam um interesse especial, haja vista que seus benefícios são não só financeiros, mas também sociais. Entre esse tipo de aplicação, a Aplicação de Mensagem de Perigo Local (Local Danger Warning Application), já definida e estudada em trabalhos anteriores surge como uma boa solução para reduzir os transtornos causados por situação de risco em uma via de trânsito.

Afim de que as simulações sejam as mais fidedignas possíveis, o modelo de mobilidade utilizado em simulações de VANETs deve considerar ao menos algumas características mais realistas, caso contrário, podem-se obter resultados impossíveis de serem reproduzidos em um ambiente real. O WDM é baseado em um "dia útil" na vida de pessoas que levantam pela manhã, vão para o trabalho e retornam para casa ao fim do dia. A validação à qual o modelo foi submetido, a partir de dados reais, o habilita como uma boa opção para simulações em VANETs.

Soluções para VANETs, sejam apenas para o roteamento de dados, sejam para aumentar a segurança, devem considerar o problema de desconexão existente em tais redes. A contribuição principal deste trabalho é um mecanismo de reputação para redes veiculares, que permita aos seus veículos atestar a confiabilidade de informações enviadas por terceiros em uma aplicação LDW. Considerando-se que a viabilidade deste mecanismo depende do sucesso no roteamento das qualificações emitidas para assegurar a confiabilidade dos veículos da VANET, o uso dos conceitos de Redes Tolerantes a Atrasos e Desconexões (DTN), discutidos na Subseção 2.5.1, tem papel decisivo no sucesso da solução apresentada. Apresentamos o mecanismo proposto e discutimos seu

funcionamento no Capítulo 4. Entretanto antes, no Capítulo 3, fazemos um estudo sobre as definições e soluções de segurança já propostas na literatura, como também sua aplicabilidade em VANETs.

Capítulo 3

Segurança em VANETs

Neste capítulo discutimos conceitos de segurança relacionados às redes veiculares. Na Seção 3.1 são listados os principais requisitos de segurança que devem ser atendidos nas VANETs. A Seção 3.2 apresenta uma discussão sobre os perfis de intrusos em VANETs, enquanto a Seção 3.3 classifica de forma geral os ataques que podem ser executados por esses inimigos. Na Seção 3.4 são discutidos conceitos de criptografia e como a aplicação destes pode ajudar no atendimento aos requisitos de segurança da VANETs. Finalmente, na Seção 3.5 mecanismos de segurança disponíveis na literatura são analisados quanto à sua aplicação e resiliência a ataques executados em redes veiculares.

3.1 Requisitos de Segurança

O sucesso de aplicações em VANETs depende principalmente da cooperação de todos os membros em prol do benefício coletivo. Entretanto, interesses difusos podem levar os membros da rede, ou mesmo intrusos externos, a tentar manipular o comportamento dos outros veículos, de forma que seus objetivos sejam satisfeitos. Como exemplo, podemos citar um proprietário de posto de gasolina que, interessado em aumentar o número de clientes, instala uma estação base fixa próxima ao seu estabelecimento, responsável por gerar e distribuir mensagens informando a existência de um congestionamento mais a frente na via, fato que pode induzir os motoristas a abastecer seus veículos, na tentativa de economizar tempo. Decisões tomadas com base em informações incorretas podem gerar transtornos simples, como o citado acima, ou complexas situações de risco, que podem culminar em graves acidentes, com possibilidade de perdas de vidas humanas. Assim, o atendimento a requisitos de segurança torna-se imprescindível em redes veiculares.

Os requisitos de segurança a serem atendidos em redes veiculares dependem prin-

cipalmente do tipo de aplicação. Aplicações de transmissão de arquivos, por exemplo, possuem requisitos bem diferentes de aplicações de segurança, nas quais os veículos trocam mensagens sobre as condições da via. Assim, segundo [Raya e Hubaux, 2005] e [Parno e Perrig, 2005], aplicações em VANETs podem necessitar de alguns ou todos os requisitos abaixo:

- **Confidencialidade:** as informações enviadas são ocultadas dos inimigos. Dessa forma, os inimigos são incapazes de saber o conteúdo das informações enviadas.
- **Autenticidade:** veículos devem tomar suas decisões baseadas em mensagens legítimas. Logo é necessário autenticar a origem de uma mensagem. Caso contrário, um veículo malicioso poderia se passar facilmente por alguém confiável, prejudicando sistematicamente a confiança no funcionamento da rede.
- **Integridade:** deve existir a garantia de que a mensagem não foi alterada no caminho entre origem e destino.
- **Frescor (*Freshness*):** aplicações em VANETs podem ter fortes restrições de tempo, de forma que mensagens antigas pode se tornar inúteis.
- **Disponibilidade:** mesmo assumindo a existência de um robusto canal de comunicação, alguns ataques de negação de serviço (DoS) podem atrapalhar o funcionamento da rede. Logo, devem existir mecanismos capazes de manter a disponibilidade mesmo sob severas condições.
- **Resiliência contra adulteração:** os componentes dos veículos inteligentes que funcionam sem a ação do motorista, como as unidades de computação, armazenamento e comunicação, devem possuir algum tipo de bloqueio contra alterações físicas, possivelmente realizadas por esses motoristas, cujo objetivo seja executar ataques no trânsito.

A tarefa de garantir a segurança em VANETs é dificultada por características específicas dessas redes, como por exemplo, a topologia extremamente variável, o que dificulta o estabelecimento e manutenção longas de relações de confiança entre os vizinhos. Todas essas características devem ser levadas em consideração no projeto de mecanismos de segurança em redes veiculares.

3.2 Inimigos

A natureza e os recursos de um inimigo determinam o tipo de defesas necessárias para assegurar o correto funcionamento de uma VANET. O estudo dessas características é

parte importante no desenvolvimento de mecanismos de defesa. Como as aplicações são as mais variadas possíveis, os invasores também podem ter perfis variados. Entretanto, podemos dividir esses perfis em três dimensões principais [Raya e Hubaux, 2005]:

- ***Inimigo interno* vs. *externo*:** um inimigo interno é um veículo autenticado na rede que pode se comunicar com os outros veículos. O inimigo externo é considerado um intruso na rede, de forma que os possíveis ataques por ele executados são limitados.

- ***Inimigo malicioso* vs. *racional*:** um inimigo malicioso é aquele que não visa obter benefícios próprios a partir de seus ataques. Seu único objetivo é prejudicar os veículos ou a funcionalidade da rede. Por outro lado, o inimigo racional visa algum ganho com suas atitudes de forma que seus ataques são mais previsíveis tanto em termos de ações quanto em termos de objetivos.

- ***Inimigo ativo* vs. *passivo*:** um inimigo ativo é aquele que injeta dados na rede, enquanto que o passivo atua apenas obtendo informações do canal sem fio, para análises posteriores.

3.3 Ataques

Um ataque é uma tentativa do inimigo de efetuar alguma ação não prevista na rede, com o objetivo de prejudicar o funcionamento das aplicações ou obter benefícios. De qualquer maneira, ataques ativos sempre prejudicam o correto funcionamento da rede. Embora seja impossível vislumbrar todos os possíveis ataques em VANETs, uma classificação geral pode ser adotada, com base nos tipos de ataques identificados até o momento [Parno e Perrig, 2005] e [Calandriello et al., 2007]:

- **Alarmes falsos:** neste ataque, o inimigo cria uma mensagem informando a existência de um evento inexistente na via. Dessa forma, outros intrusos, ao entrarem na área de reconhecimento do evento fictício, também geram mensagens informando sua existência. Como veículos cooperativos não conseguem detectar o referido evento, criam então mensagens revogando sua existência, tão logo adentrem sua área de reconhecimento.

- **Alarmes trocados:** neste ataque, o inimigo inverte a experiência por ele relatada nas mensagens distribuídas pela rede. Assim, sempre que detectar um evento, o intruso cria uma mensagem informando a inexistência de problemas na via, e vice versa.

- **Rastreamento (*Tracking*) de veículos:** é um tipo de ataque no qual o inimigo objetiva, a partir da coleta passiva de dados na rede, mapear o comportamento dos motoristas dos veículos. Assim, a partir da análise dos dados enviados por determinado veículo, seria possível predizer, por exemplo, seus horários e locais de circulação, o que poderia facilitar ações criminosas como seqüestros ou assaltos à residência de seu motorista principal.

- **Ataques de negação de serviço (*Denial of Service - DoS*):** o objetivo do inimigo aqui é causar a indisponibilidade da rede durante um determinado período de tempo, ou mesmo indefinidamente. Exemplos de ataques desse tipo incluem a interferência eletromagnética no canal de comunicação utilizado pelos veículos (*jamming*), o descarte de mensagens específicas na rede (*selective forwarding*) ou mesmo sua inundação com mensagens inúteis (*hello flood*).

- **Ataque sybil:** este ataque consiste em um veículo acessar a rede utilizando uma quantidade arbitrária de identidades virtuais. Logo, permite que apenas um inimigo realize ataques que necessitem de conluio entre os membros da rede.

Aplicações LDW, foco de estudo deste trabalho, estão sujeitas aos ataques acima listados. Todavia, como o propósito dessas aplicações é a troca de mensagens entre os veículos e estações base informando as condições da via, de forma que seja possível ao motorista tomar providências com o objetivo de reduzir os efeitos gerados por situações de risco, alarmes falsos ou trocados distribuídos pela rede tornam-se um problema importante, haja vista que o número de intrusos necessários para a execução com sucesso desses ataques não precisa ser necessariamente alto, dada a baixa densidade da rede em certos períodos do dia, como por exemplo, a noite. Assim, o mecanismo proposto neste trabalho foca reduzir a efetividade desses tipos de ataques.

3.4 Criptografia

A criptografia pode ser utilizada com o objetivo de ocultar as informações para o inimigo, garantindo assim a confidencialidade dos dados. As informações podem ser criptografadas para serem transmitidas por um meio não seguro ou então para serem armazenadas em um sistema de arquivos cujo controle de acesso é duvidoso.

Um sistema de criptografia é composto de três elementos básicos:

- **Algoritmo de criptografia:** função de embaralhamento, normalmente baseada em um ou mais parâmetros, denominados chaves.

- **Chaves de criptografia:** parâmetros dos algoritmos de criptografia que permitem a encriptação e correta decriptação dos dados enviados pela rede.
- **Terceiro confiável:** é o responsável pela distribuição das chaves ou certificados aos membros da rede.

Quanto ao tipo de chave utilizada, os algoritmos podem ser classificados em dois tipos:

- **Algoritmos de chave simétrica:** a chave usada no processo de encriptação pode ser utilizada também no processo de decriptação.
- **Algoritmos de chave pública:** são utilizadas duas chaves, uma para a cifragem e outra para a decifragem, sendo que uma delas é mantida em segredo e a outra é de conhecimento geral.

Os principais requisitos de segurança apresentados na Seção 3.1 (confidencialidade, autenticidade e integridade) podem ser atendidos pelo uso de técnicas de criptografia. Algoritmos de chave simétrica normalmente geram uma sobrecarga (*overhead*) computacional menor por mensagem, desconsiderando o processo de estabelecimento de conexão (*handshake*) necessário para a definição da chave compartilhada, que os algoritmos de chave pública. Entretanto, como em VANETs as mensagens geradas devem ser enviadas o mais rápido possível, uma vez que em muito dos casos o tempo é um requisito crítico no procedimento de tomada de decisões (Subseção 2.3.1), esse *handshake* inicial pode prejudicar o processo de troca de mensagens. Logo, o uso de uma infraestrutura de chave pública (*Public Key Infrastructure* - PKI) surge como a melhor opção para redes veiculares.

Em uma PKI, cada veículo da rede recebe um par de chaves, que podem ser emitidas pela agência governamental responsável pelo controle de trânsito ou mesmo pela fábrica deste veículo, conhecidas como *chave pública* e *chave privada*. Enquanto a chave pública deve ser divulgada por esse veículo, sua chave privada deve ser mantida sob sigilo. Assim, ele utiliza sua chave privada toda vez que encriptar uma mensagem. Todos os outros veículos da rede que possuírem sua chave pública são então capazes de ler o conteúdo dessa mensagem. De forma análoga, quando algum membro deseja enviar uma mensagem confidencial a determinado veículo, faz uso da chave pública deste para encriptar os dados. Logo, somente o veículo destinatário da mensagem pode decriptar e obter tais dados, utilizando sua chave privada. Como a chave pública não é necessariamente distribuída de forma autenticada pela rede, ela pode ser trocada pelo inimigo durante sua divulgação, o que torna necessário garantir sua autenticidade. Essa garantia pode ser dada através do uso de certificados, emitidos por autoridades certificadoras

(*Certification Authorities* - CAs), que atestam a autenticidade e integridade daquela chave.

Embora MANETs geralmente possuam restrições de recursos, fato que dificulta o uso de algoritmos de chave pública, tais restrições não existem em VANETs. Assim, o Algoritmo de Curvas Elípticas (Elliptic Curve Digital Signature Algorithm - ECDSA) [Johnson et al., 2001] foi avaliado por [Raya e Hubaux, 2005] e [Calandriello et al., 2007] como uma opção de criptografia de chave pública para redes veiculares. Os resultados obtidos foram significativos, sem que houvesse prejuízo ao desempenho da rede. Dessa maneira, o ECDSA foi a solução de criptografia utilizada neste trabalho.

3.5 Mecanismos de Reputação

Sistemas distribuídos nos quais não existe uma coordenação geral, como redes Par-a-Par (*Peer-to-Peer* - P2P), MANETs e VANETs, estão sujeitos a diversos tipos de inimigos e ataques. Soluções mais simples, como técnicas de criptografia, são capazes de neutralizar os efeitos de alguns ataques externos, uma vez que esses inimigos não conseguem acessar os dados trafegados pela rede. Todavia, quando um membro autenticado da rede atenta contra o funcionamento das aplicações, torna-se necessário o uso de mecanismos de segurança mais robustos, capazes de mitigar a eficiência dos ataques executados. Uma das soluções mais utilizadas para garantir o comportamento cooperativo nessas redes distribuídas é a utilização de sistemas de reputação.

O conceito de reputação pode ser definido como uma medida coletiva de confiabilidade em uma pessoa ou coisa baseada em indicações ou avaliações de membros de uma comunidade. Assim, o nível individual de confiança em tal pessoa ou coisa pode ser obtido a partir de uma combinação das indicações recebidas e das experiências pessoais [Swamynathan et al., 2007]. Em VANETs, a reputação de um veículo pode ser considerada como a coleção de opiniões mantidas por outros veículos sobre ele. Essa reputação é então utilizada como critério importante na tomada de decisões, tais como encaminhar ou descartar pacotes enviados por esse veículo, considerá-lo ou desconsiderá-lo como opção no roteamento de dados, considerar ou desconsiderar informações por ele repassadas, etc.

Mecanismos de reputação propostos para redes P2P e MANETs geralmente consideram uma taxa de conectividade suficiente para garantir a existência de caminhos fim-a-fim a todo o momento entre quaisquer dois membros da rede. Assim, tornam-se possíveis soluções nas quais dados utilizados pelo mecanismo de reputação são armazenados de forma distribuída na rede [Dewan e Dasgupta, 2004] ou é permitido ao mecanismo

esperar a completa execução do serviço solicitado, como, por exemplo, aguardar o recebimento de uma mensagem de ACK confirmando o roteamento correto de um pacote de dados enviado pela rede [Dewan et al., 2004]. Existem ainda propostas nas quais se considera que a movimentação dos membros da rede, de maneira geral, causará apenas pequenas alterações em sua topologia, de forma que o compartilhamento de observações diretas entre pequenos grupos, aliadas às experiências locais, seja suficiente para a construção de um robusto mecanismo de reputação [Buchegger e Le Boudec, 2004]).

A aplicabilidade de mecanismos de reputação propostos para redes P2P e MANETs no contexto das VANETs é bem restrita, haja vista que algumas considerações feitas nessas soluções, como aquelas citadas acima, não podem ser garantidas em redes veiculares, dadas as grandes velocidades de deslocamento dos veículos que compõem a rede. Assim, surge a necessidade do desenvolvimento de soluções próprias para as redes veiculares, nas quais suas características particulares são levadas em conta. Abaixo discutimos algumas propostas disponíveis na literatura.

No sistema de reputação para redes *ad hoc* veiculares (*A vehicle ad-hoc network reputation system* - VARS) [Dotzer et al., 2005], cada veículo adiciona sua opinião sobre a veracidade das mensagens por ele recebidas e encaminhadas. Essa opinião é baseada na combinação dos seguintes fatores: experiência do veículo (caso o evento relatado já tenha sido detectado por ele), reputação da fonte da mensagem e reputação dos responsáveis pelas opiniões já adicionadas à mensagem. As mensagens recebidas são armazenadas para serem utilizadas posteriormente no processo de decisão sobre o evento (o mecanismo faz uso dos conceitos de regiões geográficas ao redor dos eventos - Subseção 2.3.1). Quando a decisão é tomada, apenas a reputação das fontes dessas mensagens é atualizada.

Os primeiros veículos a receber mensagens geradas normalmente são aqueles mais próximos da área de reconhecimento e, por conseguinte, da área de decisão do evento. Em situações nas quais a fonte dos dados é desconhecida do receptor, não existe nenhuma base de confiança para o julgamento dos dados, haja vista que poucas ou nenhuma opinião foi adicionada à mensagem antes de seu recebimento. Logo, nesses casos, mensagens geradas por veículos têm o mesmo peso que aquelas geradas por intrusos.

O trabalho de [Wang e Chigan, 2007] propõe um mecanismo que, ao invés de considerar registros passados, conta apenas com o comportamento dos veículos em tempo de execução para a definição de reputações instantâneas. Segundo a proposta, um emissor envia o pacote de dados para seus vizinhos. Cada vizinho, caso não seja o destino final, reencaminha o pacote recebido. O emissor então monitora essas retransmissões. Se o pacote retransmitido não sofreu nenhuma alteração, o emissor envia um *token*

de confiança, assinado digitalmente, para o respectivo vizinho. Os vizinhos devem reencaminhar este *token*, que os certifica como confiáveis, para os veículos responsáveis pelo próximo salto. O processo de escuta e emissão do *token*, feito pelo emissor da mensagem, agora é feito pelos vizinhos certificados. Esse ciclo se repete em todos os saltos até que o pacote atinja seu destino.

O trabalho se preocupa apenas com possíveis alterações dos dados da mensagem durante o roteamento, sem avaliar o conteúdo da mensagem em si. Assim, mensagens contendo informações erradas podem facilmente ser distribuídas pela rede. Embora os resultados apresentados mostrem que cada passo da seqüência *envia mensagem - escuta reenvio - envia token*, adiciona, separadamente, uma sobrecarga aceitável na rede, não é feita uma avaliação dessa seqüência no que diz respeito ao tempo total necessário para sua execução, uma vez que topologia dinâmica das VANETs cria desafios consideráveis para soluções que necessitam de mais de uma conexão em uma mesma transação.

[Ostermaier et al., 2007] apresentam um esquema baseado em votos para aumentar a segurança das decisões tomadas pelos veículos sobre eventos reportados em aplicações LDW. A partir das mensagens recebidas dentro da área de disseminação, o trabalho avalia o desempenho de quatro diferentes métodos de decisão, executados quando o veículo adentra na área de decisão do evento: *Última mensagem*, *Maioria das mensagens*, *Maioria das últimas x mensagens* e *Maioria das últimas x mensagens considerando um limite inferior*. A eficiência desses quatro métodos é medida em uma rede submetida a ataques do tipo alarmes falsos e alarmes trocados (Seção 3.3).

Os resultados apresentados mostram que o método *Maioria das últimas x mensagens considerando um limite inferior*, onde o valor de x define as ultimas x mensagens mais recentes, consegue resultados significativos mesmo em um cenário com 40% de veículos maliciosos. Entretanto, como nenhum mecanismo de reputação é utilizado, esses intrusos podem executar seus ataques livremente, na certeza de suas mensagens serão sempre consideradas no processo de decisão dos outros veículos, uma vez que não existe nenhum tipo de punição a seu mau comportamento.

O mecanismo de [Patwardhan et al., 2006] acrescenta o uso de reputações a um esquema simples de votação, parecido com o *Maioria das mensagens* [Ostermaier et al., 2007]. Assim, um veículo colhe informações sobre eventos até que sejam recebidos dados transmitidos por uma fonte confiável, quando a decisão é tomada apenas com base nas informações contidas nessa mensagem, ou uma quantidade mínina de mensagens é recebida, quando o esquema de votação é executado. Uma vez que a decisão é tomada, o mecanismo de reputação proposto promove os veículos cujas mensagens enviadas corroboram com tal decisão enquanto rebaixa aqueles responsáveis por mensagens com opiniões contrárias. A partir do momento em que um veículo da

rede é considerado malicioso, suas mensagens são sempre descartadas.

A solução proposta não permite o compartilhamento de dados de reputação entre os veículos da rede, fato que pode representar uma demora considerável no processo de estabelecimento de relações de confiança e detecção de intrusos. Essa situação, aliada ao uso de uma metodologia na qual a promoção ou rebaixamento das fontes é feito com base apenas na opinião da maioria local, sem nenhuma validação posterior, possui uma implicação considerável. Em áreas onde é grande a concentração de veículos maliciosos ainda não descobertos, é provável que as impressões disseminadas por esses intrusos prevaleçam, levando à sua promoção com consequente rebaixamento de veículos cooperativos. Além disso, como não é definida nenhuma política de redenção de intrusos, a quantidade de falsos positivos pode se tornar um grande problema a longo prazo.

O RMDTV, mecanismo de reputação proposto neste trabalho, faz uso do método de decisão *Maioria das últimas x mensagens considerando um limite inferior* para a tomada de decisões em uma aplicação LDW. Validações posteriores das decisões tomadas sobre os eventos permitem ao mecanismo identificar com maior precisão veículos cooperativos e maliciosos. Com o armazenamento de dados históricos sobre o comportamento dos veículos, é possível o reconhecimento prévio e a exclusão de dados gerados por veículos considerados maliciosos. O compartilhamento de experiências, realizado na forma de qualificações assinadas digitalmente, também é uma característica importante da solução proposta, aumentando sua robustez e permitindo o estabelecimento de relações de confiança antes mesmo do início de transações. Os conceitos e o funcionamento do RMDTV são descritos no Capítulo 4.

3.6 Conclusão

Este capítulo foi dedicado ao estudo de aspectos de segurança em redes veiculares. Discutimos os desafios lançados pela presença inimigos executando ataques na rede, bem como as soluções existentes para tentar minimizar os efeitos dessas ações de forma que os requisitos de segurança impostos pela rede e suas aplicações possam ser atendidos.

Considerando-se que o comportamento passado é a melhor forma de tentarmos predizer o comportamento futuro de alguém, mecanismos de reputação surgem como uma boa solução na tentativa de mitigar os efeitos de ataques executados contra o funcionamento correto de uma VANET. Existem várias soluções propostas na literatura que fazem uso de reputação para aumentar a segurança em sistemas distribuídos, como redes P2P, MANETs e VANETs.

De maneira geral, sistemas de reputação para redes P2P e MANETs consideram que a topologia dessas redes se altera de maneira gradual, sem mudanças significativas

em um curto espaço de tempo. Assim, os mecanismos propostos fazem uso da conectividade existente para realizar transações mais demoradas, nas quais a execução de um serviço solicitado na rede pode ser assistida de perto por seu solicitante, permitindo a ele classificar de maneira mais precisa o comportamento de seus pares.

Por outro lado, mecanismos de reputação em VANETs não podem contar com altos graus de conectividade, haja vista que a constante mudança de topologia dessas redes pode resultar em intervalos de conexão muito curtos. Dada essa restrição, o estabelecimento de conexões com o intuito de apenas compartilhar dados de reputação pode acabar prejudicando o desempenho das aplicações sendo executadas.

O mecanismo de reputação proposto neste trabalho permite aos membros da rede atestar a confiabilidade das informações repassadas/emitidas por um veículo com base não apenas em suas próprias experiências, mas também em situações vivenciadas por outros veículos. O compartilhamento dessas experiências é feito pelo uso de qualificações que são roteadas pela rede mesmo sob condições de desconectividade. Ao receber uma qualificação, o veículo deve adicioná-la a todas as mensagens de dados por ele geradas. Assim, os receptores dessas informações podem utilizar os certificados anexados para atestar a confiabilidade do emissor dos dados. Conforme veremos no Capítulo 5, o mecanismo proposto consegue aumentar de forma considerável a segurança da rede, sem que a sobrecarga criada pela implantação da reputação prejudique o desempenho da aplicação sendo executada.

Capítulo 4

O Mecanismo de Reputação RMDTV

Neste capítulo descrevemos o mecanismo de reputação proposto, o RMDTV (*Reputation Mechanism for Delay Tolerant Vehicular Networks*). A Seção 4.1 apresenta os conceitos, as premissas e os requisitos utilizados para a especificação do mecanismo. Em seguida, a Seção 4.2 apresenta o funcionamento detalhado do mecanismo e dos algoritmos que o compõem.

4.1 Premissas e Requisitos do Mecanismo

O RMDTV é um mecanismo de reputação para redes veiculares. Ele tem como base o uso de qualificações emitidas por terceiros, atestando a confiabilidade das informações geradas por seus portadores. Embora o RMDTV possa ser utilizado em qualquer tipo de aplicação de segurança em redes veiculares, neste trabalho utilizamos as definições existentes para aplicações LDW em sua descrição e avaliação de desempenho.

Consideramos como membros da rede os veículos que possuem ao menos os componentes listados na Subseção 2.2.2 (sensores, sistemas de posicionamento, interface com o usuário, unidades de computação, armazenamento e comunicação) e as estações base existentes ao longo da via, de forma que seja possível a implementação da solução proposta e a comunicação entre essas entidades.

A partir dos conceitos acima, definimos um conjunto de premissas e requisitos sobre as características da rede veicular. Essas considerações, descritas a seguir, têm o objetivo de tornar o RMDTV um mecanismo eficiente no atendimento aos requisitos de segurança definidos na Subseção 3.1:

- **Identidade dos veículos:** as qualificações emitidas no RMDTV, descritas em detalhes na Subseção 4.2.2.2, são baseadas na identidade de seus destinos. Assim, consideramos que cada veículo V tem sua identidade definida de forma única no

início da rede. Tal identificação pode ser baseada, por exemplo, na placa do veículo. Entretanto, uma vez definida, essa identidade não pode sofrer alterações. Essa premissa pode tornar a rede mais propensa a ataques de *tracking* de veículos. O uso de pseudônimos, atualizados periodicamente [Calandriello et al., 2007] aumenta a resiliência da rede a esses ataques. Entretanto, seu estudo está além do escopo deste trabalho.

- **Detecção de eventos:** a partir do aparecimento de um evento, todos os veículos transitando dentro de sua área de reconhecimento são capazes de identificá-lo. Assim, cada veículo dentro da área de reconhecimento do evento gera e distribui, em modo de difusão, uma mensagem informando sua existência.

- **Revogação de eventos:** veículos se movendo dentro da área de disseminação de um evento ativo recebem mensagens informando sua existência. Se um veículo detectar a extinção do evento anteriormente anunciado, ao adentrar em sua área de reconhecimento, ele deve atuar de maneira análoga à detecção de eventos, gerando e distribuindo pela rede uma mensagem revogando a existência de tal evento.

- **Distribuição de chaves:** a rede veicular faz uso de uma infraestrutura de chave pública (PKI) para garantir a confidencialidade, autenticidade e integridade dos dados enviados. Consideramos que cada veículo recebe da Autoridade Certificadora (AC), que atua aqui como terceiro confiável (Seção 3.4), no início de operação da rede, seu par de chaves (pública e privada) correspondente. A AC pode ser, por exemplo, o órgão governamental responsável pelo emplacamento dos veículos. Além disso, faz parte também desse pré-carregamento o certificado, emitido pela AC, validando a chave pública daquele membro.

- **Desempenho:** o objetivo do mecanismo proposto é aumentar a confiabilidade das mensagens de dados recebidas em aplicações de segurança distribuídas executadas em redes veiculares. Os veículos responsáveis por essas informações adicionam, em cada mensagem gerada, qualificações recebidas de terceiros, atestando sua confiabilidade. Assim, a solução proposta neste trabalho, além de aumentar o tamanho das mensagens de dados, adiciona um novo tipo de mensagem às aplicações de segurança, encarregadas de transportar as qualificações emitidas até seus respectivos destinos. Apesar disso, espera-se que essa sobrecarga criada pelo RMDTV não prejudique o desempenho geral da rede.

Definidas as premissas e requisitos sobre os quais o mecanismo proposto de baseia, iremos agora descrever seu funcionamento.

4.2 Funcionamento do Mecanismo

O RMDTV é um mecanismo de reputação para redes veiculares tolerantes a atrasos de desconexões. Seu objetivo é permitir aos membros dessas redes atestarem a confiabilidade das mensagens recebidas, a partir do histórico de comportamento de seus emissores. Assim, a qualidade das decisões tomadas acerca de eventos existentes nas vias de tráfego tende a aumentar de forma considerável.

Toda vez que um veículo entra na área de reconhecimento de um evento ativo, gera e distribui pela rede, em modo de difusão, uma mensagem informando sua ocorrência. Essa distribuição ocorre continuamente enquanto este veículo estiver dentro da área de disseminação daquele evento. Outros veículos circulando por essa região recebem essa mensagem e a avaliam segundo a reputação de sua origem. No RMDTV cada veículo armazena localmente duas listas contendo, respectivamente, os membros da rede considerados confiáveis e aqueles considerados maliciosos. Assim, o emissor dos dados é classificado em uma das seguintes categorias: *malicioso*, *confiável* ou *desconhecido*.

Se o emissor é considerado malicioso, a mensagem é imediatamente descartada. Se os dados forem originários de uma fonte tida como confiável ou desconhecida, a mensagem é repassada ao mecanismo de decisão, descrito em detalhes na Subseção 4.2.1. Esse processo é repetido até que os requisitos mínimos para a tomada de decisão sejam atendidos. No RMDTV os eventos considerados são o recebimento de uma mensagem originada por uma fonte confiável ou a entrada do veículo na área de decisão do evento.

Como descrito na Subseção 2.3.1, as mensagens repassadas ao mecanismo de decisão, ou seja, consideradas relevantes pela aplicação, são retransmitidas em modo de difusão, possibilitando assim que experiências realizadas por veículos que já deixaram a área de disseminação ainda possam ser utilizadas por outros membros da rede em suas decisões. Essa redistribuição ocorre continuamente enquanto o receptor estiver dentro da área de disseminação do evento e a mensagem não exceder seu tempo de vida (*timeout*).

Uma vez que os requisitos do processo de decisão sejam atendidos e a decisão é tomada, a correção dessa decisão precisa ser atestada. Em situações reais, essa verificação pode ser feita por um das seguintes maneiras:

- Caso o veículo não utilize uma nova rota, o que acontece em casos nos quais não existem evidências suficientes da ocorrência do evento, a confirmação pode ser realizada pelos seus próprios sensores, uma vez que ele trafegará pela região apontada como local de ocorrência do evento.

- Caso seja definida uma nova rota, a validação da situação real do evento no

momento da tomada de decisão poderia ser realizada posteriormente, a partir da consulta a um servidor Web contendo informações sobre o estado das vias de trânsito da cidade, como já é possível atualmente através de aparelhos celulares.

Uma vez que a situação real do evento é conhecida, o veículo pode aferir a correção da decisão tomada. Após essa validação, ele atualiza os valores de reputação dos membros responsáveis pelas mensagens utilizadas no processo de decisão. Todavia, como veremos na Subseção 4.2.1, em alguns casos as evidências da ocorrência ou revogação de um evento podem ser insuficientes, de forma que a decisão tomada não é baseada nos dados recebidos. Para essas situações, não é realizada nenhuma alteração nos valores de reputação das origens dos dados recebidos. Para as demais, os passos executados são mostrados no algoritmo 1.

Independentemente da qualidade da decisão tomada, veículos cujas mensagens informaram o evento corretamente sempre são promovidos a confiáveis. Por outro lado, veículos cujas mensagens informaram o evento incorretamente são punidos, ou seja, passam a ser considerados maliciosos, somente quando o ataque executado obteve sucesso, ou seja, as informações por eles geradas foram relevantes o suficiente para levar o receptor a uma decisão incorreta. Caso contrário, continuarão a ser considerados desconhecidos quando suas mensagens forem submetidas novamente ao mecanismo de reputação. Com essa estratégia objetivamos atingir um número menor de falsos positivos, uma vez que é grande o risco de mensagens geradas por veículos cooperativos, mas recebidas com atraso, informarem uma condição diferente do estado atual do evento. Como veículos considerados maliciosos têm suas mensagens descartadas, o desempenho do RMDTV pode ficar dependente do tempo de redenção definido pela rede.

Algoritmo 1: Algoritmo de atualização de reputação

Entrada: Conjunto M de Mensagens sobre o Evento E utilizadas na decisão do veículo V

```
1  for M_0 to M_max do
2      if M_i informou o estado de E corretamente then
3          AdicionaListaVeiculosConfiaveis(Origem_{M_i})
           EnviaQualificacaoAtestandoConfiabilidade(Origem_{M_i})
4      end
5      else if decisão tomada foi errada then
6          if Origem_{M_i} ∈ lista de veículos confiáveis then
7              //mesmo veículo confiável passa a ser considerado malicioso
               RetiraListaVeiculosConfiaveis(Origem_{M_i})
8          end
9          AdicionaListaVeiculosMaliciosos(Origem_{M_i})
10     end
11 end
```

É importante ressaltar que o RMDTV altera apenas os dados de reputação da origem das mensagens. Tal decisão se apóia no fato de que muitas das vezes as mensagens

recebidas foram repassadas por veículos que não realizaram a experiência, mas confiaram no relato de outros membros da rede. Embora essa situação possibilite ataques de adulteração de dados, a integridade dessas informações é garantida pelo uso de uma infraestrutura de criptografia de chave pública. A solução utilizada é descrita na Subseção 4.2.2.1.

Segundo [Buchegger e Le Boudec, 2004], o compartilhamento de experiências é uma ótima maneira de aumentar a robustez de um mecanismo de reputação. Entretanto, características específicas das VANETs, como os curtos períodos de conexão experimentados pelos veículos, consequência direta das grandes velocidades de deslocamento, criam importantes obstáculos a esse compartilhamento, uma vez que a troca de opiniões deve acontecer sem prejudicar o desempenho da aplicação. Além disso, com a mudança constante na topologia da rede, a troca voluntariosa de informações pode levar os veículos a armazenar dados sobre outros membros poucas vezes ou nunca encontrados. Por outro lado, procurar informações sobre a reputação de um determinado membro da rede pode ser algo custoso e muitas vezes falho, uma vez que os detentores desses dados podem estar inacessíveis naquele momento. Assim, no RMDTV, as listas de confiabilidade de cada veículo nunca são publicadas. O compartilhamento de opiniões é feito a partir de um procedimento similar ao *Pretty Good Privacy* - PGP [Zimmermann, 1994], no qual é criada uma rede de confiança (*Web of Trust*) entre os membros da rede, a partir da troca de certificados assinados digitalmente entre os pares. Esses certificados devem ser apresentados aos novos pares em futuras transações, funcionando assim como as "credenciais" de seu portador. Dessa maneira, para cada um dos veículos promovidos pelo algoritmo 1, o receptor gera e envia uma qualificação atestando a confiabilidade daquele membro da rede. Dados os problemas de desconexões existentes nas VANETs, uma qualificação pode demorar horas, ou até mesmo dias para chegar ao seu destino. Assim, a aplicação do modelo armazenagem-e-repasse, utilizado pelas redes DTN (Subseção 2.5.1) para o encaminhamento de mensagens, surge como uma solução aos possíveis atrasos existentes durante o roteamento de qualificações.

As qualificações recebidas por um veículo devem ser adicionadas às mensagens de dados por ele geradas. Embora não sejam consideradas em um primeiro momento, quando é feita a avaliação da reputação da origem, resultando no descarte ou disponibilização dos dados recebidos para o processo de decisão, veremos na Subseção 4.2.1 que, uma vez que a mensagem não seja descartada, essas qualificações anexadas têm pesos diferenciados no mecanismo de decisão executado pelo receptor das informações. Para evitar uma sobrecarga muito grande na rede, apenas um determinado número de qualificações deve ser adicionado. Além disso, como as qualificações emitidas possuem "data de validade", somente aquelas que ainda não expiraram devem ser utilizadas.

A fim de potencializar o compartilhamento de opiniões, veículos que transitaram pela área de reconhecimento de um evento qualificam também outros veículos responsáveis por mensagens que corroboram com as impressões por eles experimentadas. Como apenas opiniões positivas são disseminadas, não existe a possibilidade de ataques ao RMDTV nos quais veículos maliciosos objetivam denegrir a imagem de veículos cooperativos.

No RMDTV o bom comportamento dos membros da rede é incentivado através do decaimento da reputação de veículos cooperativos e da redenção de veículos maliciosos em função do tempo. O decaimento da reputação é baseado principalmente na "validade" das qualificações recebidas. Com o passar do tempo, caso o veículo não receba novas qualificações, aquelas já armazenadas expirarão, de forma que suas experiências terão menor peso no processo de decisão de outros veículos. De forma análoga, as listas identificando membros confiáveis e maliciosos são atualizadas de tempos em tempos, quando então são excluídos aqueles membros cujos comportamentos foram observados há períodos de tempo maiores que um valor pré determinado.

Na Subseção 4.2.1 apresentamos os métodos de decisão utilizados pelos veículos, enquanto na Subseção 4.2.2 apresentamos a especificação dos tipos de mensagens enviadas em uma rede executando o RMDTV.

4.2.1 Processo de decisão

A tomada de decisão sobre um evento pode acontecer em dois momentos distintos. No primeiro, durante a fase de coleta de dados, o veículo recebe uma mensagem originária de uma fonte por ele considerada confiável. Neste caso, as informações recebidas são consideradas evidência suficiente da existência ou revogação do evento e a decisão é baseada apenas nesses dados. O segundo momento acontece quando o veículo atinge a área de decisão daquele evento, sem receber mensagem alguma originada por fontes confiáveis.

Nesta situação, a decisão deve ser tomada imediatamente após a entrada na área de decisão do evento, a partir do uso das mensagens cujas fontes são consideradas desconhecidas pelo veículo. O método de decisão utilizado nesse caso deve ser capaz de proporcionar ao menos alguma resiliência a ataques nos quais mensagens contendo informações incorretas sobre o estado atual do evento são disseminadas pela rede, aumentado assim a qualidade das decisões tomadas pelos veículos.

Em [Ostermaier et al., 2007] são apresentados e avaliados quatro métodos de decisão, baseados em esquemas de simples votação, para aplicações LDW em VANETs. Esses métodos foram executados em redes expostas a ataques do tipo alarmes falsos e alarmes trocados. Nas simulações realizadas, o método denominado *Maioria das*

últimas x mensagens considerando um limite inferior foi o que apresentou o melhor desempenho. Nele, o veículo utiliza apenas as últimas x mensagens recebidas com informações sobre o evento. Entretanto, existe também um limite inferior, de forma que o mecanismo de votação só é utilizado caso o veículo receba ao menos um determinado número de mensagens. Quando esse mínimo de opiniões não é atingido, o veículo sempre se decide pela negação do evento. A opção por negar a existência do evento em situações nas quais a quantidade de evidências recebidas é insuficiente justifica-se dadas as possíveis conseqüências resultantes de decisões *falso negativas* e *falso positivas*. Enquanto nas primeiras o veículo simplesmente segue se movimentando sem nenhuma alteração de velocidade ou rota, nas segundas o motorista pode se decidir pela redução da velocidade do veículo (por exemplo, em situações de proximidade a um acidente ou congestionamento), o que aumenta o risco de colisões traseiras caso algum dos próximos veículos da via, possuindo quantidade suficiente de informações para executar o processo de decisão, se decida pela inexistência do evento.

Em face às possíveis situações descritas, nomeamos as decisões tomadas por um veículo como *decisões indicadas* e *decisões forçadas*. Enquanto as primeiras são resultado da execução do mecanismo de votação, as segundas ocorrem quando o veículo não recebe o número mínimo de mensagens para a execução do método de decisão.

O algoritmo 2 mostra a adição do RMDTV ao método *Maioria das últimas x mensagens considerando um limite inferior*. Primeiramente, para cada mensagem recebida, o veículo determina o tipo de experiência nela contida (confirmação ou revogação do evento). Além disso, as qualificações apresentadas pelos emissores dessas mensagens são divididas em 2 tipos: qualificações assinadas por fontes confiáveis e por fontes desconhecidas. As qualificações assinadas por fontes consideradas maliciosas são descartadas. A soma absoluta dos parâmetros considerados é calculada. O método de decisão é então executado. Se o veículo não recebeu a quantidade mínima de experiências, definida como *THRESHOLD_MININO_DECISAO*, decide então de maneira forçada pela inexistência do evento. Se essa condição for atendida, o veículo faz um comparativo entre a soma de mensagens informando sobre o evento e a soma daquelas revogando sua existência. Se alguma delas for maioria, é considerada evidência suficiente para a tomada de decisão. Caso contrário, são consideradas as somas das qualificações adicionadas às mensagens por suas fontes. Em um primeiro momento apenas os somatórios das qualificações assinadas por veículos confiáveis são utilizados. Se isso não for suficiente, o mecanismo faz uso também daquelas qualificações cujos emissores são desconhecidos do receptor, como uma última tentativa. Na impossibilidade de tomar uma decisão baseada nos dados recebidos, o veículo se decide pela inexistência do evento, ação justificada pelo mesmo motivo descrito anteriormente

quando das decisões forçadas. Todavia, para o processo de atualização de reputação do RMDTV (algoritmo 1) esse resultado é tido como uma decisão indicada, haja vista que as impressões recebidas influenciaram na decisão tomada pelo veículo.

4.2.2 Mensagens

Aplicações de segurança em VANETs definem um formato para as mensagens de dados, como aquele apresentado na Subseção 2.3.1.2, através das quais as informações são distribuídas pela rede. O uso do RMDTV em uma aplicação desse tipo necessita, além da alteração do formato de uma mensagem de dados básica, da especificação de um novo tipo de mensagem, a mensagem de qualificação, utilizada no envio de qualificações aos veículos considerados confiáveis por seus pares. Apresentamos abaixo a especificação completa dessas mensagens.

4.2.2.1 Mensagem de dados

As mensagens com dados sobre eventos existentes na via, ou mesmo informando sua revogação, são geradas apenas pelos veículos que transitaram pela área de reconhecimento do respectivo evento. Entretanto, na esperança de aproveitar o máximo possível a experiência realizada por um membro da rede, uma vez que ele pode sair da área de disseminação do evento sem que muitos veículos tenham recebido os dados gerados, as mensagens enviadas são retransmitidas continuamente por todos os receptores que consideram a origem dos dados confiável ou desconhecida, desde que estejam trafegando dentro da área de disseminação. Essa estratégia está sujeita a ataques de adulteração, nos quais um veículo malicioso altera os dados da mensagem, sem entretanto, atualizar sua origem. Assim, além de influenciar na decisão dos próximos receptores, esse intruso pode prejudicar também a origem dos dados, uma vez que apenas os valores de sua reputação são alterados após a verificação da qualidade da decisão tomada.

Embora [Wang e Chigan, 2007] proponha que todo veículo "escute" as retransmissões realizadas por seus vizinhos, e só então libere um *token* confirmando a autenticidade da mensagem reenviada, *token* esse que deve também ser reenviado por esses vizinhos, como condição para aceitação das mensagens pelo próximo salto na rede, consideramos que esse processo pode ter seu desempenho severamente reduzido em situações nas quais os veículos se deslocam a grandes velocidades ou mesmo quando é alta a densidade da rede. Logo, é preciso garantir que cada mensagem, uma vez enviada pela origem, possa ser acessada por seus receptores apenas em modo de leitura.

A fim de atender ao requisito acima descrito, o veículo deve assinar cada mensagem de dados por ele gerada, utilizando sua chave privada, antes de enviá-la pela rede. Além

Algoritmo 2: Algoritmo de tomada de decisão

Entrada: Conjunto M de Mensagens com dados sobre o Evento E
Saída: Decisão do veículo sobre a existência do Evento E

```
1  //votos existência evento
2  votosExistenciaEvento ⟵ 0
3  totalQualifConhecExist ⟵ 0
4  totalQualifDesconhecExist ⟵ 0
5  /votos revogação evento
6  votosRevogacaoEvento ⟵ 0
7  totalQualifConhecRevog ⟵ 0
8  totalQualifDesconhecRevog ⟵ 0
9  for M_0 to M_max do
10     if M_i informou a existência de E then
11         votosExistenciaEvento ⟵ votosExistenciaEvento + 1
12         totalQualifConhecExist ⟵ totalQualifConhecExist + ObterQualifConhec(M_i)
13         totalQualifDesconhecExist ⟵ totalQualifDesconhecExist + ObterQualifDesconhec(M_i)
14     end
15     else if M_i informou a revogação de E then
16         votosRevogacaoEvento ⟵ votosRevogacaoEvento + 1
17         totalQualifConhecRevog ⟵ totalQualifConhecRevog + ObterQualifConhec(M_i)
18         totalQualifDesconhecRevog ⟵ totalQualifDesconhecRevog+ObterQualifDesconhec(M_i)
19     end
20 end
21 if votosExistenciaEvento + votosRevogacaoEvento ≥ THRESHOLD_MININO_DECISAO
   then
22     if votosExistenciaEvento > votosRevogacaoEvento then
23         DefineOpiniaoExistenciaEvento(E, true)
24     end
25     else if votosExistenciaEvento < votosRevogacaoEvento then
26         DefineOpiniaoExistenciaEvento(E, false)
27     end
28     else if votosExistenciaEvento + totalQualifConhecExist >
       votosRevogacaoEvento + totalQualifConhecRevog then
29         DefineOpiniaoExistenciaEvento(E, true)
30     end
31     else if votosExistenciaEvento + totalQualifConhecExist <
       votosRevogacaoEvento + totalQualifConhecRevog then
32         DefineOpiniaoExistenciaEvento(E, false)
33     end
34     else if votosExistenciaEvento + totalQualifConhecExist + totalQualifDesconhecExist >
       votosRevogacaoEvento + totalQualifConhecRevog + totalQualifDesconhecRevog then
35         DefineOpiniaoExistenciaEvento(E, true)
36     end
37     else if votosExistenciaEvento + totalQualifConhecExist + totalQualifDesconhecExist <
       votosRevogacaoEvento + totalQualifConhecRevog + totalQualifDesconhecRevog then
38         DefineOpiniaoExistenciaEvento(E, false)
39     end
40     else
41         DefineOpiniaoExistenciaEvento(E, false)
42     end
43 end
44 else
45     //decisão forcada
46     DefineOpiniaoExistenciaEvento(E, false)
47 end
```

disso, seu certificado emitido pela Autoridade Certificadora (AC), que é simplesmente a assinatura da AC sobre a chave pública do veículo, também é adicionado. Assim, o formato de uma mensagem de dados é dado por:

$$M, Sig_{PrK_V}(M), Cert_{AC}(PuK_V)$$

onde M é a mensagem contendo os dados descritos na Subseção 2.3.1.2, $Sig_{PrK_v}(M)$ é a assinatura de V sobre M e $Cert_{AC}(PuK_v)$ é o certificado da chave pública de V.

Para ler o conteúdo de M, cada receptor dessa mensagem deve extrair e verificar a chave pública de V, utilizando a chave pública da AC, para depois verificar a assinatura de V utilizando a chave pública certificada.

Em cada mensagem de dados enviada, V deve acrescentar um determinado número de qualificações por ele recebidas e que ainda não expiraram, no intuito de reforçar a confiabilidade de suas informações. Essas qualificações e seu formato são o assunto da próxima Subseção.

4.2.2.2 Mensagem de qualificação

Para cada mensagem recebida pelo veículo, informando corretamente o estado de determinado evento (essa validação é feita após a verificação do estado real do evento) e utilizada em uma decisão indicada, é gerada uma qualificação assinada digitalmente por este receptor, atestando a confiabilidade da origem das informações. Esta qualificação é então enviada pela rede em direção ao seu destino, que é o responsável pelo armazenamento das qualificações por ele recebidas. Este envio não é realizado em modo de difusão, como é feito com as mensagens de dados, mas através apenas de membros considerados totalmente confiáveis pela aplicação executada. Assim, a sobrecarga criada é menor e a efetividade de ataques nos quais membros intrusos descartam esse tipo de mensagem, no intuito de prejudicar o desempenho do mecanismo de reputação, é reduzida.

De maneira análoga às mensagens de dados, os dados de uma mensagem de qualificação devem ter sua integridade garantida, evitando assim qualquer tipo de adulteração maliciosa. Assim, o formato de uma mensagem de qualificação é dado por:

$$V_q|T, Sig_{PrK_V}(V_q|T), Cert_{AC}(PuK_V)$$

onde V_q é a identidade do veículo a ser qualificado, T é o horário de geração dessa qualificação, $|$ é o operador de concatenação de dados, V é o veículo qualificador de V_q, $Sig_{PrK_V}(V_q|T)$ é a qualificação emitida, na forma de uma assinatura de V sobre a identidade de V_q, concatenada com o horário de geração, e $Cert_{AC}(PuK_V)$ é o certificado da chave pública de V.

A partir do recebimento dessa mensagem, o proprietário da qualificação deve adicioná-la, enquanto esta for válida, nas mensagens de dados por ele geradas. Cada receptor de uma mensagem de dados gerada por V_q deve validar as qualificações por ele apresentadas. Essa validação só é possível se o receptor possuir a chave pública certificada de V. Como não é possível garantir essa condição para todos os veículos da rede, V_q adiciona também $Cert_{AC}(PuK_V)$ às mensagens de dados geradas, permitindo assim a validação de cada qualificação adicionada por qualquer receptor dessas informações.

4.3 Conclusão

Neste Capítulo apresentamos os requisitos e premissas para o funcionamento do nosso mecanismo e detalhamos o seu funcionamento.

O RMDTV é um mecanismo de reputação para redes veiculares tolerantes a atrasos e desconexões que permite aos usuários da rede atestar a confiabilidade das informações emitidas por outros usuários. Esse mecanismo faz uso de qualificações emitidas por terceiros, que devem ser anexadas às mensagens geradas, no intuito de atestar a confiabilidade de seu emissor.

Capítulo 5

Avaliação de Desempenho

Neste capítulo avaliamos o RMDTV quanto ao *percentual de decisões erradas*, *percentual de decisões indicadas* e *quantidade total de falsos positivos*, utilizando o simulador *Opportunistic Networking Environment* - ONE [Keränen et al., 2009]. Como o conceito de redes tolerantes a atrasos de desconexões é algo relativamente novo, até onde sabemos o simulador ONE é o único específico para redes DTN que dá suporte a contatos oportunísticos e ao paradigma de armazenamento-transporte-repasse de mensagens. A Seção 5.1 descreve as características da aplicação utilizada na simulação e as métricas avaliadas. O mecanismo foi avaliado em cenários diferentes para o estudo detalhado de seu desempenho. Comparamos uma rede executando o RMDTV com outra onde nenhum mecanismo de reputação é utilizado. A Seção 5.3 avalia o desempenho em cenários com diferentes quantidades de intrusos. A Seção 5.4 analisa o impacto da variação da extensão das áreas geográficas ao redor dos eventos. A Seção 5.5 analisa a escalabilidade do RMDTV. A Seção 5.6 avalia os tempos de entrega das qualificações e discute o uso de conceitos de redes DTNs como suporte aos possíveis atrasos ocorridos nessas entregas. Por fim, na Seção 5.7 é feita uma análise da sobrecarga criada na rede pela solução proposta.

5.1 Simulação

Avaliações de sistemas de computação geralmente são realizadas a partir do uso de uma das seguintes técnicas [Izquierdo e Reeves, 1999]: medição, análise e simulação. A medição é geralmente utilizada quando existe a possibilidade de obtenção de dados reais do sistema estudado. Já a técnica de análise se baseia na modelagem do sistema e seus possíveis comportamentos a partir de modelos matemáticos imensamente simplificados. Por fim, a simulação é baseada na construção e execução de programas, com o objetivo de reproduzir o comportamento do sistema.

Neste trabalho, escolhemos a simulação como técnica de avaliação do RMDTV. Comparada com a técnica de análise, a simulação permite um maior detalhamento da rede que o simples uso de modelos matemáticos. Já o desenvolvimento de um protótipo, o que permite o uso de medições, possui um custo muito alto, gerado principalmente pela compra, instalação e manutenção dos dispositivos em veículos reais, o que inviabilizaria o projeto. Além disso, a simulação permite a repetição dos resultados, o que nem sempre é possível em um protótipo. Todavia, uma vez que a simulação não considera todos os aspectos da rede, mas apenas os mais importantes, seus resultados devem ser interpretados com cuidado.

O simulador escolhido para a avaliação e comparação de desempenho do RMDTV foi o *Opportunistic Networking Environment* - ONE [Keränen et al., 2009]. O ONE é um simulador de eventos discretos que tem como principais funções modelar a mobilidade dos nós da rede, o contato entre eles de acordo com seus respectivos raios de alcance, o roteamento de dados e o tratamento das mensagens através de um modelo de comunicação tolerante a interrupções. Os nós seguem o paradigma armazenar-transportar-repassar mensagens (*store-carry and foward*), mantendo-as em um *buffer* até que exista uma oportunidade para o repasse dos dados.

No simulador ONE, modelos de mobilidade baseados em mapas, como o *Working Day Movement* - WDM, utilizam arquivos no formato *Well Known Text* - WKT para definir a movimentação dos nós da rede. Arquivos WKT são gerados e editados a partir de mapas digitais com o uso de Sistemas de Informações Geográficas (*Geographic Information System* - GIS). Neste trabalho, utilizamos o OpenJUMP [OpenJUMP, 2009], um aplicativo GIS *open source* desenvolvido em Java, para a geração do arquivo WKT representando seção digital do mapa de Belo Horizonte. Na Figura 5.1, podemos visualizar a representação gráfica no ONE do arquivo WKT gerado.

5.2 Caracterização do Cenário

Simulações de redes veiculares geralmente são feitas sobre mapas englobando áreas urbanas de conhecimento dos pesquisadores, como a região de *Dupont Circle* em Washington, EUA utilizada em [Patwardhan et al., 2006] e a região central de Munique, Alemanha, utilizada em [Ostermaier, 2005]. Neste trabalho, escolhemos a cidade de Belo Horizonte como palco de nossas simulações, uma vez que esta é de conhecimento de todos os envolvidos no projeto. Dentre os vários corredores existentes na cidade, a Avenida Antônio Carlos se mostra como um dos mais importantes, não só por ser utilizada diariamente por milhares de pessoas em seus deslocamentos entre casa e trabalho, mas também por ser o principal acesso ao estádio Governador Magalhães Pinto (Mineirão),

uma das principais sedes da Copa do Mundo de 2014, a ser realizada no Brasil. Assim, entendemos que o estabelecimento de uma rede veicular nesta avenida, na qual os veículos trocam mensagens objetivando a melhoria das suas condições de tráfego, seria de grande valia não só para aqueles que nela circulam diariamente, mas também para os turistas que visitarem a cidade durante a Copa. O mapa digital da Figura 5.1 mostra a região de Belo Horizonte utilizada nas simulações. Com uma área de aproximadamente 55 km^2, este mapa engloba toda a Avenida Antônio Carlos, além da região central da cidade.

Utilizamos 300 carros, movendo-se de acordo com o *Working Day Movement* - WDM, discutido na Subseção 2.4. Dados todos os carros que circulam diariamente pela Av. Presidente Antônio Carlos, consideramos plausível que uma VANET real tenha ao menos essa quantidade de veículos. Além disso, adicionamos à rede 6 ônibus (equivalente a 2% do total de carros), que circulam ininterruptamente por uma rota pré-definida, e uma estação base, disposta ao lado da referida avenida, mais ou menos em seu ponto médio.

O tempo de simulação foi o equivalente a vinte dias, iniciando-se às 7h da manhã do primeiro dia. Como o WDM modela o comportamento dos nós da rede durante os chamados "dias úteis", foram simuladas quatro semanas de trabalho na rotina desses membros. Utilizamos os valores padrões do IEEE 802.11 para alcance de rádio e largura de banda dos membros, com 200m e 1Mbps respectivamente. Dado que simulações em redes veiculares não consideram restrições de processamento e armazenamento, os dados recebidos por cada membro foram armazenados em um *buffer* de tamanho ilimitado.

5.2.1 Mobilidade

As regiões residenciais, comerciais e de atividades noturnas definidas no WDM estão marcadas na Figura 5.1. As áreas numeradas de 1 a 4 identificam regiões residenciais, enquanto as áreas 5 e 6 referenciam regiões comerciais. Por fim, as áreas 7 e 8 marcam regiões de atividades noturnas. A partir das regiões definidas, foram criados dois grupos de nós na rede. Cada nó corresponde a um par veículo-pessoa. O primeiro grupo vive nas regiões 1 ou 2, trabalha na região 6 e realiza atividades noturnas na região 8. Já o segundo vive nas regiões 3 ou 4, trabalha na região 5 e realiza atividades noturnas na região 7. Como atualmente as pessoas tendem a viver em lugares mais afastados do centro das grandes cidades (região 6), dividimos os 300 carros utilizados nas simulações entre os dois grupos na proporção de 60% e 40%, respectivamente. A partir da alocação de um nó em determinado grupo, as localizações de sua residência, local de trabalho e atividades noturnas foram definidas de forma aleatória, dentro das regiões destinadas

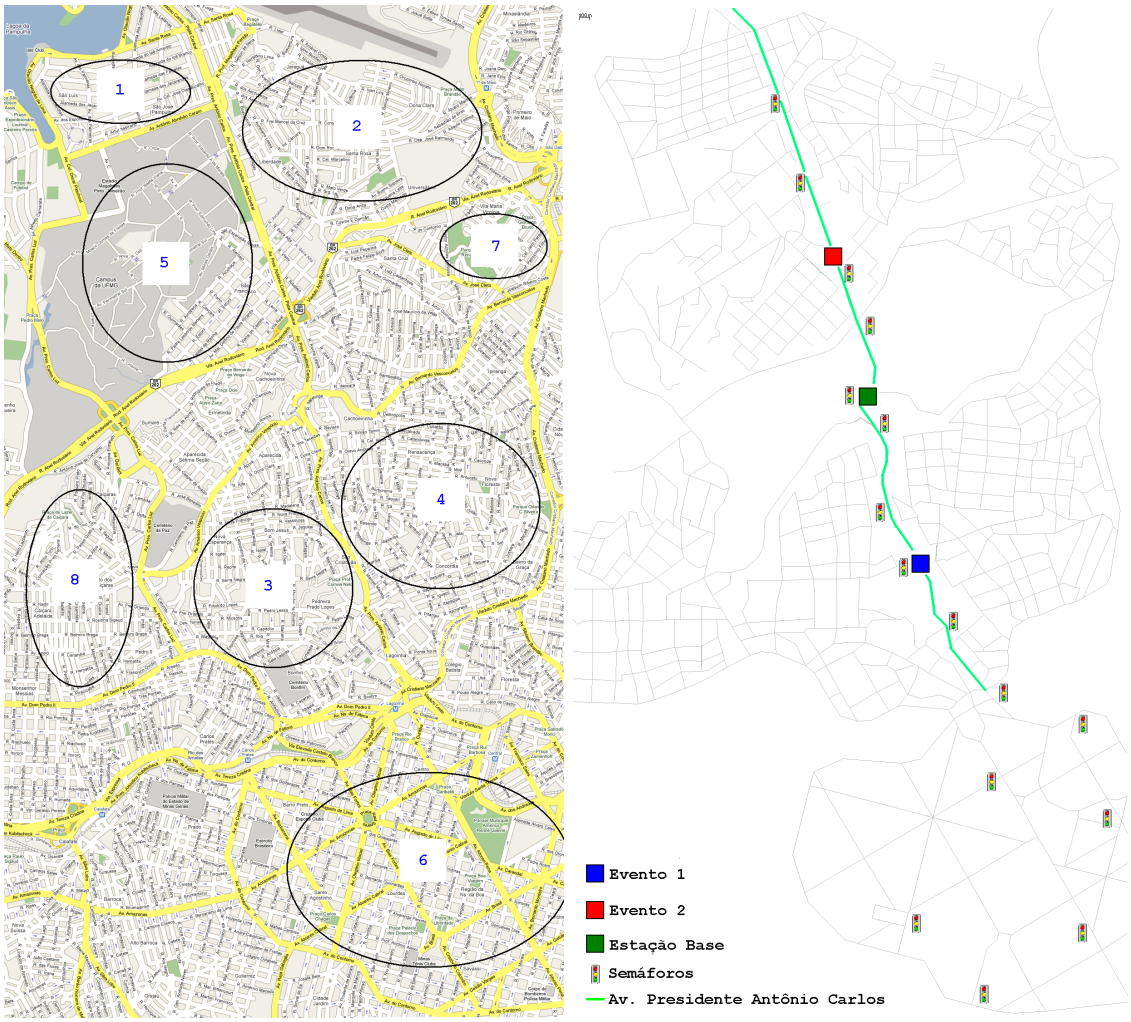

Figura 5.1. Mapa digital de Belo Horizonte e a representação gráfica do arquivo WKT gerado

aquele grupo. As definições de distribuição dos veículos simulados são sumarizadas na Tabela 5.1.

Tabela 5.1. Distribuição dos veículos entre as regiões da Figura 5.1

	Percentual veículos	**Moradia**	**Trabalho**	**Diversão Noturna**
Grupo 1	60%	1 ou 2	6	8
Grupo 2	40%	3 ou 4	5	7

A rotina dos nós simulados segue a seguinte regra: inicialmente foi definido um horário padrão para cada membro, escolhido aleatoriamente entre 7h30min e 9h30min, indicando o início diário do percurso casa-trabalho. Como em situações reais existem pequenas variações diárias no horário padrão definido, permitimos a cada nó um atraso ou adiantamento de até quinze minutos, calculado aleatoriamente, em cada dia. Uma

vez em seu local de trabalho, os nós lá devem permanecer durante oito horas seguidas. Após esse período, cada nó decide, com probabilidades de 80% e 20% respectivamente, entre seguir direto para casa ou realizar alguma atividade noturna. Essa distribuição indica que cada membro da rede executa atividades noturnas em média uma vez por semana. A duração dos eventos noturnos varia entre uma e três horas. Em casa, os nós dormem até o horário de seguir novamente para o trabalho.

Nos trajetos realizados dentro da rotina definida, os carros simulados se movem com velocidades entre 30km/h e 60km/h. Já os ônibus presentes na rede mantêm sua velocidade dentro da faixa de 25km/h a 55km/h. Esses valores respeitam a velocidade máxima permitida nas avenidas de Belo Horizonte, que é de 60km/h.

Semáforos foram dispostos em alguns cruzamentos (Figura 5.1), possibilitando assim maiores oportunidades de conexão entre os veículos da rede. Cada semáforo permanece aberto, e posteriormente fechado, por exatamente 125 segundos simulados, tempo esse igual à média real dos semáforos existentes em Belo Horizonte, segundo a Empresa de Transportes e Trânsito de Belo Horizonte [BHTRANS, 2009], órgão municipal responsável pelo controle de trânsito na cidade.

5.2.2 Eventos

Foram considerados dois eventos dentro da área simulada, identificados na Figura 5.1 como 1 e 2. Enquanto o evento 1 indica a existência de um congestionamento no sentido bairro-centro, o evento 2 indica um congestionamento no sentido centro-bairro. Levando-se em conta que informações sobre as condições do tráfego em prováveis pontos de congestionamento de uma via sempre interessam aos membros de uma VANET, qualquer veículo, ao atingir a área de reconhecimento de um dos eventos, gera uma mensagem informando sua condição, ou seja, se o trânsito está livre ou congestionado naquele ponto. Cada mensagem de dados gerada sobre a condição de um evento expira trinta minutos após sua criação.

O aparecimento dos eventos segue a seguinte regra: entre 8h e 9h da manhã, há 80% de chances de ocorrência do evento 1 enquanto o evento 2 conta com uma probabilidade de apenas 20%. Essa distribuição é baseada no fato de um número maior veículos se deslocar no sentido bairro-centro pela manhã, em comparação com aqueles que se deslocam no sentido centro-bairro. Assim, ao final do dia de trabalho, entre 17h e 18h, as probabilidades se invertem, haja vista que este é o horário em que a maioria dos veículos retorna para casa. Logo, dentro desse intervalo, as chances de ocorrência dos eventos são respectivamente 20% e 80%, para os eventos 1 e 2.

A fim de simular possíveis acidentes, ou mesmo outros problemas de tráfego que podem acontecer fora dos horários de *rush*, definimos uma probabilidade diária de

20% de ocorrência dos eventos 1 e/ou 2, em horários diferentes daqueles cobertos pelos intervalos acima citados. Assim, uma vez que um evento aconteça, seu horário de início e tempo de duração são definidos de maneira aleatória. Entretanto, a duração de um evento não pode exceder seu dia de ocorrência. As probabilidades de ocorrência dos eventos simulados são sumarizadas na Tabela 5.2.

Tabela 5.2. Probabilidade de ocorrência dos eventos ao longo do dia

	8h - 9h	**17h - 18h**	**Outros horários**
Evento 1	80%	20%	20%
Evento 2	20%	80%	20%

Os raios das áreas de reconhecimento, decisão e disseminação foram baseados em [Ostermaier et al., 2007], que utilizaram, respectivamente, raios iguais a 25m, 150m e 350m. Todavia, para esses valores, um veículo que não recebeu mensagens enviadas por fontes confiáveis, e que está se deslocando a uma velocidade média de 60Km/h (16,67m/s), tem, ao adentrar na área de decisão do evento, aproximadamente apenas 7,5s ((150m - 25m) / 16,67m/s) para tomar a decisão e agir antes de atingir a área de reconhecimento. Considerando ainda a necessidade de validação dos certificados adicionados às mensagens recebidas (Seção 5.7), este tempo é ainda menor. Logo, são necessárias áreas maiores, capazes não só de garantir a viabilidade da aplicação LDW, mas também do mecanismo de reputação proposto. Assim, utilizamos raios de 50m, 300m e 700m respectivamente, para as áreas de reconhecimento, decisão e disseminação ao redor dos eventos.

5.2.3 Mensagens de qualificação

As qualificações emitidas expiram vinte dias após sua emissão, ou seja, uma vez geradas, são válidas durante todo o período simulado. Assim, supondo que cada veículo receba, em média, uma qualificação por dia, limitamos a quantidade de qualificações adicionadas às mensagens de dados a no máximo vinte. Da mesma forma, o histórico de comportamento dos veículos, armazenado nas listas de confiabilidade, deve ser mantido também por vinte dias. Os ônibus e a estação base presentes na rede são considerados a *priori* confiáveis por todos os membros da rede. Além disso, como consideramos esses membros à prova de qualquer tipo de sabotagem, seus níveis de reputação não sofrem alterações.

A fim de reduzir a sobrecarga criada pelas mensagens de qualificação, cada carro portando mensagens desse tipo realiza o seu repasse apenas em duas situações: em caso de conexão direta com o destino daquela qualificação ou em caso de conexão com

os membros considerados a *priori* totalmente confiáveis (ônibus e estação base). Os ônibus, por sua vez, realizam o repasse apenas para o destino ou para a estação base. Já a estação base só é permitido o encaminhamento das qualificações diretamente ao seu destino final. Assim, além da diminuição da quantidade de mensagens de qualificação circulando pela rede, existe também a garantia de que elas são encaminhadas apenas a membros confiáveis, diminuindo então a possibilidade de ataques de descarte de mensagens.

5.2.4 Decisão e ataques

O método de decisão utilizado pelos veículos foi o *Maioria das últimas x mensagens considerando um limite inferior*, proposto em [Ostermaier et al., 2007]. Entretanto, como descrito na Subseção 4.2.1, no RMDTV informações provenientes de fontes confiáveis são consideradas evidência suficiente da existência ou revogação de um evento. Assim como em [Ostermaier et al., 2007], o número máximo de mensagens utilizadas pelo método *Maioria das últimas x mensagens considerando um limite inferior* foi 22, enquanto o mínimo de opiniões necessárias para a execução desse método de decisão foi fixado em 3.

Os intrusos presentes na rede executam apenas ataques do tipo alarmes trocados durante as simulações. Neste tipo de ataque, cada intruso simplesmente gera e distribui mensagens informando impressões opostas àquelas por eles experimentadas, ou seja, caso a via esteja livre, é gerada uma mensagem informando a existência de um congestionamento e vice versa. No mais, esses veículos se comportam de maneira similar aos membros cooperativos da rede. Não consideramos a execução de nenhum outro tipo de ataque mais estruturado.

Nossa avaliação se concentrou em comparar o desempenho entre duas redes: uma utilizando o RMDTV como mecanismo de reputação e outra na qual nenhum mecanismo é utilizado. As métricas utilizadas nas simulações foram: *percentual de decisões erradas*, ou seja, o percentual de decisões tomadas que diferiram do estado real do evento naquele momento, *percentual de decisões indicadas*, ou seja, aquelas decisões que foram tomadas a partir das informações contidas nas mensagens recebidas, e *quantidade total de falsos positivos*, que indica a quantidade de veículos cooperativos que foram considerados erroneamente como maliciosos pelo RMDTV. Avaliamos também os impactos dos *intervalos de tempo entre a geração e o recebimento das qualificações* quanto à necessidade suporte à possíveis atrasos em seu encaminhamento. Todos os resultados apresentados possuem 90% de intervalo de confiança. Cada simulação foi executada com oito sementes diferentes. Nas seções seguintes discutimos esses resultados.

5.3 Impacto da Quantidade de Intrusos

Neste cenário variamos o percentual de carros de comportamento malicioso existentes na rede. Partimos de um cenário com 0% intrusos, finalizando com uma situação onde 50% dos carros existentes são inimigos, aumentando esse percentual a taxas de 10%. Assim, em um primeiro momento, definimos o desempenho básico das redes com e sem a execução do RMTV. Posteriormente, com o aumento da quantidade de intrusos, avaliamos então a robustez dessas redes aos ataques executados por esses inimigos.

Os resultados obtidos nas simulações são analisados a partir do percentual total de decisões erradas tomadas pelos veículos e também a partir das variações diárias dessas decisões.

5.3.1 Percentual geral de decisões erradas

O gráfico da Figura 5.2 mostra o desempenho geral das redes com e sem a execução do RMDTV. Podemos perceber que existe uma relação quase linear entre o percentual de intrusos e de decisões erradas. A rede executando o RMDTV possui um desempenho melhor que a rede sem reputação em todos os cenários simulados. Considerando-se os pontos médios, essa melhoria varia entre 14% (rede sem intrusos) e 45% (rede com 50% de intrusos).

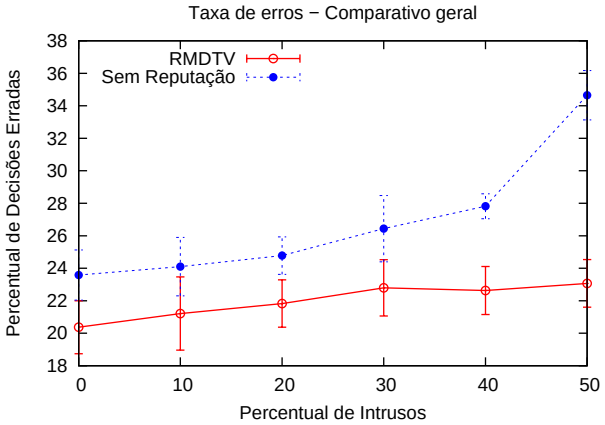

Figura 5.2. Percentual total de decisões erradas variando o percentual de intrusos na rede

5.3.2 Variação diária das decisões erradas

Os gráficos da Figura 5.3 mostram o percentual de erros diários na rede com e sem a execução do RMDTV, variando a quantidade de intrusos desde sua ausência completa até o percentual de 50% do total de veículos na rede.

Podemos observar variações diárias, tanto positivas quanto negativas, no percentual diário de decisões erradas. Essas variações são fruto das pequenas mudanças aleatórias permitidas no horário em que cada veículo da rede inicia o percurso casa-trabalho diariamente. Com alterações nesse horário, o subgrupo de veículos encontrados durante os percursos realizados está sujeito a variações consideráveis de um dia para o outro. Assim, da mesma forma que a mudança de horário pode fazer com que um veículo encontre mais membros cooperativos (ou confiáveis, no caso da rede com reputação) em um dia, pode implicar também, de maneira oposta, no estabelecimento de conexões com uma maioria de membros maliciosos, no dia seguinte.

A rede com reputação apresentou resultados melhores durante todos os dias simulados, para todos os percentuais de intrusos presentes na rede. Além disso, podemos observar uma evolução no distanciamento entre as curvas a medida que o percentual de intrusos aumenta, corroborando o resultado mostrado na Figura 5.2. Todavia, existem dois pontos que merecem ser discutidos: o primeiro diz respeito aos resultados obtidos quando da inexistência de veículos maliciosos, enquanto o segundo se refere aos resultados obtidos no primeiro dia de cada um dos cenários simulados.

O melhor resultado da rede com reputação mesmo na ausência de intrusos é resultado de uma tomada de decisão mais ágil quando o mecanismo de reputação é executado. Para que um veículo executando o RMDTV tome sua decisão acerca de um evento, basta que ele receba informações geradas por uma fonte confiável. Já em redes onde não existe um mecanismo de reputação, o veículo deve coletar informações sobre o evento até atingir sua área de decisão. Durante o intervalo de tempo entre o início e fim dessa coleta, podem ocorrer mudanças no estado do evento, de maneira que a decisão tomada seja influenciada de forma determinante por mensagens desatualizadas. Assim, até que o sistema se estabilize, várias decisões erradas são tomadas.

A existência de um percentual menor de erros desde o primeiro dia de simulação, quando ainda não existem relações de confiança entre os veículos, é justificada pela presença dos ônibus, considerados sempre confiáveis, circulando pela área simulada.

5.4 Impacto das Áreas Geográficas

Nesta seção analisamos a relação entre o tamanho das áreas geográficas ao redor dos eventos simulados e o percentual de decisões indicadas e decisões erradas tomadas pelos veículos, além da quantidade total de falsos positivos detectados pelo RMDTV. As simulações foram executadas em uma rede com 30% de intrusos, na qual o tamanho do raio das áreas geográficas variou segundo os valores mostrados na Tabela 5.3. Os gráficos das Figuras 5.4, 5.5 e 5.6 mostram os resultados obtidos.

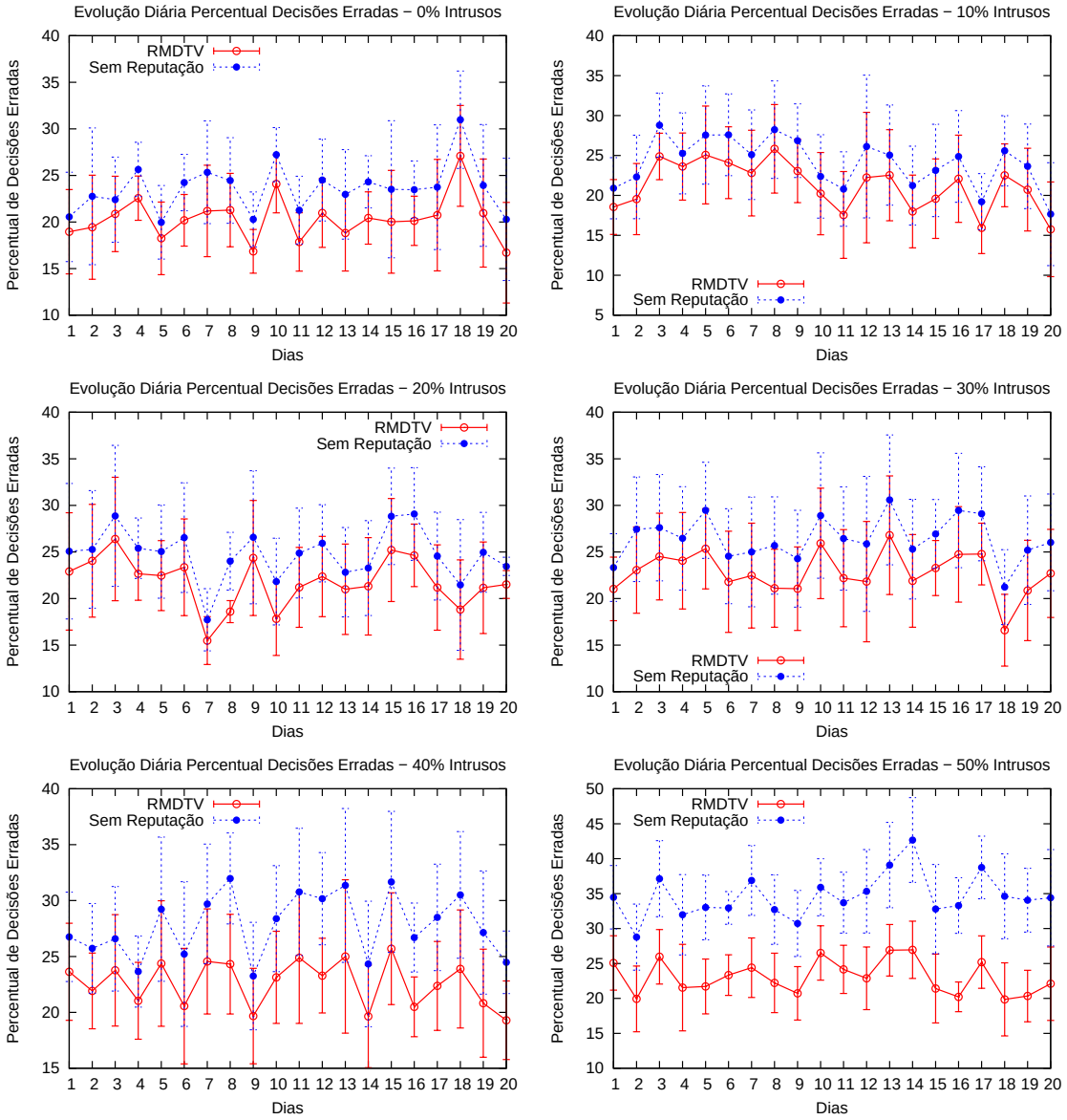

Figura 5.3. Percentual diário de decisões erradas na rede

Podemos perceber que, entre a *distância curta* e a *distância média*, o percentual de decisões indicadas praticamente triplicou. Isso comprova a afirmação de que, com áreas maiores, maior é a quantidade de informações coletadas. Com isso, houve uma redução de aproximadamente 30% no percentual de decisões erradas. Todavia, houve também um aumento de aproximadamente cinco vezes no número de falsos positivos. Assim, embora os veículos tenham recebido mais informações sobre os eventos ocorridos na rede, nem todas eram atualizadas, de forma que algumas decisões tomadas foram comprometidas. Entretanto, mesmo sob o custo de um número maior de falsos positivos, a variação no tamanho das áreas geográficas apresentou um bom desempenho, haja vista a sensível redução nas decisões erradas.

Tabela 5.3. Variação do raio das regiões geográficas de um evento

	curta	**média**	**larga**
Área de reconhecimento	25	50	100
Área de decisão	150	300	600
Área de propagação	350	700	1400

A comparação entre a *distância curta* e a *distância larga*, por sua vez, apresenta os seguintes resultados: com um aumento maior que quatro vezes no percentual de decisões indicadas, houve uma diminuição de aproximadamente 39% no percentual de decisões erradas, com um aumento de aproximadamente nove vezes na quantidade de falsos positivos. Comparadas proporcionalmente, enquanto a *distância média* gerou um custo de cinco vezes (quantidade de falsos positivos) para um benefício de 30% (diminuição da quantidade de decisões erradas), a *distância larga* gerou um custo de nove vezes para um benefício de 39%.

O desempenho de mecanismos de reputação depende, entre outros fatores, do tempo de redenção definido para os membros intrusos. Assim, embora o aumento indefinido da extensão das regiões pareça ser, a princípio, uma boa alternativa no intuito de aumentar o desempenho da rede, uma vez que tende a diminuir o percentual de decisões erradas, a grande quantidade de membros considerados maliciosos erroneamente, pode torná-la, a longo prazo, dependente do tempo de redenção definido. Além disso, dado que em situações reais podem ocorrer vários eventos em uma mesma via, a adoção de áreas muito extensas pode gerar sobreposição de regiões, fazendo com que haja colisão entre as mensagens LDW de eventos distintos.

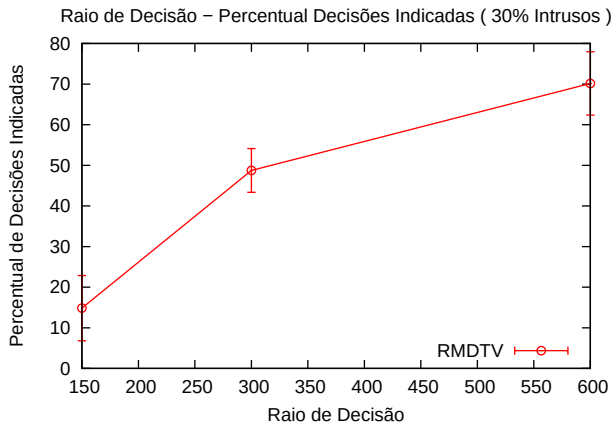

Figura 5.4. Percentual total de decisões indicadas variando o tamanho das áreas geográficas

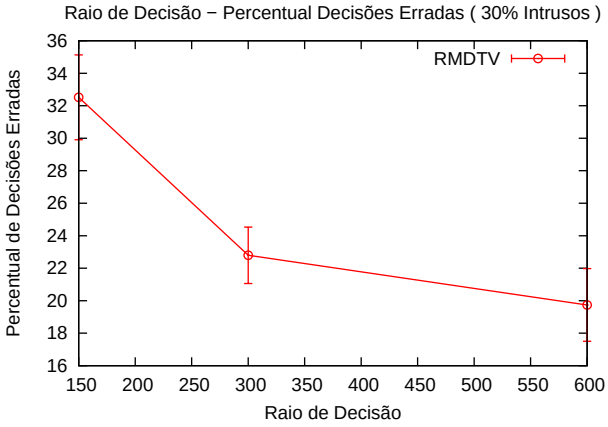

Figura 5.5. Percentual total de decisões erradas variando o tamanho das áreas geográficas

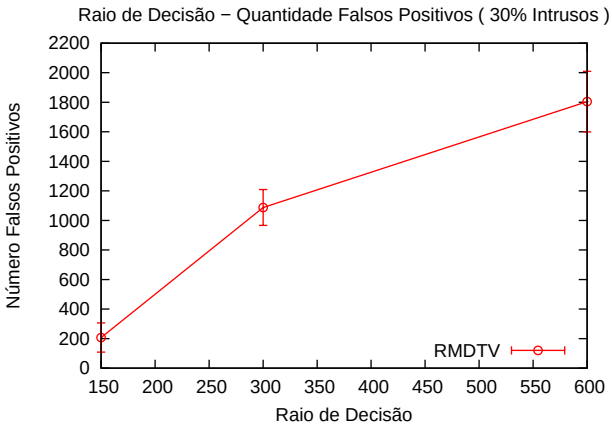

Figura 5.6. Quantidade total de falsos positivos variando o tamanho das áreas geográficas

5.5 Escalabilidade

Nessa seção, a fim de analisar a escalabilidade do RMDTV, comparamos o desempenho entre uma rede na qual nenhum mecanismo de reputação é utilizado e outra na qual o RMDTV é a solução escolhida, submetidas à um percentual de 30% de intrusos. Observamos então o comportamento das duas redes, quanto ao percentual total de decisões erradas tomadas, à medida que a quantidade de veículos aumenta. Variamos a quantidade de veículos entre 60 e 960. O motivo paras esses valores se deve aos limites computacionais do ambiente de simulação empregado. Para executar uma simulação com 960 veículos em um computador QuadCore 2.6GHz, foram necessários em média 5 dias e meio. Por essa razão, para a maior quantidade de veículos, as simulações foram repetidas apenas 3 vezes variando a semente de aleatoriedade.

No cenário com apenas 60 veículos, percebemos que o percentual de decisões erradas

nas redes com e sem reputação é bem parecido. Como existem poucos veículos na rede, a probabilidade de receber informações sobre os eventos existentes é bem baixa, uma vez que as mensagens geradas são encaminhadas apenas dentro da área de disseminação de cada evento. Assim, como a maioria das decisões é tomada de maneira forçada, o mecanismo de reputação não tem efeito algum na qualidade dessas decisões.

À medida que a quantidade de veículos aumenta, mais mensagens sobre os eventos são recebidas pelos veículos dentro de sua área de disseminação. Com mais informações sobre determinado evento, o veículo consegue executar o algoritmo de decisão e posteriormente classificar as origens das mensagens recebidas. A partir dessa classificação, as decisões posteriores tendem a ser mais acertadas, uma vez que se torna possível a distinção entre os veículos confiáveis e aqueles maliciosos pelos receptores das mensagens. Dessa maneira, a rede executando o RMDTV apresenta um resultado melhor que aquela na qual nenhum mecanismo de reputação é utilizado.

Entretanto, a partir de certa quantidade de veículos (480 em nossas simulações), voltamos a observar um desempenho parecido entre os dois cenários simulados. Esse resultado é explicado pelo fato de toda mensagem recebida por um veículo ser reenviada enquanto este estiver dentro da área de disseminação do evento, na tentativa de aproveitar experiências realizadas por veículos que já deixaram a área de disseminação. Assim, ocorre uma saturação de mensagens circulando dentro da área de disseminação ao redor dos eventos, de forma que a quantidade de informações disponíveis é tão grande que poucas decisões são tomadas erroneamente, mesmo no cenário sem reputação.

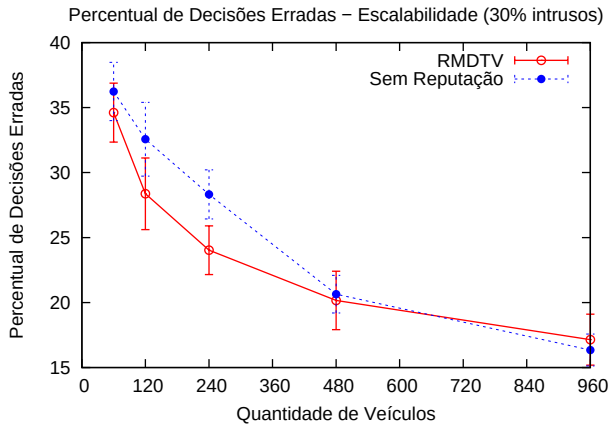

Figura 5.7. Escabilidade do percentual de decisões erradas variando a quantidade de veículos

Embora esperemos que as redes veiculares reais sejam compostas por milhares de veículos, entendemos que essa saturação de mensagens, ocorrida nas regiões mais movimentadas, não invalida o mecanismo proposto, uma vez que sempre existirão regiões de menor circulação, como as periferias das cidades, nas quais a quantidade de veículos

passantes justifica a utilização de um mecanismo de reputação, de forma a aumentar a qualidade das decisões tomadas.

5.6 Tempo de Entrega das Qualificações

Nesta seção analisamos os intervalos de tempo decorridos entre a geração e a entrega das qualificações geradas pelo RMDTV. As simulações foram executadas em uma rede com 30% de intrusos e as médias dos intervalos são mostradas na Figura 5.7.

Podemos perceber que aproximadamente 65% das qualificações são recebidas entre 6 e 18 horas após sua geração. Dado esse considerável atraso, o protocolo de transporte utilizado assume um papel importante no sucesso do mecanismo proposto. Protocolos de transporte atuais, como o TCP, podem finalizar a conexão em caso de grandes atrasos, o que leva a falhas no processo de entrega de qualificações emitidas. Por outro lado, como o UDP não possui garantia de entrega, não existe nenhum controle que possibilite verificar se o destino foi alcançado ou não, quando de seu uso. A utilização dos conceitos das DTNs possibilita que os possíveis atrasos existentes entre a geração e a entrega das qualificações se tornem transparentes para o RMDTV, uma vez que a implementação da camada *bundle* permite o isolamento de tais atrasos através da técnica de armazenagem-e-repasse, ou seja, um veículo deve armazenar uma qualificação recebida até que seja possível repassá-la ao próximo veículo na rede.

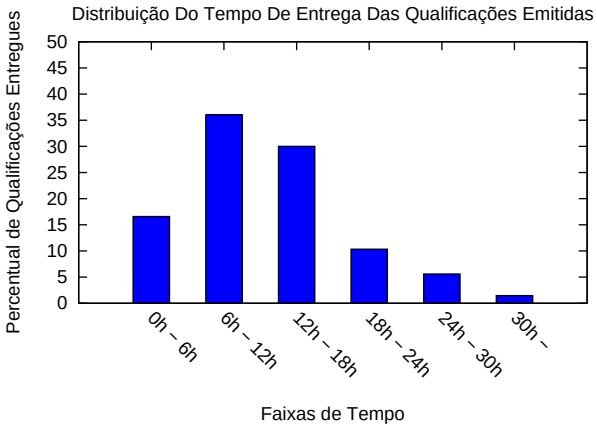

Figura 5.8. Intervalos médios entre a geração e a entrega das qualificações emitidas

5.7 Análise de Sobrecarga

Nesta seção fazemos uma análise da sobrecarga adicionada à rede pelo RMDTV, no que se refere ao consumo da banda disponível pelas mensagens de qualificação e, pos-

teriormente, pela adição dessas qualificações às mensagens de dados enviadas por seus portadores. Avaliamos também a sobrecarga computacional criada pela necessidade de validação dessas qualificações em cada receptor das mensagens de dados geradas.

Mensagens de qualificação contêm a identificação do destino e seu horário de emissão, além da assinatura e do certificado da chave pública de seu emissor. A utilização de uma infraestrutura de chave pública garante a segurança desses dados. Neste trabalho, utilizamos o Algoritmo de Curvas Elípticas (*Elliptic Curve Digital Signature Algorithm* - ECDSA) [Johnson et al., 2001] como solução de criptografia, uma vez que ele é mais leve que o RSA, sem no entanto, comprometer a segurança da rede.

Em [Calandriello et al., 2007] foram realizadas medições do ECDSA 256 bits, utilizando uma máquina equipada com um processador Centrino de 1,5GHz, hardware esse compatível com aquele proposto para as VANETs pelo projeto de Sistemas Cooperativos de Infraestrutura Veicular (*Cooperative Vehicle-Infrastructure Systems* - CVIS) [CVIS, 2009]. A partir dessas medições, foram definidos os seguintes valores para o ECDSA-256:

- ***Tempo de assinatura :*** $\approx$ 0.8 ms;
- ***Tempo de verificação:*** $\approx$ 4,2 ms;
- ***Tamanho da assinatura:*** 64 bytes;
- ***Tamanho da chave pública:*** 33 bytes;
- ***Tamanho da chave privada:*** 32 bytes.

Supondo que 100 bytes sejam suficientes para definir o cabeçalho da mensagem de qualificação, 50 para identificar o veículo qualificado e o horário de geração da qualificação, 64 para a assinatura da qualificação, 64 para o certificado da chave pública do emissor e 33 para essa chave. Assim, o tamanho total de uma mensagem de qualificação é de 311 bytes. Essa mensagem, com uma banda de 1Mbps disponível, ocupa o canal de comunicação por aproximadamente 3,0ms durante sua transmissão, desconsiderando o tempo de estabelecimento de conexão. Como mensagens de qualificação não são distribuídas em modo de difusão pela rede, mas encaminhadas apenas para membros específicos, podemos concluir que a sobrecarga gerada no canal de comunicação por essas mensagens é aceitável no cenário das redes veiculares.

Qualificações recebidas devem ser adicionadas por seu portador a todas as mensagens de dados por ele geradas. A partir do cálculo realizado acima, concluímos que a adição de uma qualificação aumenta em 211 bytes o tamanho da mensagem de dados. Seja cada qualificação válida por 30 dias e o limite máximo permitido de qualificações

adicionadas às mensagens igual a 30, equivalente a uma por dia, temos então um aumento total, no pior caso, de 6330 bytes por mensagem. Sejam 200 bytes suficientes para os dados relativos ao cabeçalho e às informações do evento, o tamanho final de uma mensagem de dados pode atingir até 6530 bytes. A transmissão desses dados, por um enlace de 1Mbps, leva aproximadamente 55,0ms. Seja um veículo movendo-se em linha reta a uma velocidade de 60Km/h (16,67m/s), velocidade máxima permitida na maioria das avenidas brasileiras dentro da área de disseminação de um evento. Sejam os raios das áreas de disseminação e decisão, respectivamente, 700 e 300 metros (Seção 5.4). Esse veículo tem aproximadamente 24s (400m / 16,67m/s) para colher informações, antes de tomar a decisão sobre o evento, caso não receba dados gerados por uma fonte confiável. Logo, ele pode receber, durante a coleta de dados, aproximadamente 436 mensagens (24000ms / 55ms), quantidade essa mais que suficiente para evidenciar a existência ou não do evento.

Uma vez dentro da área de decisão, o veículo executa o processo descrito na Subseção 4.2.1, caso não tenha recebido dados gerados por fontes confiáveis. Nesse processo, pode ser preciso validar as qualificações anexadas às mensagens recebidas. Seja 22 o valor de x utilizado pelo método *Maioria das últimas x mensagens considerando um limite inferior*, como proposto em [Ostermaier et al., 2007]. O tempo total de validação das qualificações, quando nenhuma chave pública é conhecida pelo receptor das informações, é dado por: 4,2ms(verificação da chave pública do emissor da qualificação) + 4,2ms(verificação da qualificação) = 8,4ms * 22 * 30 $\approx$ 5,6s. Seja a velocidade de deslocamento do veículo igual a 60Km/h (16,67m/s), ele percorre então aproximadamente 93m durante a execução dessa validação. Essa distância não compromete o processo de decisão, pois, se considerarmos os raios das áreas de decisão e reconhecimento com 300 e 50 metros (Seção 5.4), respectivamente, ainda é possível ao veículo tomar a decisão antes de atingir a área de reconhecimento do evento. Além disso, como as qualificações são utilizadas apenas como critério de desempate no processo de decisão, sua verificação completa nem sempre é necessária.

5.8 Conclusão

Este capítulo apresentou uma avaliação por simulação do mecanismo de reputação RMDTV. As simulações procuraram se aproximar de um cenário real, no qual a rede é composta por veículos utilizados por seus proprietários em deslocamentos seguindo *Working Day Movement*, discutido na Seção 2.4.

Analisamos e comparamos o desempenho de uma rede executando o RMDTV com outra na qual nenhum mecanismo de reputação é utilizado. Os resultados obtidos mos-

traram que o RMDTV aumenta consideravelmente a qualidade das decisões tomadas em uma rede sob ataques do tipo alarmes trocados, proporcionando uma melhoria entre 14% (rede sem intrusos) e 45% (rede com 50% de intrusos).

Percebemos que o aumento do tamanho das áreas geográficas ao redor de um evento pode proporcionar melhores resultados nas decisões tomadas. Entretanto, a partir de certo ponto, o número de falsos positivos gerados passa a ser muito alto. Assim, como no RMDTV mensagens e qualificações emitidos por membros da rede considerados maliciosos são sumariamente descartados, a longo prazo o desempenho da rede pode se deteriorar consideravelmente, dada a indisponibilidade de fontes confiáveis.

Analisamos a escalabilidade do RMDTV variando a quantidade de veículos na rede. Os resultados mostraram que em uma rede com poucos veículos, a quantidade de informações recebidas é insuficiente para influenciar o processo de tomada de decisão, de forma que o estabelecimento de relações de confiança entre os veículos é quase nulo. À medida que a quantidade de veículos aumenta percebemos que o percentual de decisões erradas diminui não só pelo recebimento de mais informações sobre os eventos, mas também pelo estabelecimento de relações de confiança entre os veículos. Todavia, a partir de certo ponto, ocorre uma saturação da quantidade de informações disponíveis sobre os eventos, de forma que o percentual de decisões tomadas erroneamente, mesmo quando da inexistência de qualquer mecanismo de reputação, se iguala ao resultado obtido quando o RMDTV é utilizado. Todavia, entendemos que este resultado não invalida o RMDTV, haja vista que sempre existirão regiões de menor circulação nas quais o estabelecimento de reputações contribuirá para um aumento na qualidade das decisões tomadas pelos veículos.

Percebemos que o uso dos conceitos de Redes Tolerantes a Atrasos e Desconexões neste trabalho teve também importância significativa nos resultados obtidos pelo RMDTV, uma vez que os consideráveis atrasos existentes entre a geração e o recebimento das qualificações emitidas poderiam inviabilizar o mecanismo proposto, caso fossem utilizados protocolos de transporte tradicionais, como o TCP e o UDP.

Embora a execução do RMDTV adicione certa sobrecarga à rede, resultado da definição de um novo tipo de mensagem e da adição das qualificações recebidas pelos veículos às mensagens de dados geradas, mostramos que o mecanismo, de maneira geral, não prejudica o desempenho da aplicação, uma vez que possibilita aos veículos a recepção de uma quantidade suficiente de informações sobre o evento durante a fase de coleta de dados e, posteriormente a esse passo, permite também a tomada de decisão em tempo hábil para que ações no intuito de minimizar os efeitos do evento possam ser executadas em segurança pelo conjunto veículo-motorista.

Capítulo 6

Conclusões

O sucesso de aplicações em redes veiculares depende principalmente da cooperação de todos os veículos em prol do benefício coletivo. Todavia, existe sempre o risco de um ou mais membros agirem de forma egoísta, condicionando seu comportamento ao atendimento de objetivos pessoais, geralmente diferentes do interesse geral. Mecanismos de reputação contribuem para a resolução deste problema, uma vez que permitem aos membros da rede a escolha de pares para a realização de transações com base em seu histórico comportamental, aumentando assim a probabilidade de resultados satisfatórios advindos dessas transações.

Neste trabalho, propusemos um mecanismo de reputação para redes veiculares, o RMDTV, que possibilita aos membros da rede atestar a confiabilidade das informações emitidas por outros veículos. Esse mecanismo faz uso de qualificações emitidas por terceiros e roteadas pela rede mesmo sob condições de desconectividade, aliadas às experiências que o próprio membro teve com os emissores dessas qualificações, certificadas por uma Autoridade Certificadora

Analisamos o RMDTV utilizando o modelo de mobilidade conhecido como *Working Day Movement*, que reflete o comportamento de pessoas durante um dia normal de trabalho. O cenário escolhido para as simulações foi uma seção do mapa digital de Belo Horizonte, representando parcialmente as regiões central e norte da cidade. A rede veicular simulada executava uma aplicação distribuída de segurança, na qual seus membros trocavam mensagens informando as condições de tráfego em pontos específicos da cidade. Os resultados obtidos mostraram que o RMDTV é um mecanismo de reputação escalável capaz aumentar consideravelmente a resiliência de redes veiculares sujeitas a ataques do tipo alarmes trocados, em comparação com cenários onde nenhum mecanismo de reputação é utilizado. Essa melhoria é obtida sem que o mecanismo crie uma sobrecarga capaz de prejudicar o desempenho geral da aplicação executada.

6.1 Contribuições

As atividades realizadas durante a execução deste trabalho trouxeram as seguintes contribuições:

- Levantamento do estado da arte em soluções de segurança para alguns tipos de sistemas distribuídos, como redes P2P, MANETs e VANETs.
- Identificação dos desafios específicos relacionados à proposição de soluções de segurança em redes veiculares.
- Concepção e implementação de um mecanismo de reputação para redes veiculares tolerantes a atrasos e desconexões, chamado RMDTV.
- Avaliação do mecanismo proposto através de simulações, comprovando sua eficácia na diminuição da quantidade de decisões erradas tomadas pelos veículos da rede acerca de eventos existentes nas vias de tráfego.

6.2 Trabalhos Futuros

Como trabalho futuro, é possível continuar o desenvolvimento do RMDTV alterando a forma de classificação dos veículos em confiáveis ou intrusos. Atualmente, se um nó apresenta um comportamento cooperativo em uma única transação, já é promovido a confiável. A mesma coisa acontece para aqueles que agem de maneira maliciosa uma única vez, rebaixados à condição de intrusos imediatamente. Considerando-se que mensagens enviadas por membros confiáveis têm um peso muito grande no processo de decisão, enquanto aquelas enviadas por intrusos são totalmente descartadas, acreditamos que a definição de funções de promoção e rebaixamento progressivos pode aumentar o desempenho do sistema, uma vez que a quantidade de membros promovidos a confiáveis ou rebaixados a intrusos erroneamente tende a diminuir consideravelmente.

Outra possibilidade seria avaliar o desempenho da rede em situações nas quais é permitido aos membros a publicação das informações de reputação armazenadas localmente nas listas de confiabilidade. Essa troca de informações permitiria uma maior convergência das opiniões sobre os comportamentos dos veículos da rede. Além disso, tais dados poderiam ser utilizados pela Autoridade Certificadora para a elaboração e divulgação de Listas de Revogação de Certificados (LRC), a fim de revogar as chaves dos veículos de comportamento malicioso.

Por fim, com o objetivo de aumentar a confiabilidade dos resultados obtidos nas redes simuladas, seria interessante variar também as distribuições estatísticas utilizadas

no *Working Day Movement*, além de avaliar também o desempenho do RMDTV em redes funcionando sob a regência de outros modelos de mobilidade.

Referências Bibliográficas

Adler, C. e Strassberger, M. (2006). Putting together the pieces - a comprehensive view on cooperative local danger warning. In *ITS '06: Proceedings of 13th ITS World Congress and Exhibition on Intelligent Transport Systems and Services*.

BHTRANS (2009). Empresa de transportes e trânsito de belo horizonte. `http://www.bhtrans.pbh.gov.br`.

Buchegger, S. e Le Boudec, J. Y. (2004). A robust reputation system for p2p and mobile ad-hoc networks. In *Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems*.

Burgess, J.; Gallagher, B.; Jensen, D. e Levine, B. N. (2006). Maxprop: Routing for vehicle-based disruption-tolerant networks. In *INFOCOM 2006: Proceedings of the 25th IEEE International Conference on Computer Communications*, pp. 1–11.

Calandriello, G.; Papadimitratos, P.; Hubaux, J.-P. e Lioy, A. (2007). Efficient and robust pseudonymous authentication in vanet. In *VANET '07: Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, pp. 19–28, New York, NY, USA. ACM.

Car2Car (2009). Car2car communication consortium. `http://www.car-2-car.org`.

Cerf, V.; Burleigh, S.; Hooke, A.; Torgerson, L.; Durst, R.; Scott, K.; Fall, K. e Weiss, H. (2007). Delay-tolerant networking architecture. Technical report, Internet RFC 4838.

Cerf, V.; Burleigh, S.; Hooke, A.; Torgerson, L.; Durst, R.; Scott, K.; Travis, E. e Weiss, H. (2001). Interplanetary internet (ipn): Architectural definition. Technical report, IPN Research Group.

Choffnes, D. R. e Bustamante, F. E. (2005). An integrated mobility and traffic model for vehicular wireless networks. In *VANET '05: Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pp. 69–78, New York, NY, USA. ACM.

CVIS (2009). The cooperative vehicle-infrastructure systems project. http://www.cvisproject.org/.

Dewan, P. e Dasgupta, P. (2004). Securing reputation data in peer-to-peer networks. In *PDCS: Proceedings International Conference on Parallel and Distributed Computing and Systems*, MIT Cambridge, USA.

Dewan, P.; Dasgupta, P. e Bhattacharya, A. (2004). On using reputations in ad hoc networks to counter malicious nodes. In *ICPADS '04: Proceedings of the Parallel and Distributed Systems, Tenth International Conference*, p. 665, Washington, DC, USA. IEEE Computer Society.

Dotzer, F.; Fischer, L. e Magiera, P. (2005). Vars: A vehicle ad-hoc network reputation system. In *WOWMOM '05: Proceedings of the Sixth IEEE International Symposium on World of Wireless Mobile and Multimedia Networks*, pp. 454–456, Washington, DC, USA. IEEE Computer Society.

DSRC (2009). Dedicated short range communications. http://grouper.ieee.org/groups/scc32/dsrc/index.html.

Ekman, F.; Keränen, A.; Karvo, J. e Ott, J. (2008). Working day movement model. In *MobilityModels '08: Proceedings of the 1st ACM SIGMOBILE workshop on Mobility models*, pp. 33–40, New York, NY, USA. ACM.

Fall, K. (2003). A delay-tolerant network architecture for challenged internets. In *SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 27–34, New York, NY, USA. ACM.

Härri, J.; Filali, F. e Bonnet, C. (2007). Mobility Models for Vehicular Ad Hoc Networks: A Survey and Taxonomy. Technical report, Technical Report RR-06-168, Institut Eurecom, January 2007.

Hubaux, J. P.; Čapkun, S. e Luo, J. (2004). The security and privacy of smart vehicles. *IEEE Security and Privacy*, 2(3):49–55.

Izquierdo, M. R. e Reeves, D. S. (1999). A survey of statistical source models for variable-bit-rate compressed video. *Multimedia Syst.*, 7(3):199–213.

Johnson, D.; Menezes, A. e Vanstone, S. A. (2001). The elliptic curve digital signature algorithm (ecdsa). *Int. J. Inf. Sec.*, 1(1):36–63.

Johnson, D. B. e Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In *Mobile Computing*, pp. 153–181. Kluwer Academic Publishers.

Juang, P.; Oki, H.; Wang, Y.; Martonosi, M.; Peh, L. S. e Rubenstein, D. (2002). Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet. *SIGARCH Comput. Archit. News*, 30(5):96–107.

Keränen, A.; Ott, J. e Kärkkäinen, T. (2009). The one simulator for dtn protocol evaluation. In *SIMUTools '09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, pp. 1–10, Rome, Italy. ACM.

Kosch, T. (2004). Local danger warning based on vehicle ad-hoc networks: Prototype and simulation. In *WIT '04: Proceedings of 1st International Workshop on Intelligent Transportation*.

Li, M. e Lou, W. (2008). Opportunistic broadcast of emergency messages in vehicular ad hoc networks with unreliable links. In *QShine '08: Proceedings of the 5th International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, pp. 1–7, ICST, Brussels, Belgium.

Manet (2009). Internet engineering task force manet working group. `http://www.ietf.org/html.charters/manet-charter.html`.

OpenJUMP (2009). The free, java-based and open source geographic information system for the world. `http://www.openjump.org/`.

Ostermaier, B. (2005). Analysis and improvement of inter-vehicle communication security by simulation of attacks. Master's thesis, Technische Universität München.

Ostermaier, B.; Dotzer, F. e Strassberger, M. (2007). Enhancing the security of local danger warnings in vanets - a simulative analysis of voting schemes. In *ARES '07: Proceedings of the The Second International Conference on Availability, Reliability and Security*, pp. 422–431, Washington, DC, USA. IEEE Computer Society.

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

Patwardhan, A.; Joshi, A.; Finin, T. e Yesha, Y. (2006). A data intensive reputation management scheme for vehicular ad hoc networks. In *Proceedings of the Second International Workshop on Vehicle-to-Vehicle Communications*. IEEE.

Raya, M. e Hubaux, J. P. (2005). The security of vehicular ad hoc networks. In *SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pp. 11–21, New York, NY, USA. ACM.

Seth, A.; Kroeker, D.; Zaharia, M.; Guo, S. e Keshav, S. (2006). Low-cost communication for rural internet kiosks using mechanical backhaul. In *MobiCom '06: Proceedings of the 12th annual international conference on Mobile computing and networking*, pp. 334–345, New York, NY, USA. ACM.

Sun, Q. e Garcia-Molina, H. (2004). Using ad-hoc inter-vehicle networks for regional alerts. Technical Report 2004-51, Stanford InfoLab.

Swamynathan, G.; Zhao, B. Y.; Almeroth, K. C. e Zheng, H. (2007). Globally decoupled reputations for large distributed networks. *Adv. MultiMedia*, 2007(1):12–12.

Wang, Z. e Chigan, C. (2007). Countermeasure uncooperative behaviors with dynamic trust-token in vanets. In *ICC '07: Proceedings of IEEE International Conference on Communications*, pp. 3959–3964, Glasgow, Scotland. IEEE.

Warthman, F. (2003). Delay-tolerant networks. Technical report, A Tutorial. DTN Research Group Internet Draft.

Xue, F. e Kumar, P. R. (2004). The number of neighbors needed for connectivity of wireless networks. *Wirel. Netw.*, 10(2):169–181.

Yang, G.; Chen, L.-J.; Sun, T.; Zhou, B. e Gerla, M. (2006). Ad-hoc storage overlay system (asos): A delay-tolerant approach in manets. In *MASS '06: Proceeding of the 3rd IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, pp. 296–305.

Zimmermann, P. (1994). Pgp user's guide. Cambridge, MA: MIT Press.