REDES SOCIAIS PARA CONFIANÇA EM REDES VEICULARES TOLERANTES A INTERRUPÇÕES

THIAGO RODRIGUES DE OLIVEIRA

REDES SOCIAIS PARA CONFIANÇA EM REDES VEICULARES TOLERANTES A INTERRUPÇÕES

Tese apresentada ao Programa de Pós-Graduação em Ciência da Computação do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais como requisito parcial para obtenção do grau de Doutor em Ciência da Computação.

ORIENTADOR: JOSÉ MARCOS SILVA NOGUEIRA

CO-ORIENTADOR: DANIEL FERNANDES MACEDO

Belo Horizonte

Dezembro de 2016

O48r Oliveira, Thiago Rodrigues de
Redes sociais para confiança em redes veiculares tolerantes a interrupções / Thiago Rodrigues de Oliveira. – Belo Horizonte, 2016
173f. : il.; 29cm.

Tese (doutorado) – Universidade Federal de Minas Gerais
Orientador: José Marcos da Silva Nogueira
Coorientador: Daniel Fernandes Macedo.

1. Computação - Teses. 2. Redes de computadores - Medidas de segurança. 3 Redes de computação - segurança. 4. Gerenciamento de redes. 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

Redes sociais para certificação em redes veiculares tolerantes a interrupções

THIAGO RODRIGUES DE OLIVEIRA

Tese defendida e aprovada pela banca examinadora constituída pelos Senhores:

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

PROF. DANIEL FERNANDES MACEDO - Coorientador
Departamento de Ciência da Computação - UFMG

PROF. EDMUNDO ROBERTO MAURO MADEIRA
Instituto de Computação - UNICAMP

PROF. MARIO SÉRGIO FERREIRA ALVIM JÚNIOR
Departamento de Ciência da Computação - UFMG

PROFª. MICHELE NOGUEIRA LIMA
Departamento de Informática - UFPR

PROF. LUIZ HENRIQUE ANDRADE CORREIA
Departamento de Ciência da Computação - UFLA

Belo Horizonte, 15 de janeiro de 2016.

Agradecimentos

Agradeço primeiramente a Deus, é d'Ele a vitória alcançada em minha vida! O tempo de oração diminuiu, mas não a fé. Durante este trabalho, muita coisa aconteceu e uma pessoa chegou para ficar na minha vida: agradeço muito à Cíntia, minha esposa e companheira, que incentivou nos momentos difíceis mesmo grávida de nossos filhos gêmeos na reta final. Pedro e Thiago José ainda chegaram para fazer parte desta história!

A família é fundamental em cada conquista, pelo incentivo e confiança. Agradeço à minha mãe, pela vontade de estudar e transmitir conhecimento. Ao meu pai, que sempre será lembrado. À minha sogra, meus irmãos e madrinha, também os cunhados e outros amigos que se tornaram presentes me apoiando.

Ao meu orientador José Marcos, por toda a atenção e exemplo antes e durante o doutorado. Também ao orientador Daniel, que colaborou muito desde o início deste trabalho. Aos amigos do laboratório Winet, especialmente Vinícius e Ewerton, que ajudaram na construção deste trabalho. Todos os professores da UFSJ e amigos do DCC, que proporcionam constante aprendizado.

Aos amigos que confiaram em mim e que tudo seria possível.

Resumo

Redes veiculares tolerantes a interrupções são redes *ad hoc* móveis em que a comunicação pode sofrer longas interrupções, são formadas por motoristas em busca de informações. Em regiões urbanas ou rodovias, geralmente não existe uma infraestrutura de rede ou a sua cobertura não é contígua. Disponibilizar novas tecnologias e aplicações tornará mais seguro o trânsito nas ruas e avenidas por meio de maior comunicação entre os motoristas. A rede deve incluir mecanismos para garantir a confiança e a segurança das fontes de informação, pois pessoas podem ser tendenciosas ou serem induzidas a divulgar informações falsas para ganhos pessoais. O envio de informações considera que os requisitos de segurança variam de acordo com o cenário e a situação da utilização das redes veiculares, assim como a comunicação tolerante a interrupções inclui desafios de segurança para gerenciamento de chaves. Este trabalho propõe estabelecer confiança em redes veiculares por meio de redes sociais, com utilização de certificação (SNVC – *Social Networks for Vehicular Certification*). Assim, possibilita o compartilhamento de chaves por meio de contato direto entre duas pessoas que se conhecem e garantem sua confiança, então um assina o certificado do outro. Um certificado assinado por um terceiro é validado se a outra parte tiver armazenada a chave pública desse usuário, que seja um amigo em comum na rede social. Um mecanismo de reputação associado ainda possibilita aos motoristas beneficiados gerar uma assinatura para identificar usuários que colaboram com a rede social proposta. A partir do relacionamento e conhecimento prévio dos usuários da rede veicular, são definidos critérios de confiança na seleção de mensagens para prover segurança. As avaliações realizadas utilizam *traces* reais de mobilidade e mostram o comportamento de uma rede veicular com a utilização de redes sociais para estabelecer confiança entre os usuários. Os resultados encorajam o aumento de amigos como uma forma de melhorar a troca de mensagens confiáveis, bem como a atribuição de reputação promove o reconhecimento de usuários confiáveis.

Palavras-chave: *redes sociais, redes veiculares, segurança em DTN, redes DTN, confiança, reputação, certificados, gerenciamento de chaves, mecanismos de segurança.*

Abstract

Vehicular Disruption Tolerant Networks are mobile ad hoc networks that may suffer from long interruptions, they appear due to the search of information by drivers. In urban areas or roads, generally there is no network infrastructure or their coverage is not contiguous. Provide new technologies and applications can become safer traffic in the streets and avenues through increased communication among users. The network should incorporate mechanisms to assert the trust and reliability of the information sources because humans can be biased or may be compelled to disseminate false information for personal gains. Sending information should consider the security requirements may vary depending on the scenario and situation of the use of vehicular networks such as the need for tolerance to interruptions. This work proposes to establish trust by means of social networks, using certification as SNVC – Social Networks for Vehicular Certification. It enables cars to share keys through direct contacts between two acquaintances that warrant their identity, so they sign a reciprocal certificate. Certificates signed by a friend can be validated if the public key of this user is available to the other party, that can be other user who knows this friend too and they are friends in common on the social network. Further, the reputation mechanism can identify certificates of users that collaborate with the proposed social network. From the relationship and previous knowledge of the vehicular network users, criterias of trust are defined for the selection of messages enabling secure communication. The evaluations performed include real mobility traces and show the behavior of a vehicular network that uses social networks to establish trust between users. The results encourage the increase of friends as a way to improve the exchange of reliable messages, as well as the attribution of reputation promotes the recognition of reliable users.

Keywords: *social networks, vehicular networks, DTN security, DTN networks, certificates, trust, reputation, key management, security mechanisms.*

Sumário

1. **Introdução** **21**

1.1. Definições *23*

1.2. Problema *24*

1.3. Objetivos *25*

1.4. Contribuições *27*

1.5. Estrutura do documento *28*

2. **Conceitos Fundamentais** **29**

2.1. Redes Veiculares *29*

2.2. Redes Tolerantes a Interrupções (DTN) *32*

2.3. VANETs ou vDTN? *35*

2.4. Gerenciamento de chaves *38*

2.5. Certificação digital *40*

2.6. Confiança e reputação *42*

2.7. Redes sociais *44*

2.8. Conclusão *46*

3. **Segurança em Redes Veiculares** **49**

3.1. Requisitos de segurança *49*

3.2. Mecanismos de segurança *53*

3.2.1. Mecanismos de reputação 53

3.2.2. Detecção de intrusos 54

3.2.3. Mecanismos criptográficos 55

3.3. Desafios de segurança em DTN *57*

3.4. Ataques de segurança em vDTN *62*

3.5. Segurança na arquitetura WAVE *66*

3.6. Conclusão *67*

4. **Trabalhos Relacionados** **69**

4.1. Confiança em VANETs *70*

4.2. Redes sociais veiculares *76*

4.3. Redes DTN e infraestrutura *78*

4.4. Taxonomia *82*

4.5. Conclusão *85*

5. **Redes Sociais para Confiança** **87**

5.1. Modelo de rede veicular *87*

5.2. Modelo de relacionamentos *89*

5.3. Modelo de confiança *90*

5.3.1. Graus de confiança 93

5.3.2. Visão geral 95

5.3.3. Certificação SNVC 100

5.3.4. Reputação certificada 103

5.3.5. Remoção de amigos 107

5.3.6. Ataques evitados 110

5.3.7. Aplicações *versus* privacidade 111

5.4. Conclusão *114*

6. **Avaliação** **117**

6.1. Metodologia aplicada *118*

6.2. Cenário *120*

6.3. Resultados e discussão *122*

6.4. Avaliação com traces de mobilidade *127*

6.5. Conclusão *136*

7. **Estudo comparativo** **139**

7.1. Metodologia e comparação *139*

7.2. Cenário da comparação *142*

7.3. Resultados e análise *145*

7.4. Conclusão *151*

8. **Conclusões** **153**

8.1. Contribuições *154*

8.2. Trabalhos futuros *156*

9. **Referências Bibliográficas** **157**

Lista de Figuras

2.1. Exemplos do modelo de uma rede veicular 29

2.2. Pilha de protocolos da Internet e de uma DTN 32

4.1. Taxonomia de propostas em relação aos temas abordados 82

5.1. Relacionamentos de A antes e depois de adicionar B como amigo 89

5.2. Relacionamentos antes e depois de A adicionar o usuário E como amigo 90

5.3. Diagrama de participação de usuários 95

5.4. Algoritmo principal 96

5.5. Diagrama de reconhecimento de mensagens confiáveis 97

5.6. Algoritmo para validar mensagens por grau de confiança 97

5.7. Algoritmo de adição de amigos 99

5.8. Diagrama de eventos da adição de amigos 100

5.9. Diagrama de participação de usuários no mecanismo de reputação 101

5.10. Algoritmo de atribuição e propagação de bônus de reputação 102

5.11. Relacionamentos antes e depois de D atribuir bônus de reputação a G 103

5.12. Diagrama de eventos da reputação de usuários 104

5.13. Algoritmo de cômputo da reputação 104

5.14. Algoritmo para remoção de amigos 106

5.15. Diagrama de eventos da remoção de amigos 106

5.16. Usuário D antes e depois de remover o usuário B como amigo 107

6.1. Cenário das simulações com modelo sintético 119

6.2. Percentual médio de usuários confiáveis por cada nó da rede veicular 121

6.3. Mensagens confiáveis em relação a recebidas por nós da rede 121

6.4. Impacto da reputação e de amigos de amigos com 20% de amigos na rede 122

6.5. Impacto da reputação e amigos de amigos na seleção de mensagens confiáveis 122

6.6. Impacto de intrusos e reputação negativa 123

6.7. Média de atraso na entrega de mensagens 124

6.8. Percentual de usuários confiáveis (DieselNet) 127

6.9. Percentual de mensagens confiáveis (DieselNet) 128

6.10. Mediana e média do atraso das mensagens entregues (DieselNet) 128

6.11. Percentual de usuários confiáveis nos *traces* 129

6.12. Percentual de mensagens confiáveis nos *traces* 129

6.13. Percentual de mensagens confiáveis por reputação 130

6.14. Percentual de mensagens ignoradas por reputação negativa 131

6.15. Média do atraso com modelo de confiança ou todos confiáveis 132

6.16. *Overhead* de mensagens com utilização do SNVC nos *traces* utilizados 132

7.1. Cenário da comparação e representação no simulador 141

7.2. Decisões certas em relação ao total de mensagens recebidas 144

7.3. Decisões indicadas do RMDTV em relação a decisões da rede social 144

7.4. Redução de tempo para tomada de decisões 145

7.5. Decisões erradas em relação à probabilidade de contato entre usuários 146

7.6. Decisões erradas afetadas por intrusos ou falsos positivos 146

7.7. Percentual de mensagens confiáveis em relação às analisadas pelo RMDTV 147

Lista de Tabelas

2.1 Comparativo de redes DTN e MANET 36

4.1. Comparativo de propostas em relação aos temas abordados 81

5.1. Modelo de relacionamento entre usuários no grafo da rede social 88

5.2. Lista de amigos e usuários confiáveis após A adicionar B 90

5.3. Lista de amigos e usuários confiáveis após A adicionar E 90

5.4. Graus de confiança segundo modelo proposto 92

6.1. Características do cenário da avaliação 120

6.2. Métricas e resultados sumarizados da avaliação 125

6.3. Características dos *traces* utilizados na avaliação 127

6.4. Métricas e resultados aproximados na avaliação com *traces* reais 133

7.1. Matriz de confusão para decisões do RMDTV 139

7.2. Características do cenário e modelo de rede da comparação 142

7.3. Métricas e resultados qualitativos da comparação 148

Lista de Abreviaturas

CA	*Certificate Authority*
DSRC	*Dedicate Short-range Communications*
DTN	*Disruption Tolerant Networks*
GPS	*Global Position System*
MANET	*Mobile Ad Hoc Networks*
ONE	*Opportunistic Networking Evaluator*
P2P	*Peer-to-Peer*
PGP	*Pretty Good Privacy*
PKI	*Public Key Infrastructure*
RMDTV	*Reputation Mechanism for Delay Tolerant Vehicular Networks*
SNVC	*Social Network for Vehicular Certification*
vDTN	Vehicular *Disruption Tolerant Networks*
WAVE	*Wireless Access in the Vehicular Environment*
VANET	*Vehicular Ad Hoc Networks*
V2I	*Vehicle-to-Infrastructure*
V2V	*Vehicle-to-Vehicle*

Capítulo 1

Introdução

As redes veiculares *(VANETs - Vehicle Ad Hoc NETworks)* são redes de computadores sem fio denominados como nós móveis em veículos, que possivelmente incluem também equipamentos fixos localizados às margens das ruas e estradas, nas quais a comunicação ocorre entre veículos e de veículos com algum ponto de acesso fixo. As aplicações para informações dessas redes são inúmeras e diversificadas, que levarão à otimização de recursos, economia de tempo, redução de consumo, previsão de congestionamentos, entre outras vantagens [Alves, 2009].

O surgimento de redes veiculares é favorecido pela popularização de dispositivos móveis como *notebooks, tablets e smartphones* com mais recursos disponíveis, utilizados por motoristas e autoridades de trânsito para compartilhar dados em qualquer lugar ou tempo [Silva, 2013]. Alguns desses equipamentos poderão estar conectados à Internet móvel nas áreas urbanas, facilitando a divulgação e obtenção de informações sobre o trânsito como definição de rotas, alerta sobre acidentes etc. Será possível fornecer outras informações úteis ao motorista, tais como: informações meteorológicas; eventos do trânsito como congestionamentos, desvios, mudanças em sentido de direção de vias, barreiras e obstáculos; vagas para estacionamento; descontos e localização de postos de combustíveis; e até informações sobre o veículo, como velocidade, consumo e problemas mecânicos por meio de conexão física com sensores nos veículos.

As redes veiculares são heterogêneas e utilizam a infraestrutura existente nas cidades como as redes metropolitanas e os dispositivos dos próprios usuários, que já incluem mapas e GPS [Alves, 2009]. Para possibilitar conexões entre dispositivos móveis sem a necessidade de infraestrutura de rede, os motoristas formam redes *ad hoc* veiculares. Devido às mudanças rápidas na topologia, o modelo de rede DTN (*Disruption Tolerant Networks*) [Fall, 2003] é aplicado com frequência, pois os protocolos de roteamento

convencionais de redes *ad hoc* não funcionam de forma eficiente em ambientes veiculares [Luo, 2008].

Os conceitos e tecnologia DTN [Fall, 2003][Mota, 2009] são mais adequados para redes com interrupções de comunicação, como redes veiculares. Em redes DTN, a comunicação é assíncrona e não há necessidade de um caminho fim-a-fim, o que as torna adequadas para uso em redes com conectividade intermitente ou sujeitas a atrasos longos [Fall, 2004]. Os nós seguem o paradigma guardar-carregar-repassar (*store-carry-forward*), o que possibilita que nós mantenham mensagens temporariamente em *buffer* caso não haja conexão direta com o próximo passo ou com o destino.

Neste trabalho, são abordadas redes veiculares em que a comunicação entre veículos é intermitente e a transmissão dos dados é tolerante a atrasos e interrupções. Tais redes são denominadas DTN veiculares (vDTN) [Pereira, 2012], que exploram o movimento físico dos veículos e contatos oportunísticos (no primeiro momento possível) para transportar dados entre partes desconectadas da rede.

As aplicações de redes DTN veiculares apresentam grande potencial e terão impacto considerável no cotidiano das pessoas. Entretanto, tais aplicações são limitadas em relação à segurança e à privacidade [Burgess, 2007], particularmente quando se consideram vDTN com características específicas, como mobilidade imprevisível e latência variável. A segurança torna-se mais desafiadora em redes DTN, um exemplo trata-se da necessidade de definição de novos mecanismos de gerenciamento de chaves [Symington, 2011].

A motivação deste trabalho é a necessidade de suprir as redes veiculares com mecanismos para aumentar a confiança das informações na comunicação entre usuários. Os motoristas visam obter e divulgar informações relacionadas à alteração de rotas de trânsito. Algum desses usuários pode tentar interferir nas rotas dos demais, por exemplo, o gerente de um posto de combustível com objetivo de atrair clientes. Nesse contexto, observa-se a necessidade de estabelecer confiança entre usuários na troca de mensagens para comunicação segura, mesmo não havendo conexão no momento do envio das mensagens.

O desafio para estabelecer confiança entre os usuários é maior em redes DTN, pois nenhum esquema de gerenciamento de chaves ainda é reconhecido como adequado para redes tolerantes a interrupções [Symington, 2011][Lv, 2014]. É necessária uma alternativa que torne viável o gerenciamento de chaves criptográficas nos ambientes de conectividade intermitente, pois é impraticável serviço de distribuição de chaves ou checagem *on-line*, o que ainda é uma questão em aberto em vDTN.

Este trabalho propõe um modelo de confiança baseado em redes sociais, que utiliza certificação (SNVC – *Social Networks for Vehicular Certification*) para estabelecer confiança entre usuários da rede, como alternativa ao gerenciamento de chaves em redes vDTN. São propostas soluções de segurança para redes veiculares sem hierarquia de nós para distinção das mensagens consideradas confiáveis por meio de algoritmo para tomada de decisões.

A segurança em redes veiculares é um desafio crucial e a confiança é um elemento chave nesse aspecto, devido ao grande número de nós independentes envolvidos e presença de fatores humanos na rede que aumentam a tendência de mau comportamento [Raya, 2007]. Neste trabalho é utilizado o conhecimento prévio existente entre os usuários das redes veiculares para estabelecer graus de confiança e possibilitar a comunicação segura para divulgação de informações para suas redes sociais.

1.1. Definições

A seguir são apresentadas definições de termos no contexto necessário para o entendimento das propostas deste trabalho:

- Chave é uma informação restrita que controla a operação de algoritmos de criptografia. As chaves são base das técnicas criptográficas e são utilizadas em conjunto com os algoritmos criptográficos na realização de operações de cifrar/decifrar. As chaves são também usadas em outros algoritmos criptográficos, tais como esquemas de assinatura digital ou autenticação.
- Chave pública é a chave divulgada pelo próprio veículo para que os outros veículos da rede sejam capazes de ler o conteúdo de suas mensagens criptografadas, por isso devem armazenar sua chave pública.
- Chave privada é a chave utilizada para encriptação de mensagens dos usuários, que é mantida sob sigilo.
- Gerenciamento de chaves é a administração de tarefas envolvendo a geração, armazenamento, distribuição, proteção e revogação de chaves criptográficas, de modo que elas estejam disponíveis aos usuários autênticos da rede. O gerenciamento de chaves é responsável por manter as relações criptográficas e o material criptográfico, por exemplo, os pares de chaves pública e privada, os parâmetros de inicialização e os parâmetros não secretos.

- Autoridades certificadoras são entidades que assinam certificados digitais, o que atesta a posse de uma chave pública pelo proprietário do certificado. Tais assinaturas permitem estabelecer relações de confiança em assinaturas ou em afirmações feitas pela chave privada que corresponde à chave pública certificada. Nesse modelo de relações de confiança, a autoridade certificadora (CA) é uma terceira parte confiável.
- Certificado é um documento eletrônico assinado digitalmente por uma autoridade certificadora confiável, que confirma a identidade de um usuário e contém uma cópia da sua chave pública. A certificação digital garante requisitos de segurança essenciais na rede como autenticidade e integridade.
- Certificado autoassinado é um certificado assinado pelo proprietário do mesmo, que realiza a função da autoridade certificadora e assina o próprio certificado.
- Certificado assinado por um terceiro, que não representa autoridade certificadora oficial, é um certificado válido se a chave pública da assinatura estiver disponível à outra parte.
- Material criptográfico é composto de certificados e chaves utilizados para validar e autenticar os motoristas envolvidos, cifrar e decifrar mensagens.
- Reputação é um princípio de reconhecimento e divulgação do comportamento do usuário. O conceito de reputação é uma medida coletiva de confiança em uma pessoa ou sistema, baseada em indicações ou avaliações de membros de uma comunidade [Paula, 2010].
- Grau de confiança é uma medida da confiança de um usuário em relação ao outro. A escolha de usuários confiáveis inclui quanto os demais usuários da rede confiam no emissor de uma mensagem.
- Redes sociais modelam em grafos a relação entre pessoas, comumente denominados como amigos ou conhecidos na rede, o que é usado para modelagem de redes sem fio [Verma, 2011].

1.2. Problema

O problema abordado neste trabalho é o modelo de confiança em redes veiculares tolerantes a interrupções para viabilizar a autenticação e troca de mensagens confiáveis entre usuários. A aceitação ou rejeição de mensagens das redes veiculares baseia-se no

nível de confiança do usuário remetente. O nível individual de confiança em uma pessoa ou dispositivo pode ser obtido a partir de uma combinação das indicações recebidas e das experiências pessoais [Wangham, 2014]. O ponto crítico nessas relações de confiança é o estabelecimento inicial da confiança entre duas pessoas que não se conhecem.

Os usuários das redes veiculares precisam estabelecer um grau de confiança para troca de mensagens, por meio da definição de critérios para tomada de decisões e uso de chaves para comunicação segura. Tais questões são abordadas neste trabalho com aspectos de confiança e reputação para prover autenticação das mensagens. Mecanismos de prevenção de acesso são utilizados para impedir a ação de adversários, bem como técnicas de criptografia para garantir a autenticidade das informações.

DTN exige a definição de novos protocolos de segurança e gerenciamento de chaves, pois protocolos tradicionais de segurança fim-a-fim não funcionam [Bhutta, 2014]. Em redes DTN é irreal assumir que haverá autoridades certificadoras com infraestrutura presente e disponível para utilização de criptografia de chave pública [Jia, 2012]. Este trabalho pretende tratar da distribuição e o gerenciamento de chaves para criptografia em redes veiculares DTN, bem como a utilização de certificados e chaves públicas para determinar a confiança dos usuários da rede.

O maior desafio em segurança para redes DTN é a ausência de um método de gerenciamento de chaves que apresente tolerância a interrupções. Os protocolos atuais necessitam de serviço de distribuição de chaves ou verificação *on-line*, impraticável nos ambientes de conectividade intermitente como em redes veiculares. Nenhum esquema de gerenciamento de chaves ainda é reconhecido como adequado para redes tolerantes a interrupções [Symington, 2011] [NASA, 2014].

Resumindo o problema desta tese, destacam-se as questões de pesquisa:

1. Como definir a confiança dos usuários em redes sem conectividade?
2. Como estabelecer graus de confiança e reputação para trocas de mensagens?
3. Como realizar a autenticação em redes veiculares tolerantes a interrupções?
4. Como gerenciar e compartilhar chaves criptográficas em redes vDTN?

1.3. Objetivos

Os objetivos deste trabalho consistem no estudo de aspectos relacionados à confiança em redes veiculares DTN, na identificação de requisitos de segurança, na concepção e

validação de um modelo de confiança. Não há demanda para que os usuários tomem decisões sobre as mensagens recebidas, o que deve ser baseado em critérios estabelecidos para confiança prévia entre usuários. Assim como em outras redes, características como confiança e disponibilidade são fundamentais.

O objetivo principal da tese é propor um modelo de confiança que utiliza certificados para prover segurança em redes veiculares tolerantes a interrupções. Por meio da formação de redes sociais, usuários que se conhecem e garantem sua identidade compartilham chaves por meio de contato direto, com um usuário assinando o certificado do outro. Assinar o certificado recíproco e compartilhar sua chave pública com outros usuários possibilita uma rede de relacionamento social. Dessa forma, todos que possuem amigos em comum validam seus certificados usando as chaves do amigo.

A proposta deste trabalho para abordar a confiança em redes veiculares é usar material criptográfico recebido em relacionamentos cotidianos, como encontro com amigos ou ajuda a outro veículo, para que se estabeleça um grau de confiança entre os usuários. Um certificado assinado por um terceiro, que não seja reconhecido como autoridade certificadora oficial, é considerado válido se sua chave pública estiver disponível à outra parte. Complementando esse material, propõe-se um mecanismo de reputação que possibilita também aos usuários beneficiados gerar uma assinatura para o certificado de quem o ajudou ou, caso haja divergência, com uma pontuação a ser reconhecida para identificá-lo como um usuário confiável.

O princípio básico para confiança com utilização da rede social é ampliar as possíveis assinaturas para um certificado, incluindo assinaturas de amigos e assinaturas de reputação, para que os usuários confiáveis possam ser reconhecidos. Além da certificação SNVC (*Social Networks for Vehicular Certification*), o modelo de confiança deste trabalho propõe também que o interesse dos outros usuários nas informações seja manifestado por meio de um mecanismo de reputação para divulgar se foram beneficiados.

O escopo deste trabalho delimita-se pelo estudo relativo à segurança para possibilitar a troca de informações confiáveis por meio de uma rede social entre veículos, para que tomem decisões mais precisas no trânsito. O modelo de confiança proposto permite a troca de informações entre amigos sobre suas experiências durante o deslocamento atual. Inicialmente, este trabalho considera a definição de rotas de trânsito como exemplo e motivação, mas há outras aplicações para a proposta apresentada como gerenciamento de ônibus, otimização de horários de deslocamentos e compartilhamento de veículos.

1.4. Contribuições

As contribuições deste trabalho são um modelo de confiança e a certificação por meio de redes sociais, que possibilitam a utilização de certificados e chaves públicas para estabelecer graus de confiança para redes tolerantes a interrupções (DTN), especificamente no cenário de redes veiculares.

Entre as contribuições deste trabalho de tese, sobressaem as seguintes:

1. criação de um modelo de confiança por meio de redes sociais veiculares;
2. definição de uma cadeia de certificação e compartilhamento de chaves;
3. proposição de um esquema de atribuição de confiança por meio de certificados;
4. definição de um mecanismo de reputação com utilização de certificados.

A utilização de confiança por meio de redes sociais e mecanismos de segurança relacionados, com controle prévio dos usuários pela definição de seus amigos, é uma proposta inovadora na abordagem de problemas relacionados à segurança em redes veiculares DTN. [Karagiannis, 2011] cita tais necessidades para redes veiculares definindo-as sobre o termo privacidade adaptativa. Dessa forma, a concepção e a implementação dessa proposta podem motivar outros trabalhos seguindo tal inovação.

A avaliação deste trabalho com realização de simulações com uso de *traces* reais apresenta novos dados a respeito da confiança em redes veiculares tolerantes a interrupções, sendo possível estender a certificação SNVC (*Social Networks for Vehicular Certification*) proposta para outras redes DTN. Além de comprovar que os usuários alcançam o grau de confiança necessário para troca de mensagens, representam avanço na pesquisa com utilização de conceitos de redes sociais em redes veiculares.

Este trabalho foi publicado (*SNVC: Social Networks for Vehicular Certification*) na revista *Computer Networks* para "*Special Issue on Cyber-Physical Systems for Mobile Opportunistic Networking*" 2016. As principais contribuições e parte dos resultados deste trabalho de tese foram publicados no 10º IEEE *WiMob* 2014, *"Social Networks for Certification in Vehicular Disruption Tolerant Networks"* [Oliveira, 2014]. Os resultados iniciais foram publicados no SBRC 2013, "Certificados Sociais para Segurança em Redes Veiculares Tolerantes a Interrupções" [Oliveira, 2013].

1.5. Estrutura do documento

O conteúdo deste documento é apresentado em oito capítulos. Este primeiro capítulo apresenta o problema abordado e os objetivos do trabalho. O capítulo seguinte apresenta os tipos de redes abordadas e os conceitos fundamentais necessários para o entendimento deste trabalho, descrevendo as características das redes veiculares.

As principais contribuições deste trabalho são apresentadas a partir do terceiro capítulo, que apresenta um estudo sobre os requisitos de segurança para redes veiculares e mecanismos de segurança existentes. O quarto capítulo descreve os trabalhos relacionados, comparados e separados em categorias. O quinto capítulo apresenta o modelo de confiança e a certificação propostos por meio da formação de rede social.

Os resultados e a avaliação realizada sobre o modelo de confiança proposto são mostrados a partir do sexto capítulo, com as métricas de funcionamento e utilização de *traces* reais de mobilidade para validação. No sétimo capítulo, é descrita a comparação do mecanismo com proposta anterior da literatura e a análise relacionada. Por fim, no oitavo capítulo, são mostradas as considerações finais e próximos trabalhos.

Capítulo 2

Conceitos Fundamentais

Neste capítulo são apresentados os principais conceitos abordados neste trabalho: redes veiculares, DTN, redes sociais, confiança e gerenciamento de chaves. Redes veiculares são redes compostas por computadores embarcados em veículos. Nem todos os veículos terão o equipamento necessário, então a rede é esparsa e a comunicação deve utilizar a arquitetura DTN (*Disruption Tolerant Networks*). Por haver problemas de disponibilidade, são necessários novos mecanismos criptográficos, sendo inviável o uso de mecanismos de segurança convencionais.

2.1. Redes Veiculares

Redes veiculares são redes de computadores sem fio com nós móveis e embarcados em veículos e/ou equipamentos fixos localizados às margens das ruas e estradas [Alves, 2009]. A existência de uma infraestrutura que permita a comunicação entre veículos e de veículos com algum ponto de acesso dá suporte a diversas aplicações que levam à economia de tempo, otimização de recursos, redução de consumo, previsão de problemas e apresentar diversas outras vantagens [Silva, 2014].

Segundo [Alves, 2009], as aplicações de redes veiculares são divididas em três classes: segurança no trânsito, entretenimento e assistência ao motorista. As aplicações de segurança possuem caráter preventivo e emergencial, onde o principal desafio é divulgar rapidamente as informações para que o condutor tenha tempo para reagir. Nessa classe de aplicações destacam-se a divulgação de informações sobre acidentes, sobre ocorrências no trânsito e sobre condições adversas de ruas e estradas. Em geral, em aplicações de segurança, a divulgação é limitada aos nós localizados próximos ao perigo. Por exemplo, em situações em que os veículos precisam realizar uma mudança de faixa, mensagens são

trocadas para evitar colisões laterais [Chen, 2005]. Além das comunicações entre veículos, as comunicações com a infraestrutura reduzem o número de colisões em cruzamentos [VSCC 2005] [Biswas, 2006].

A classe das aplicações de entretenimento inclui adaptações de aplicações da Internet para redes veiculares. Nessa classe se destacam os sistemas de compartilhamento de conteúdo como músicas e filmes. A ideia básica é que os veículos troquem pedaços de arquivos desejados entre si, como ocorre no protocolo BitTorrent usado na Internet. Entre exemplos de propostas de sistemas par-a-par para compartilhamento de conteúdo em redes veiculares encontram-se: SPAWN [Nandan, 2005], CodeTorrent e CarTorrent [Lee, 2007]. Para difusão de vídeo há o V3 [Guo, 2005], onde é proposto um sistema para difusão de vídeo ao vivo veículo-a-veículo (V2V). Diferentemente dos sistemas de compartilhamento de conteúdo, a requisição do vídeo não é enviada inicialmente para um gateway localizado às margens da via. Toda a comunicação se dá entre os próprios veículos.

Por fim, as aplicações de assistência ao motorista envolvem o recebimento de informações que auxiliem o condutor em buscas ou automatizem serviços. São exemplos aplicações de localização de vagas em estacionamentos [Caliskan, 2006] [Panayappan, 2007], divulgação de informações sobre informações das vias [Nadeem, 2004], [Wischhof, 2003], auxílio em cruzamentos [VSCC 2005], aplicações de localização de postos de abastecimento, controle de frotas e cobrança automatizada de pedágio.

As redes veiculares estão se popularizando a partir do uso de equipamentos de navegação baseados em GPS e expansão da cobertura de Internet móvel. Diversas outras formas de comunicação agregam valor a esses equipamentos, como a comunicação *ad hoc* veículo a veículo, bem como uma rede metropolitana, sensores ao longo da via e até etiquetas de identificação RFID.

Redes veiculares são formadas por veículos com dispositivos embarcados e heterogêneos em *hardware*, com a utilização de *notebooks, palmtops, tablets,* celulares e equipamentos da via em sua composição e várias tecnologias de rede para comunicação entre esses nós. A conectividade dessas redes no trânsito não é considerada constante, pois o ambiente é altamente suscetível à interrupção de comunicação. As redes veiculares, compostas por diversos nós, devem ser tolerantes a atrasos e interrupções. Em geral, são tratadas como VANETs (*Vehicle Ad Hoc NETworks*), mesmo quando existe a infraestrutura nas vias [Alves, 2009].

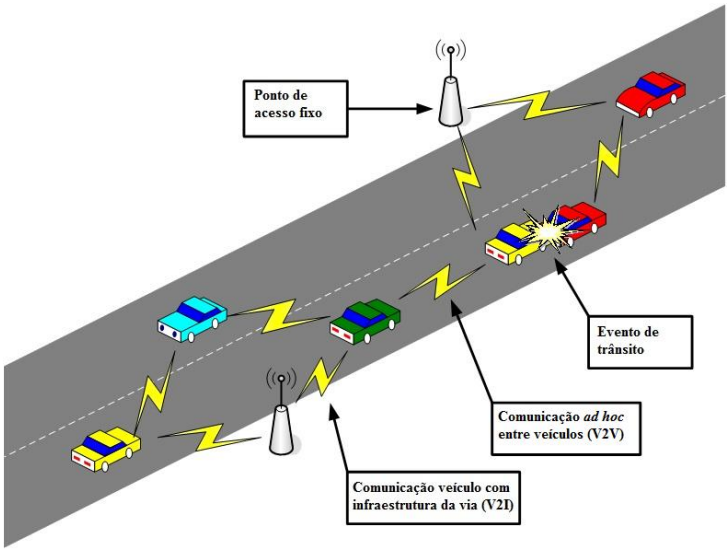

Figura 2.1. Exemplos do modelo de uma rede veicular [Raya, 2007].

A Figura 2.1 ilustra os componentes da infraestrutura da rede veicular e os três modos de comunicação: infraestruturado, *ad hoc* ou híbrido. No modo infraestruturado, os veículos comunicam com a infraestrutura às margens das vias de trânsito, comunicação referenciada como V2I (*Vehicle-to-Infrastructure*). No modo *ad hoc*, também chamado de V2V (*Vehicle-to-Vehicle*), os veículos comunicam-se entre si, mas não é prevista a comunicação com a infraestrutura. Finalmente, há o modo híbrido onde os veículos comunicam-se entre si e também com a infraestrutura, como ilustrado.

A comunicação veicular é definida pelos padrões IEEE 802.11p e WAVE (*Wireless Access in the Vehicular Environment*). O padrão IEEE 802.11p [IEEE 2010] foi definido por um grupo de trabalho do IEEE para facilitar a implantação de redes veiculares em ambientes de alta velocidade (comunicação V2V e V2I). O padrão de acesso sem fio em ambientes veiculares WAVE, um modo de operação do IEEE 802.11p, é composto por um conjunto de normas, dentre as quais se destaca a IEEE 1609.2 (serviços de segurança WAVE) [IEEE 2013]. A reserva de uma faixa de comunicação de curto alcance dedicada (DSRC - *Dedicate Short-range Communications*) [FCC 2006] é considerada uma das primeiras iniciativas de padronização das tecnologias, específicas para as comunicações veiculares de curto alcance [Wangham, 2014].

Os nós da rede representam veículos, nós sensores para o monitoramento, pontos de acesso fixos que provêem conexão externa aos veículos e servidores com pessoas qualificadas para controle do tráfego. Sensores e etiquetas RFID ainda são utilizados para monitoramento do trânsito e envio de informações. Os equipamentos podem se limitar à

comunicação *ad hoc* ou perder conectividade com a rede metropolitana em alguns trechos das vias.

Em casos de acidentes ou na otimização do trânsito, seja em centros urbanos ou em regiões isoladas, geralmente não existe uma infraestrutura de rede ou a cobertura da mesma não possui áreas complementares. As pessoas envolvidas nessas situações buscam o maior número possível de informações, tais como mapas, fotos e informações que melhoram o entendimento dos problemas ou de sua localização.

São destacadas como principais características/desafios das VANETs, segundo [Paula, 2010]: (i) a banda disponível nas redes sem fio é significativamente menor que nas redes cabeadas; (ii) a conectividade da rede é variável no tempo, pois depende de fatores como sua densidade em determinado ponto, velocidade dos veículos, sentido do deslocamento e raio de alcance dos dispositivos móveis instalados nesses veículos ou na via; (iii) a cooperação entre veículos tende a ser fator determinante para que as informações geradas se tornem de conhecimento geral; (iv) as redes veiculares têm potencial de escala na ordem de milhares de veículos distribuídos por todos os lugares, as VANETs possivelmente serão a maior rede *ad hoc* móvel existente no futuro; (v) os nós de uma VANET se movimentam dentro de vias de tráfego existentes e sob a regência de leis de circulação; (vi) a topologia da rede é dinâmica graças à alta mobilidade aliada a grandes velocidades; (vii) não há restrições severas de recursos energéticos e computacionais como acontece com redes de sensores; (viii) assim como outras redes sem fio, o acesso ao meio é compartilhado e os nós podem ser violados, por isso são muito mais suscetíveis a ataques que as redes cabeadas convencionais.

2.2. Redes Tolerantes a Interrupções (DTN)

Neste trabalho são tratadas redes veiculares DTN (vDTN) [Benamar, 2014]. Uma DTN [Fall, 2003] é uma tecnologia de rede adequada para suportar atrasos longos, como em redes de satélites, e interrupções de comunicação, como em redes de sensores sem fio [Mota, 2009]. Em uma DTN, a comunicação é assíncrona e não há necessidade de um caminho fim-a-fim, sendo adequada para uso em redes com conectividade intermitente ou sujeitas a atrasos longos [Fall, 2004]. Em [Pereira, 2012] foram pesquisadas as abordagens em redes DTN veiculares, com abordagem de aspectos da tolerância a interrupções e discussão de desafios de pesquisa.

As redes DTN têm o objetivo de prover conexões entre dispositivos em áreas que não possuem ou não terão disponível a atual tecnologia de rede. Os protocolos de roteamento convencionais necessitam da existência de um caminho fim-a-fim entre a origem e o destino, o que é inviável em redes de conectividade intermitente. Além disto, o desempenho degrada consideravelmente com o aumento do número de saltos em uma comunicação sem fio [Ott, 2006].

Redes com características como baixa densidade de nós, altas taxas de erros de comunicação, alta latência, limitações de banda e longevidade de nós criam cenários desafiadores [Fall, 2003]. Essas características das redes fazem com que as aplicações nesses cenários tenham um comportamento diferente do que teriam em uma rede tradicional. O conceito de DTN originalmente tem objetivo de dar suporte a comunicações intermitentes e com atrasos longos em redes que interligam pontos a longas distâncias, como no caso das redes interplanetárias.

Cerf et al. [2001] propuseram uma arquitetura capaz de suportar interrupções de comunicação utilizando armazenamento temporário de mensagens e reencaminhamento quando do retorno de conectividade. Apesar de o termo DTN ser o mais utilizado na literatura, também são encontradas outras terminologias, tais como: redes com conectividade eventual, redes móveis parcialmente conectadas, redes desconectadas, redes com conectividade transiente, redes incomuns, redes extremas ou *Challenged Networks* [Chen, 2006].

O RFC 4838 [Cerf, 2007] define a arquitetura de uma rede DTN como uma composição da pilha de camadas definida para a Internet, acrescida de uma nova camada de agregação, denominada *bundle*, sobreposta à camada de transporte. Essa camada comum permite que redes DTN sejam compostas de várias sub-redes heterogêneas, possibilitando protocolos de comunicação das camadas inferiores inteiramente distintos.

A Figura 2.2 apresenta as pilhas de protocolos da Internet e de uma rede DTN. Os protocolos de comunicação da rede são específicos para cada sub-rede, que variam de acordo com o ambiente tecnológico em que estão operando, mas todas as sub-redes precisam possuir a camada *bundle*, que irá fazer a interface entre a aplicação e as diversas tecnologias de comunicação entre as sub-redes.

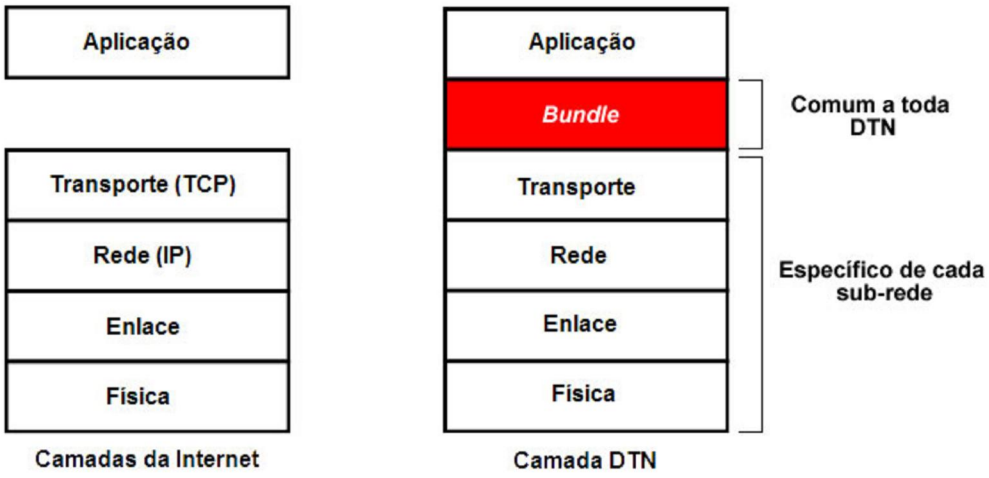

Figura 2.2. Pilha de protocolos da Internet e de uma DTN [Mota, 2009].

A arquitetura DTN propõe utilizar esse tipo de rede para encaminhar mensagens completas a cada salto. O roteamento da rede é feito da forma armazenar-carregar-repassar, paradigma *store-and-forward* [Fall, 2004], que mantém mensagens temporariamente em *buffer* caso não haja conexão direta com o próximo passo ou com o destino. Esse procedimento define que cada nó intermediário no caminho armazena a mensagem até que seja possível o estabelecimento de um contato com outro nó e o encaminhamento dessa mensagem armazenada, o que pode levar um longo tempo.

Somente alguns dos nós estão conectados, enquanto os demais não tem conectividade. As possibilidades de comunicação alteram-se a qualquer momento, devido a falhas, deslocamentos ou outros tipos de eventos. Quando há conectividade entre nós, um nó tem oportunidade de enviar dados pela rede em direção a seus destinos finais. Tal oportunidade é chamada "contato" [Fall, 2003]. Um par de nós possui, ao mesmo tempo, vários contatos disponíveis, estabelecidos por meio de enlaces físicos diferentes (*Wi-Fi*, *Bluetooh*, etc). A qualidade de cada um desses contatos oscila devido a obstáculos e variações na distância entre os nós.

Os protocolos convencionais da Internet não funcionam em redes *ad hoc* móveis quando a mobilidade dos nós é muito alta e a topologia da rede muda constantemente, provocando frequentes desconexões [Fall, 2005]. As características desses e de outros novos ambientes de rede conduzem a uma série de desafios: frequentes desconexões, atrasos longos e/ou variáveis (da ordem de horas ou dias), conectividade intermitente, recursos limitados dos dispositivos de comunicação, alta taxa de erros etc.

Segundo [Oliveira, 2007], as principais características encontradas nas DTN são:

- atrasos longos e/ou variáveis: uma DTN chega a ter atrasos da ordem de horas e, até mesmo, dias. O atraso fim-a-fim é determinado por meio da soma dos tempos de atraso salto-a-salto. Basicamente, é formado por quatro componentes: tempo de espera, atraso nas filas, atraso de transmissão e atraso de propagação [Jones, 2005];
- frequentes desconexões: desconexões ocorrem pela mobilidade que provoca constantes mudanças na topologia da rede, por péssimas condições de comunicação (desvanecimentos), por economia de recursos como em sensores sem fio onde nós sensores dormem para poupar energia, por negação de serviço como o ato do inimigo sujar a frequência (*jamming*) em operações militares. Esses eventos resultam em uma conectividade intermitente da rede, ou seja, na inexistência de um caminho fim-a-fim entre um nó fonte e um nó de destino.

2.3. VANETs ou vDTN?

Neste trabalho as redes veiculares são abordadas com tolerância a interrupções (vDTN) [Pereira, 2012]. Nos últimos anos, houve uma extensa atividade de investigação na área emergente de redes móveis *ad hoc* conectadas intermitentemente [Jamalipour, 2011]. Ao considerar a natureza da conectividade intermitente na maioria dos ambientes móveis do mundo real sem quaisquer restrições impostas sobre o comportamento dos usuários, essas redes são eventualmente formadas sem qualquer suposição no que diz respeito à existência de um caminho fim-a-fim entre dois nós que desejam se comunicar.

Redes de conectividade intermitente são diferentes das redes móveis *ad hoc* convencionais (VANETs, por exemplo), que foram vistas implicitamente como um grafo conexo com caminhos completos estabelecidos entre cada par de nós [Jamalipour, 2011]. Para VANETs convencionais, a mobilidade dos nós é considerada como um desafio e precisa ser tratada adequadamente para permitir a comunicação contínua entre nós. No entanto, para superar a conectividade intermitente no contexto vDTN, a mobilidade é reconhecida como um componente crítico para a comunicação de dados entre os nós que podem nunca ser parte da mesma porção conectada da rede. Isso agrega o custo da adição de um atraso considerável na transmissão de dados, pois os dados são frequentemente armazenados e transportados pelos nós intermediários que esperam a mobilidade para gerar

a próxima oportunidade de encaminhamento que provavelmente pode trazê-lo para perto do destino [Jamalipour, 2011].

As redes DTN surgiram na última década como uma das evoluções mais interessantes de redes *ad hoc* clássicas, em que os nós não exigem uma alta conectividade, a fim de se comunicar uns com os outros [Reina, 2015]. Por essa característica, DTNs são também referenciadas como redes oportunistas, onde cada encontro entre dois nós na rede é visto como uma nova oportunidade para fornecer informações. Em contraste com redes *ad hoc*, a mobilidade é vista como uma vantagem para divulgação de informação em DTN, pois quanto maior a mobilidade, maior o número de possíveis encontros com outros nós.

Redes DTN podem ser amplamente utilizadas no ambiente de frequência dividida e interrompida de rede sem fio, que pode terminar a transmissão de dados e alternar entre um modo de "*storage carry forward*". A rede DTN é muito semelhante com a rede *ad hoc* no ambiente de aplicativos e *design* de *software*, mas no custo de aplicação de algoritmos de roteamento, QoS, etc. ambas têm vantagens e desvantagens [Yu, 2011].

Em cenários onde a alta densidade de nós pode não ser garantida ou quando eles se movem com alta mobilidade, redes vDTN são adequadas. Essas condições podem causar um mau funcionamento dos mecanismos normais de roteamento *ad hoc* (descoberta de rotas mais estabelecimento de rota) [Reina, 2015]. Na comunicação DTN, a informação é enviada em unidades chamadas *bundles*. Quando um nó gera informação, ela é dividida em diferentes pacotes e, em seguida, o nó espera até encontrar outro nó, a fim de entregar a informação (protocolos *bundle*). Assim, enquanto protocolos de roteamento *ad hoc* trabalham na camada de rede, os protocolos *bundle* para DTN trabalham sobre uma camada superior denominada camada *bundle*, que está entre a camada de transporte e a camada de aplicação.

Redes vDTN contrastam com redes *ad hoc* em cenários veiculares, pois em VANETs quando um nó não pode transmitir uma mensagem para o destino, ele coloca a mensagem em um *buffer* de envio, e, após determinado tempo de espera, o nó irá descartar a mensagem armazenada [Reina, 2015]. Além disso, DTN também são adequadas em redes de alta mobilidade, onde redes *ad hoc* tradicionais falham devido às contínuas quebras de rotas entre os pares de nós origem-destino. Por fim, os autores afirmam que muitos dos esquemas propostos para DTN dependem de intervenção manual do usuário, o que pode ser ineficiente, e sistemas independentes mais automatizados devem ser pesquisados.

O paradigma MANET (*Mobile Ad hoc NETworks*) não coincide com as redes móveis *ad hoc multihop* e na última década claramente divergiram [Conti, 2014]. Os autores listam

razões pelas quais o paradigma MANET não teve um grande impacto sobre a comunicação de computadores e discutem a evolução das redes *ad hoc multihop*, com base nas lições aprendidas com a pesquisa MANET. Especificamente, analisam os paradigmas de redes de sucesso como redes oportunísticas e veiculares, que emergiram do mundo de MANET como uma aplicação mais pragmática das redes *ad hoc multihop*. Nesses tipos de redes, protocolos de roteamento *ad hoc* tradicionais não conseguem transferir mensagens da origem para o destino, devido à indisponibilidade de conectividade fim-a-fim e de rede totalmente conectada [Saha, 2011].

A grande maioria das pesquisas de rede móvel *ad hoc* realiza uma grande suposição: que a comunicação só pode existir entre os nós que são simultaneamente acessíveis dentro da mesma nuvem conectada (isto é, que a comunicação é síncrona). Na realidade, é provável que essa hipótese seja pobre, especialmente para ambientes escassamente ou irregularmente povoados [IPCAS, 2016]. Redes móveis *ad hoc* dependem de protocolos de roteamento que tentam primeiro estabelecer uma rota completa e, em seguida, depois da rota ser estabelecida, transmitir os dados atuais.

Os algoritmos de roteamento para redes DTN diferem dos algoritmos para redes *ad hoc* tradicionais devido às incertezas sobre a duração das conexões entre os nós. Esses algoritmos são classificados quanto à quantidade de informação que os nós possuem principalmente a respeito da mobilidade dos nós. Os algoritmos estocásticos assumem que não possuem nenhum conhecimento sobre o estado da rede como em redes veiculares, já os algoritmos determinísticos assumem possuir algum conhecimento a respeito da topologia da rede ou tempo médio entre os contatos.

A Tabela 2.1 resume as diferenças entre redes DTN e MANET. DTN é uma área reconhecida na pesquisa de redes agora, em parte devido a experiências práticas com redes móveis *ad hoc* (MANET). Assim como conceitos DTN estão também relacionados com MANETs, este trabalho aborda redes veiculares vDTN com utilização de conceitos já definidos para VANETs. Neste trabalho são consideradas apenas questões específicas de DTN e as soluções propostas são específicas para DTN. Não há descrição detalhada de MANET, mas de DTN.

As diferenças citadas nesta seção mostram a necessidade de mecanismos específicos para vDTN como o problema deste trabalho, visto que os protocolos de roteamento de redes *ad hoc* não funcionam com uso da camada *bundle.* Como consequência dessas diferenças, os desafios de segurança específicos de redes DTN serão discutidos na Seção 3.3.

Tabela 2.1. Comparativo de redes DTN e MANET.

DTN	MANET
comutação de mensagens	comutação de pacotes
roteamento salto-a-salto	roteamento origem-destino
alta mobilidade	baixa mobilidade
comunicação assíncrona	comunicação síncrona
atraso fim-a-fim incerto e alto	atraso fim-a-fim confiável e baixo
protocolo *Bundle*	TCP/IP tradicional

2.4. Gerenciamento de chaves

O gerenciamento de chaves é a administração segura das chaves, que são base das técnicas criptográficas e são utilizadas em conjunto com os algoritmos criptográficos na realização de operações de cifrar/decifrar. A técnica consiste na geração, armazenamento, distribuição, proteção e revogação das chaves, de modo que elas estejam disponíveis aos nós autênticos da rede. A falta de um método tolerante a atraso para o gerenciamento de chaves [Pereira, 2012] limita a utilização de DTN.

O gerenciamento de chaves é responsável por manter as relações criptográficas e o material criptográfico, que são os pares de chaves pública e privada, os parâmetros de inicialização e os parâmetros não secretos. O estabelecimento de chaves entre os vizinhos permite a autenticação no enlace. Na comunicação entre os nós, a autenticação é verificada salto a salto, em toda a rota percorrida pelos pacotes. A autenticação salto-a-salto permite eliminar os pacotes não autenticados e resulta em um controle de acesso, onde apenas os nós da rede enviam mensagens, o que evita presença de nós intrusos.

As características das redes veiculares exigem novas abordagens para que seja possível atender os requisitos de segurança necessários a algumas aplicações. Atualmente, nenhum esquema de gerenciamento de chaves ainda é reconhecido como adequado para redes DTN, devido às características específicas dessas redes [Lv, 2014] [Symington, 2011]. Os protocolos atuais necessitam de serviço de distribuição de chaves ou checagem *on-line*, impraticável nos ambientes de conectividade intermitente.

É necessário um esquema de distribuição de chaves seguro e eficiente que permita a autenticação em diferentes tipos de comunicação. Esquemas de gerenciamento de chaves são: centralizados ou distribuídos, gerenciados ou auto-organizados. O controle de acesso à rede impede e elimina diversos tipos de ataques, a menos que o inimigo comprometa nós

legítimos da rede. Uma forma de efetuar o controle de acesso à rede é implementando autenticação salto-a-salto das mensagens enviadas. Para implementar autenticação salto-a-salto, um nó precisa autenticar os nós vizinhos, não importando o tipo de comunicação, salto-a-salto ou em modo difusão.

Os processos de criptografia têm como objetivo comum impedir que uma determinada entidade denominada intruso obtenha informações sigilosas. A captura e adulteração de um nó permitem ao inimigo utilizar as chaves armazenadas nesse nó. É necessário prever quais chaves são descobertas a partir dessa adulteração. Há ameaças como o comprometimento da confidencialidade e da autenticidade das chaves públicas e privadas e o uso não autorizado dessas chaves.

Os sistemas de chaves simétricas consistem, basicamente, na substituição de uma determinada informação por outra calculada e cifrada. A inversão dessa informação cifrada para uma forma compreensível necessita a aplicação de chaves que são idênticas, secretas e de conhecimento apenas para os seus donos (remetente e destinatário). Assim, a passagem dessa chave entre eles é feita por meio de um canal seguro.

Para se comunicar em sistemas de chave pública, primeiramente, uma determinada entidade A utiliza a chave pública de outra entidade B para cifrar sua mensagem usando um algoritmo de criptografia também conhecido ou padronizado. Logo a entidade B decifra essa mensagem enviada pela entidade A usando a sua chave secreta e com o algoritmo de inversão conhecido ou padronizado. Assim, nessa comunicação não houve a necessidade de troca de nenhuma chave, logo não há a necessidade de um canal seguro. Um exemplo de criptografia por chave pública é a RSA (*Rivest Shamir Adleman*, nome dos inventores), que utiliza aritmética modular para cifrar e decifrar a mensagem transmitida [Kurose, 2003].

A maior parte dos métodos de segurança em redes procura autenticar a identidade e integridade das mensagens, mas não tentam autenticar os roteadores que encaminham as informações. Em redes DTN, nós encaminhadores (roteadores e *gateways*) também são autenticados [Warthman, 2008] e a informação enviada também é autenticada por eles, logo os recursos da rede são conservados ao prevenir o transporte de tráfego proibido na primeira oportunidade.

Os dados são criptografados o mais perto da sua origem possível, o que evita transitar dados não cifrados por toda a rede com o risco de serem copiados indevidamente. No entanto, implica também uma gerência de chaves mais sofisticada. Em particular, para lidar com esse gerenciamento, o uso de criptografia com chaves públicas é imprescindível.

As informações são criptografadas para serem transmitidas por um meio não seguro ou então para serem armazenadas em um sistema cujo acesso tem segurança duvidosa.

2.5. Certificação digital

Um certificado é um documento eletrônico, assinado digitalmente por uma autoridade certificadora (CA) confiável, confirmando a identidade do usuário e contendo uma cópia confirmada da chave pública do usuário. Na criptografia de chave pública, cada usuário tem um par de chaves privada e pública. Em uma PKI (*Public Key Infrastructure*), cada veículo da rede recebe um par de chaves emitidas pela agência governamental responsável pelo controle de trânsito ou mesmo pela fábrica desse veículo.

O uso de uma infraestrutura de chave pública é indicado por [Paula, 2010] como a melhor opção para redes veiculares, pois o estabelecimento de conexão inicial prejudica o processo de troca de mensagens em VANETs. As mensagens geradas são enviadas o mais rápido possível, uma vez que em muito dos casos o tempo é um requisito crítico no procedimento de tomada de decisões. Os principais requisitos de segurança que serão apresentados na Seção 3.1 (confidencialidade, autenticidade e integridade) são atendidos por técnicas de criptografia.

Enquanto a chave pública é divulgada pelo próprio veículo, sua chave privada é 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 serão capazes de ler o conteúdo dessa mensagem. De forma análoga, quando algum usuário deseja enviar uma mensagem confidencial a determinado veículo, faz uso da chave pública desse veículo para encriptar os dados. Logo, somente o veículo destinatário da mensagem consegue decriptar e obter tais dados, utilizando sua chave privada.

A chave pública não é necessariamente distribuída de forma autenticada pela rede, o que permite um inimigo trocá-la durante sua divulgação, o que torna necessário garantir sua autenticidade [Paula, 2010]. Essa garantia ocorre por meio do uso de certificados, que atestam a autenticidade e integridade daquela chave.

No entanto, a certificação apenas identificaria que o veículo não foi adulterado e tem uma identidade única, sem diferenciá-lo de outros veículos que atrapalham o funcionamento da rede veicular, mesmo possuindo certificados. Este trabalho propõe formas de diferenciar os usuários por meio de certificados e considera que o investimento

necessário por parte do governo ou empresas automotivas inviabilizaria a utilização de redes veiculares, sendo aspecto diferencial o interesse que os usuários tem pelas informações dos demais para que eles próprios busquem a certificação.

Duas soluções são previstas como CA responsáveis pela certificação em veículos em [Raya, 2007]: autoridades governamentais de transporte ou fabricantes de veículos. Seria necessário incluir cadeias de certificados comuns para que certificados emitidos por governos ou fábricas diferentes fossem reconhecidos pelos outros. Segundo o autor, as vantagens de utilizar PKI em VANETs são acompanhadas de desafios como a revogação de certificados, necessária para adversários da rede após detecção do seu comportamento.

O Algoritmo de Curvas Elípticas (*Elliptic Curve Digital Signature Algorithm* - ECDSA) [Johnson, 2001] foi avaliado por [Raya, 2007] e [Calandriello, 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. Em [Raya, 2007] são propostas chaves de 224 bits (28 bytes) e assinaturas de 56 bytes, o *overhead* aproximado seria 140 bytes – uma assinatura digital, uma chave e um certificado. Dessa maneira, o ECDSA é utilizado na certificação proposta neste trabalho.

Afirma-se em [Kargl, 2008], sem ignorar outros fatores, que o *overhead* computacional de segurança é devido à geração e verificação de certificados e assinaturas, que são anexados aos pacotes e assim causam *overhead* na comunicação. Este autor afirma ainda ser possível a comunicação segura de forma prática e efetiva como VANETs abertas. Em geral, algoritmos de chave simétrica geram uma sobrecarga computacional (*overhead*) menor por mensagem, desconsiderando o processo de estabelecimento de conexão necessário para a definição da chave compartilhada, que os algoritmos de chave pública.

Segundo [Papadimitratos, 2009], todos os esforços para prover segurança em VANETs utilizam autoridades certificadoras (CA) e criptografia de chave pública para proteger a comunicação, pois esta é vulnerável a ataques e a privacidade dos usuários é o limite. Em redes DTN, ambos usuários e nós encaminhadores possuem pares de chaves e certificados, e os certificados dos usuários também indicam a classe de serviço [Durst, 2002]. Nós enviam seus pacotes e assinatura com sua chave privada, o que produz uma assinatura digital para o agregado específico. A assinatura permite aos recebedores confirmar a autenticidade do nó origem, a integridade da mensagem e os direitos relativos à classe de serviço, por meio do uso da chave pública do nó que enviou.

Segundo Fall [2003], a utilização dos pares de chaves e certificados ocorre da seguinte forma:

- Nó origem envia seu pacote, juntamente com assinatura específica, para que um nó adjacente a encaminhe. Se esse nó ainda não possui uma cópia do certificado do nó origem, ele obtém uma do próprio nó ou de uma CA.
- O primeiro nó que recebe o pacote para encaminhá-lo verifica a identidade da origem e sua classe de serviço, utilizando as cópias armazenadas de certificados dos nós adjacentes e chaves públicas da autoridade certificadora. Então substitui a assinatura do nó origem pela sua própria assinatura e encaminha a informação.
- Cada nó subsequente no encaminhamento verifica somente a identidade do nó anterior, usando suas cópias armazenadas de certificados de roteadores adjacentes e chaves públicas de uma CA. Então realiza o mesmo processo de substituição da assinatura pela sua própria e encaminha o pacote. Isso ocorre até que a informação alcance o destino.

2.6. Confiança e reputação

A confiança é um aspecto importante da tomada de decisões para aplicações e, em particular influencia a especificação da política de segurança, isto é, quem está autorizado a executar ações, bem como as técnicas necessárias para gerenciar e implementar a segurança para os aplicativos [Grandison, 2000]. O gerenciamento de confiança objetiva coletar informações necessárias para estabelecer relações de confiança, avaliar os critérios relacionados, monitorar e reavaliar as relações na evolução existentes [Grandison, 2000]. O estabelecimento inicial da confiança entre duas entidades que não se conhecem é o ponto crítico nessas relações de confiança.

O desenvolvimento de soluções para incentivar comportamentos cooperativos e punir os comportamentos maliciosos baseia-se em mecanismos de reputação e modelos de confiança para permitir aos nós decidirem em quem confiar. Esses mecanismos assumem que o comportamento antigo de um nó da rede indica de forma bem confiável suas ações futuras [Paula, 2010].

A confiança é definida como a firme convicção de que uma entidade agirá de forma confiável e segura, dentro de um contexto especificado [Grandison, 2000]. Em termos computacionais, a confiança é definida como a crença que um usuário tem na boa vontade do outro em prover a qualidade de serviço esperada, em um dado contexto e um determinado período [Chang, 2006].

Estabelecer a confiança entre os nós por meio de um sistema de reputação é uma forma de evitar ataques de nós maliciosos, que visa calcular a confiança dos nós de uma rede para permitir a identificação e o isolamento dos nós maliciosos [Fernandes, 2006]. Baseando-se nessa confiança, os nós podem decidir em quem confiar antes de tomar uma ação em relação à informação recebida.

O estabelecimento de confiança é necessário para permitir aos nós trocar informações entre si de forma segura, mesmo não tendo uma autoridade centralizadora. Essa descentralização é característica de redes veiculares e P2P (*Peer-to-Peer*). A partir da confiança estabelecida, é possível determinar quais recursos serão disponibilizados ou revelados para outros nós. Uma comunicação bem sucedida entre homem e máquina é importante para o motorista ganhar a confiança no sistema [Mitropoulos, 2010].

O gerenciamento de confiança visa a criação de grupos que confiam entre si e cooperam no intuito de combater nós egoístas e maliciosos, assim agregam opiniões sobre o comportamento passado dos nós com o objetivo de estimar o seu comportamento futuro. Um grau (valor) é atribuído aos nós para indicar o nível de confiança que o mesmo possui. As opiniões de reputação são atualizadas pelos usuários à medida que interagem, o que aumenta a reputação dos nós bem comportados e diminui a dos nós maliciosos [Liu, 2007].

Os termos reputação e confiança estão fortemente ligados [Jiangyi, 2009]: reputação representa o quão bem um nó se comporta, e serve para decidir se o nó é cooperativo ou possui mau comportamento. Por outro lado, a confiança representa o quão honesto um nó é e serve para decidir se o nó é confiável ou não. A reputação direta é obtida através da observação direta, na qual um nó monitora o comportamento dos outros nós geralmente em um salto (vizinho). Em contrapartida, a reputação indireta obtém as informações sobre a reputação de um nó é por outros nós da rede.

As recomendações de outros nós armazenadas em forma de histórico visam acelerar o processo de descoberta de nós maliciosos. O compartilhamento de experiências permite o estabelecimento de relações de confiança antes mesmo do início de transações [Wangham, 2014]. As relações de confiança entre os nós podem ser definidas: **de um para um,** confiar em um nó para executar uma ação específica; **de um para vários,** confiar em um conjunto de nós que troca conteúdos com segurança; **de vários para um**, todos confiam em um único nó, um líder, por exemplo; **e de vários para vários,** um grupo confia em outro grupo [Grandison, 2000].

Um estudo sobre gerenciamento de confiança para VANETs identifica os desafios nesse ambiente [Zhang, 2011]. A falta de eficácia dos modelos de confiança existentes

para VANETs é mostrada, além de chamar a atenção para a robustez dos modelos de confiança. Detectar a ação de nós maliciosos tornou-se um dos problemas mais difíceis no que diz respeito à segurança em redes veiculares [Li, 2012].

Minimizar os ataques e as consequências de comportamentos maliciosos é muito importante em soluções que necessitam da cooperação e da honestidade dos nós, tais como as aplicações de Alerta de Perigo Local [Fernandes, 2015]. Tais aplicações podem ser muito úteis para prover segurança do trânsito nas rodovias, porém, a confiança nos nós que propagam e difundem os alertas precisa ser avaliada. Alertar motoristas sobre um perigo que não está em sua visão não é uma tarefa fácil, pois caso este alerta seja disseminado muito cedo, pode ser que o motorista esqueça ou ignore-o. Apenas repetir os alertas sobre o mesmo perigo diversas vezes, além de irritar o motorista, pode perder a sua importância para o condutor resultando em uma inadequada reação para ele.

Para otimizar a formação e a propagação da confiança em aplicações colaborativas em redes móveis *ad hoc,* [Gray, 2003] baseia-se em noções humanas sobre confiança, risco e conhecimento. Afirma-se que as pessoas usam esses conceitos para decidir até que ponto devem cooperar com os outros. Uma rede de confiança visa o estabelecimento de novas relações de confiança entre partes que nunca interagiram previamente. Este trabalho utiliza o conceito de "mundo pequeno" *(Small World)* para a formação e propagação de confiança entre usuários da rede, a reputação ainda visa lidar com nós maliciosos.

Utiliza-se reputação e confiança na concepção de mecanismos para obter uma avaliação preliminar de ações que podem ser executadas de forma mais segura e confiável, evitando assim ataques de nós maliciosos, mesmo que existam veículos que nunca interagiram previamente devido ao dinamismo das redes veiculares. Em geral, sistemas de confiança estão ligados a sistemas de reputação, assim como este trabalho, pois a decisão de um veículo confiar nos alertas de outro veículo será tomada como base nas experiências passadas (reputação) dos veículos que compõem sua rede social.

2.7. Redes sociais

Redes sociais modelam em grafos a relação entre pessoas, comumente denominados como amigos ou conhecidos na rede, o que é usado para modelagem de redes sem fio [Verma, 2011]. Em geral, redes sociais são aplicações do conceito *"Small World"*. Característico de redes complexas, esse modelo mostra que uma pessoa conhece qualquer outra pessoa do

mundo direta ou indiretamente com poucos intermediários. As redes sociais são usualmente utilizadas para descrever qualquer grupo de pessoas que interagem por meio de mídias de comunicação on-line, existindo assim desde o início da Internet.

Em [Benevenuto, 2009] define-se uma rede social que permite a indivíduos: construir um perfil público ou semi-público em um sistema limitado; articular uma lista de outros usuários com quem possuirá uma conexão; visualizar e transmitir pela rede sua lista de conexões para outros que utilizam o sistema. Neste trabalho, o perfil é representado por certificados, que permitirão a identificação dos usuários da rede social. Há vários sistemas baseados em redes sociais disponíveis na Internet. Como exemplos, há redes sociais *on-line* de: profissionais (*LinkedIn*), amigos (*MySpace, Facebook, Orkut, Google+*), mensagens curtas (*Twitter*), diários e blogs (*LiveJournal*), fotos (*Flickr*) e vídeos (*Youtube, Metacafe,* entre outros).

Os usuários de uma rede social são chamados de amigos quando passam a fazer parte da rede social de outro usuário, ou seja, tornam-se amigos em suas redes sociais. Um amigo representa nesse contexto uma pessoa previamente conhecida, que compartilha informações com esse usuário. A interseção das redes sociais de cada usuário mostra os amigos que estão presentes nos grafos de amizade de dois ou mais usuários, denominados como amigos em comum desses usuários. A tendência de existir amigos em comum [Gakenheimer, 1999] motiva o interesse dos usuários pelos amigos dos amigos, ou seja, nós da rede que participam da rede social de algum amigo desse usuário.

O conceito de *Small World* [Gakenheimer, 1999] tornou-se conhecido após um experimento com cartas que foram encaminhadas por voluntários a pessoas conhecidas. As cartas tinham um destinatário específico em uma cidade americana e a pessoa com posse da carta deveria encaminhá-la para alguém que imaginasse estar mais próximo de entregar ao destino final. Ao encaminhar a carta, foi incluído o nome da pessoa ao fim da carta para possibilitar rastrear o caminho percorrido. Entre as cartas que chegaram ao destino, seis saltos foi o número médio necessário, resultado conhecido como princípio dos seis graus de separação, ampliado atualmente para alcançar qualquer pessoa do mundo.

Em relação às propriedades das redes sociais, um grafo é considerado *Small World* se tiver duas propriedades básicas: um coeficiente forte de agrupamento e um pequeno diâmetro [Benevenuto, 2009]. O coeficiente de agrupamento de um grafo é a medida que indica o quão perto um vértice e seus vizinhos estão de um clique, e o coeficiente de agrupamento de uma rede é a média do coeficiente de todos os vértices.

Um grafo regular, que tem o diâmetro proporcional ao tamanho da rede, com adição de apenas um pequeno número de conexões de longo alcance [Guidoni, 2012] é transformado em um modelo *Small World*, que tem um pequeno número médio de ligações entre dois vértices quaisquer e um valor alto para o coeficiente de agrupamento. Em um grafo regular, cada vértice tem o mesmo número de vizinhos e o grafo tem um alto coeficiente de agrupamento, com alto caminho médio. Em um grafo aleatório, a probabilidade de conectar qualquer par de vértices no grafo é a mesma, o grafo tem baixo coeficiente de agrupamento e baixo caminho médio. O modelo conhecido como *"Small World"* é apresentando como intermediário entre um grafo regular e um grafo aleatório.

As características do modelo *Small World* são utilizadas em [Guidoni, 2012] para criar uma rede de sensores sem fio para melhorar a comunicação de dados, já que o grafo dessa rede tende a apresentar maior agrupamento que redes aleatórias e características de alto caminho médio. Redes sem fio são grafos em que as ligações entre os nós dependem do raio de comunicação, sendo alterado em função da distância entre aqueles nós [Almiron, 2010].

Relações sociais tiveram sua investigação ampliada em redes sociais de relacionamentos entre pessoas com interesses comuns [Yu, 2008] [Chaintreau, 2007]. Tais relações sociais são base para caracterizar as propriedades da confiança social e evitar usuários falsos (ataques *sybil)*. Redes sociais com foco na construção de relações baseadas na confiança social entre entidades são estendidas para ciência da computação pela definição de confiança como um descritor bem definido de segurança e criptografia, como uma métrica para refletir metas de segurança [Golbeck, 2006].

O crescimento das "Redes Sociais Online" segundo [Maaroufi, 2014] está incitando o desenvolvimento de um novo tipo de redes *ad hoc* que são "Redes Veiculares Sociais" (*Vehicular Social Networks* - VSNs). A inclusão de redes sociais dentro de veículos tem atraído pesquisadores para elaborar protocolos de roteamento e arquiteturas para a construção de comunidades sociais para veículos, para facilitar a interação humana entre os usuários [Chaintreau, 2006].

2.8. Conclusão

Foram apresentados neste capítulo os conceitos relativos às redes veiculares e redes tolerantes a interrupções (DTN). A mobilidade e falta de garantia da existência de

conectividade representam uma interseção nesses dois tipos de rede. Logo, propõe-se abordar neste trabalho as redes veiculares utilizando a arquitetura DTN para comunicação entre os veículos.

Também foram abordados nesta seção os conceitos relacionados ao gerenciamento de chaves, confiança e reputação, certificação e redes sociais, que estão diretamente ligados à proposta deste trabalho. A partir de uma revisão da literatura, foi possível identificar a necessidade de mecanismos para prover autenticação e confiança em redes veiculares DTN (vDTN), particularmente no que se refere à segurança dessas redes.

Capítulo 3

Segurança em Redes Veiculares

Neste capítulo é apresentado um estudo sobre os requisitos de segurança em redes veiculares, os mecanismos já existentes e a sua possível utilização nessas redes. Este trabalho propõe um modelo de confiança com mecanismo alternativo ao gerenciamento de chaves e utilização de reputação, conceitos abordados nesta seção; além de conceitos de mecanismos de criptografia e detecção de intrusos.

As contribuições deste capítulo incluem a discussão sobre mecanismos de segurança aplicáveis em redes vDTN, como forma de entendimento para abordar os trabalhos relacionados ao modelo de confiança por meio de redes sociais proposto para redes veiculares tolerantes a interrupções. São apresentados também os ataques de segurança que ameaçam as redes abordadas neste trabalho e os componentes de segurança na arquitetura WAVE para redes veiculares.

A estrutura deste capítulo é composta em sua primeira parte dos requisitos de segurança em redes veiculares. Os mecanismos de segurança existentes são mostrados na Seção 3.2. A Seção 3.3 apresenta as características pelas quais o gerenciamento de chaves tradicional não é usado em redes DTN. Os ataques de segurança em redes vDTN são descritos na Seção 3.4. Na Seção 3.5 são apresentados os aspectos de segurança da arquitetura WAVE, seguidos da conclusão deste capítulo.

3.1. Requisitos de segurança

Questões de confiança, envolvendo segurança, privacidade e legitimidade são tratadas nas redes veiculares. Os dados enviados pelos usuários são cifrados, de forma a garantir o anonimato e a privacidade dos usuários. Além disso, os dados são analisados para a detecção de informações maliciosas. Por exemplo, o dono de um posto anuncia que certa

avenida está com um fluxo muito melhor que a realidade, pois quer aumentar a quantidade de carros que passam na região para aumentar o seu lucro, ou um usuário mal intencionado que quer provocar um engarrafamento em uma região da cidade.

Os requisitos de segurança em redes veiculares variam de acordo com as situações e cenários em que elas operam, pois há diferentes motivações para ataques a essas redes: informações sigilosas sobre vítimas de acidentes que interessem à imprensa, aumento do congestionamento para dificultar o acesso de equipes ao local, ideais políticos que levem pessoas a atrapalhar o atendimento, interesse de alguma empresa concorrente em explorar o congestionamento ou prejudicar uma empresa afetada pelo acidente, entre outros.

Os recursos de comunicação entre veículos devem prover autenticidade, integridade e confidencialidade, baseados nas necessidades dos usuários finais e suas aplicações. O padrão IEEE 1609.2 refere-se aos serviços de segurança para as aplicações e o gerenciamento de mensagens. O documento relativo [IEEE 2013] define os métodos de processamento e os formatos das mensagens de segurança utilizados pelos sistemas WAVE (*Wireless Access in the Vehicular Environment*) e DSRC (DSRC - *Dedicate Short-range Communications*), padrão de acesso sem fio em ambientes veiculares. Para prover segurança para as mensagens de aplicações e gerenciamento, as funções necessárias para suportar mensagens seguras e privacidade dos veículos são descritas em [Wangham, 2014].

Há requisitos de segurança essenciais às redes veiculares que, quando atendidos, garantem a privacidade entre os nós que fazem parte da rede, além de impedirem o uso indevido e o acesso não autorizado às informações. Dada a diversidade de *hardware* possível, os equipamentos não contam com resistência contra captura e adulteração. Assim, a captura de um nó compromete a segurança da rede, revelando informações como chaves, ou se permitir a reprogramação do nó, torná-lo ferramenta de ataque de adversários.

Os requisitos de segurança considerados neste trabalho para redes veiculares são listados abaixo e pressupõem a utilização de redes DTN. Um sistema de segurança para comunicação segura em redes veiculares [Raya, 2007] atende os requisitos:

- autenticação, para garantir a legitimidade dos usuários que enviam informações;
- verificação de consistência das mensagens, para analisar o conteúdo de mensagens mesmo de usuários legítimos;
- disponibilidade, garantida mesmo sob ação de ataques na rede;
- não-repudiação, um usuário não é capaz de negar a transmissão de uma mensagem;

- restrições de tempo real, respeitar restrições estritas de tempo causadas pelas altas velocidades;
- privacidade, para proteger os usuários contra observadores não autorizados.

Tais requisitos também são discutidos em [Wangham, 2014], afirmando-se que redes veiculares satisfazem, no suporte aos diferentes tipos de aplicações, os requisitos: confidencialidade, integridade, autenticidade, disponibilidade, não repúdio e privacidade. Em [Alves, 2009], além da autenticação dos nós, confidencialidade e integridade dos dados, são destacados dentre os requisitos de segurança mais importantes no contexto de redes veiculares: privacidade, anonimato e controle de acesso. Segundo [Karagiannis, 2011], um trabalho significativo é necessário nas áreas de privacidade, anonimicidade e responsabilidade, pois soluções efetivas ainda não foram providas.

Segundo [Cavalcanti, 2008], o anonimato é fundamental para prever contatos com outros veículos. Em redes veiculares, liberar informações sobre o usuário permite a um atacante rastrear sua trajetória. É indesejável permitir acesso à informação sobre a trajetória de um indivíduo, pois essa informação fere a privacidade da vítima ou ainda seria utilizada para ataques pessoais. Este trabalho propõe formas de restringir quais usuários terão acesso a informações e mensagens de um veículo.

Para um bom funcionamento de redes veiculares, é necessário que os mecanismos de segurança sejam eficientes e de baixo custo computacional [Gansen, 2008]. O interesse em segurança varia dependendo do ambiente e aplicação, embora autenticação e privacidade sejam geralmente críticos [Portmann, 2008]. Essas garantias de segurança são difíceis de serem estabelecidas em uma rede sem conectividade persistente porque a rede teria de utilizar protocolos de criptografia complexos, troca de chaves, e cada nó identificar outros nós esporadicamente visíveis. A autenticação proposta neste trabalho apresenta eficiência e baixo custo devido à forma que o mecanismo utiliza redes sociais.

A mobilidade presente é um desafio fundamental para as redes veiculares, sendo necessário suportar recursos altamente variáveis dentro de curtos períodos de tempo, ou ainda atrasos de propagação longos. As situações e cenários em que as redes veiculares são utilizadas também influenciam os requisitos necessários, sendo um fator essencial considerar a conectividade intermitente. A maior parte das técnicas de segurança envolve a autenticação mútua e a troca de dados restrita entre dois usuários da rede, deixando o restante da rede sem participação nesse processo. No caso de redes tolerantes a interrupções, como as vDTN abordadas, há maior interesse em verificar o acesso para o

tráfego de dados para evitar o encaminhamento por longas distâncias de tráfego que depois será considerado proibido ou indesejado.

Alguns dos requisitos de segurança necessários para proteger as redes veiculares dos ataques e garantir o funcionamento correto dessas redes, como a garantia da integridade dos dados e autenticação dos nós da rede, são também comuns a outras redes, tais como redes *ad hoc* sem fio. Outros, como a garantia da privacidade dos nós, são mais importantes para redes veiculares, já que essas redes revelam detalhes importantes sobre o deslocamento de um veículo. A resposta da rede é diferente quando ocorre uma falha ou uma invasão. No caso de uma falha, a rede tenta contornar o problema identificando outro nó que possa assumir a função do nó com falha. No caso de uma intrusão, a rede isola o nó intruso. A segurança em redes veiculares é uma tarefa mais desafiadora que a segurança de redes sem fio tradicionais.

A limitação de recursos conjugada com outras características das redes tolerantes a interrupções faz com que a segurança nessas redes possua características peculiares. Em redes veiculares DTN, nas quais a comunicação foge dos padrões, a capacidade das conexões é um recurso precioso e o acesso ao serviço de encaminhamento de dados é protegido por alguns mecanismos de controle de acesso, pelo menos em pontos críticos da topologia. Devido à conectividade esporádica e a possibilidade de atrasos na transmissão de mensagens, é necessário eliminar mensagens expiradas e evitar vazamento de informações ao replicar mensagens [Oliveira, 2010]. As redes DTN possuem vulnerabilidades específicas, além daquelas similares às de outras redes sem fio, tais como a possibilidade de adversários manipularem ou injetarem mensagens, comprometerem a disponibilidade, confidencialidade e integridade dos sistemas.

As funções de segurança fundamentais em comunicações veiculares consistem em assegurar a responsabilidade para o criador de um pacote de dados [Engoulou, 2014], de modo que a responsabilidade implica que o remetente da mensagem é responsável pela mensagem gerada. Percebe-se que os requisitos de segurança para uma rede veicular dependem da sua aplicação, sendo necessário prover autenticidade, garantia e flexibilidade nos aspectos de segurança, baseados nas necessidades dos usuários finais e restrições de seus equipamentos. Os mecanismos de segurança consideram a conectividade intermitente, de forma a evitar interferência de agentes externos à rede.

3.2. Mecanismos de segurança

Esta seção apresenta os mecanismos de segurança existentes e sua possível aplicação em redes veiculares, quais sejam mecanismos criptográficos, baseados em reputação ou detecção de intrusos. A utilização de mecanismos de segurança em redes veiculares se justifica na quase totalidade das aplicações, especialmente considerando a conectividade como recurso precioso e tráfego de informações sobre usuários, sendo necessário manter a privacidade dos motoristas.

3.2.1. Mecanismos de reputação

O conceito de reputação é definido como uma medida coletiva de confiança em uma pessoa ou coisa, baseada em indicações ou avaliações de membros de uma comunidade [Paula, 2010]. Em VANETs, a reputação de um veículo é considerada como um histórico sobre as informações repassadas aos outros veículos. Essa reputação é então utilizada como critério 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 (*Peer-to-Peer*) e VANETs geralmente consideram que há conectividade suficiente para garantir a existência de caminhos fim-a-fim a todo o momento entre quaisquer dois nós da rede. Existem ainda propostas nas quais se considera que a movimentação dos nós da rede, de maneira geral, causará apenas pequenas alterações em sua topologia. Em redes veiculares DTN, restringe-se a aplicabilidade desses mecanismos de reputação propostos para redes P2P e VANETs.

Sistemas distribuídos que não possuem uma coordenação geral como redes *ad hoc* ou redes *Peer-to-Peer* (P2P) estão sujeitos a diversos tipos de adversários e ataques. Técnicas de criptografia são capazes de neutralizar os efeitos de alguns ataques externos, uma vez que esses adversários não conseguem acessar os dados trafegados pela rede. Porém, quando um nó autenticado da rede atenta contra o funcionamento das aplicações, torna-se necessário o uso de mecanismos de segurança adicionais. Sistemas de reputação são utilizados para garantir o comportamento cooperativo em redes distribuídas.

No modelo deste trabalho, os veículos que divulgam informações úteis para outros veículos podem receber uma assinatura em seu certificado por meio do mecanismo de reputação. Assim, é possível que outros usuários reconheçam-no como confiável segundo

o mecanismo de reputação proposto por meio de certificados, o que atuará como recompensa para os usuários que repassam informações verdadeiras.

3.2.2. Detecção de intrusos

Sistemas de detecção de intrusos são meios técnicos de descobrir em uma rede acessos não autorizados que indicam a ação de um intruso ou até de usuários mal intencionados. Um intruso é considerado como uma entidade interna (nó malicioso) ou externa à rede [Burgess, 2007], que age sobre a rede de forma ativa, modificando, suprimindo ou inserindo pacotes de mensagens trafegadas, impedindo assim o funcionamento correto da rede. Intrusos também agem de forma passiva, obtendo sem autorização informações sigilosas das mensagens trafegadas em uma determinada rede.

Na presença de um intruso, a rede pode se comportar de diversas formas: continuar funcionando normalmente, sem permitir o acesso do adversário à rede, tampouco sofrer os efeitos da sua presença; reduzir a produção da rede, silenciando alguns nós, ou até mesmo interromper o funcionamento de toda a rede. Assim, neste trabalho as redes veiculares permanecem confiáveis, em bom funcionamento, ainda que haja presença de intrusos.

Para proteger as redes contra alguns tipos de ataques e prevenir que nós adversários se façam passar por nós legítimos de uma rede, são utilizados mecanismos de identificação baseados em métodos criptográficos, por exemplo. Entretanto, existem ataques para os quais não são conhecidos mecanismos preventivos, por exemplo, o ataque de canalização (*wormhole*). Para esses casos, a rede precisaria de um sistema de detecção de intrusos e a presença de adversário colocaria a rede em estado de alerta. Se não for possível decidir qual é o nó intruso, a rede reduzirá as possibilidades de comunicação.

Muitos ataques são facilitados se o adversário conseguir influenciar o estabelecimento de rotas na rede, manipulando a comunicação entre nós legítimos. Essa manipulação inclui injeção de mensagens maliciosas na rede, replicação de mensagens antigas e modificação do conteúdo de mensagens válidas. Nesse caso, o objetivo do adversário é o controle das mensagens enviadas pelos usuários quando não há conectividade. Uma atualização na árvore de roteamento resolve o problema, ocasionado por uma falha, em relação ao roteamento. A execução da atualização do roteamento não elimina o intruso, pois ele está preparado para participar dessa atualização. Entre os objetivos deste trabalho na segurança das redes vDTN, a reputação dos usuários permitirá que a rede opere normalmente mesmo sob a ação de um ataque.

Diversos mecanismos evitam a ação de um adversário em redes veiculares. O *controle de acesso* à rede impede a entrada de nós adversários, a *detecção de intrusos* aponta os nós intrusos em ação na rede e, finalmente, *mecanismos de revogação* de nós isolam os nós intrusos, de forma que sua ação não tenha mais efeito. Por meio da detecção de intrusão, é possível verificar que um mecanismo de defesa foi violado, possibilitando a reação automática.

Mesmo para ataques para os quais já existam mecanismos de prevenção, a necessidade da detecção de intrusos ou abordagens complementares se justifica porque mesmo os métodos mais eficazes de prevenção podem falhar. A vantagem de técnicas descentralizadas é a disponibilidade instantânea da informação, visto que os nós detectam adversários no momento da comunicação. O mecanismo de reputação proposto neste trabalho atuará em conjunto aos mecanismos preventivos.

A detecção de intrusos é normalmente seguida da revogação dos nós com comportamento indevido. A revogação representa a exclusão do nó da rede, tornando impossível para ele a comunicação com seus vizinhos. Esse processo é autenticado, para evitar revogação de nós autênticos por intrusos. Como os nós não são protegidos contra violação física (*tampering*) no modelo de rede utilizado neste trabalho, o mecanismo de reputação encaminha implicitamente a revogação de nós. De outra forma, um nó intruso autenticado pela rede, provavelmente originado de uma violação física, isolaria nós autênticos, promovendo assim outros tipos de ataque de negação de serviço.

3.2.3. Mecanismos criptográficos

A criptografia é uma técnica usada para ocultar as informações do adversário, garantir a autenticidade da informação ou ainda garantir a integridade e o frescor dos dados. O uso de criptografia com gerenciamento adequado de chaves é necessário para atender a requisitos de segurança. Atualmente são utilizadas técnicas de segurança aceitas como criptografia de chave pública comum e assinatura digital, que não são adequadas a redes DTN devido à dependência de entidades centralizadoras sem conectividade constante para gerenciar a distribuição de chaves de forma confiável, por exemplo.

As técnicas fim-a-fim para segurança em DTN não são atrativas, pois existe a possibilidade de utilizar recursos escassos para mensagens indesejáveis quando se transporta tráfego por todo o caminho até seu destino sem realizar autenticação e checagem de controle de acesso. A alternativa é usá-los a cada passo do roteamento. Nesse caso, é

necessário um compartilhamento de chaves entre os vários nós que precisam se comunicar diretamente para a execução do roteamento, conforme a proposta deste trabalho.

Encriptação

Encriptação é o processo de transformar informação para impossibilitar a sua leitura por usuários não autorizados. Os protocolos DTN devem prover um meio de encriptar elementos de forma que mensagens em trânsito não possam ser lidas por terceiros. A camada de agregação DTN (*bundle)* não provê nenhuma confidencialidade para a origem ou destino [Fall, 2003]. Similarmente, protocolos de redes DTN devem possibilitar a aplicação de uma verificação de integridade de maneira que a identidade do nó origem seja provada e alterações em partes específicas da mensagem possam ser detectadas.

Para resolver os problemas do compartilhamento e multiplicação das chaves [Di Pietro, 2014], utiliza-se a criptografia assimétrica em que são geradas duas chaves, uma pública e uma privada. Essas chaves são matematicamente relacionadas de forma que qualquer uma cifra um documento, mas somente a outra decifra, ou seja, se um documento foi cifrado com a chave privada, somente a chave pública correspondente poderá decifrá-lo. Assim, cada usuário que necessite realizar transações eletrônicas terá uma única chave pública e uma única chave privada, sendo que só a chave pública é compartilhada.

Assinatura digital

Assinatura é um processo criptográfico que adiciona um código gerado utilizando uma chave a uma mensagem e o verificador tem que conhecer a chave de verificação para assinatura. Em redes DTN, as chaves são compartilhadas pelos nós vizinhos para permitir a verificação salto-a-salto. Técnicas de assinatura tornam possível a autenticação e integridade na comunicação. O uso dessas técnicas de segurança evita a inserção de pacotes falsos e a adulteração de mensagens.

Uma das diferenças das redes DTN é que uma mensagem autenticada usando uma assinatura digital, em princípio, é verificada por qualquer elemento da rede no caminho. Se a mensagem contém informação suficiente, então qualquer nó consegue pelo menos verificar a exatidão criptográfica da assinatura [Burgess, 2007].

Gerenciamento de chaves

Gerenciamento de chaves é a administração de tarefas envolvendo a geração, armazenamento, distribuição, proteção e revogação de chaves criptográficas, de modo que elas estejam disponíveis aos nós autênticos da rede. O gerenciamento de chaves é responsável por manter as relações criptográficas e o material criptográfico, por exemplo, os pares de chaves pública e privada, os parâmetros de inicialização e os parâmetros não secretos.

Um esquema de distribuição de chaves seguro e eficiente permite a autenticação dos nós da rede. Os processos de criptografia têm como objetivo comum impedir que adversários obtenham informações sigilosas. A captura e adulteração de um nó permite ao adversário utilizar as chaves armazenadas nesse nó. É necessário prever quais chaves são descobertas a partir dessa adulteração.

As características das redes veiculares exigem novas abordagens para que seja possível atender os requisitos de segurança necessários a algumas aplicações [Symington, 2011]. Este trabalho propõe um mecanismo alternativo para compartilhamento de chaves, por meio da utilização de certificados assinados pelo próprio usuário e por usuários que já confiam nele.

3.3. Desafios de segurança em DTN

Para estabelecer confiança entre os usuários em redes DTN, é necessária uma alternativa que torne viável o gerenciamento de chaves criptográficas com tolerância a desconexões, pois nenhum esquema de gerenciamento de chaves ainda é reconhecido como adequado para redes tolerantes a interrupções [Symington, 2011][Lv, 2014]. Os protocolos de redes *ad hoc* necessitam de serviço de distribuição de chaves ou verificação *on-line*, impraticável nos ambientes de conectividade intermitente como em redes veiculares.

A abordagem tradicional de PKI não é adequada em DTN, pois sem acesso *on-line* a certificado ou chave pública de um nó arbitrário, o envio de uma mensagem criptografada em tempo real não é possível [Seth, 2005]. Além disso, a ausência de acesso imediato a listas de revogação de certificados impede de autenticar a chave pública do remetente ou o certificado em DTN. À primeira vista, redes DTN são muito parecidas com as redes *ad hoc*, porém a diferença é nítida quando se avalia a abordagem do problema de roteamento. Em redes *ad hoc* é necessário que se conheça todo o percurso para que os protocolos

funcionem. Há casos em que é possível construir toda uma rota de envio, mas existem diversas situações em que isso não é alcançável.

Segundo [Bhutta, 2014], DTN exige a definição de novos protocolos de segurança e gerenciamento de chaves, pois protocolos tradicionais de segurança fim-a-fim não funcionam. Em redes DTN é irreal assumir que haverá autoridades certificadoras com infraestrutura sempre presente e disponível para utilização de criptografia de chave pública [Jia, 2012]. A rede social proposta neste trabalho utiliza certificados e chaves públicas para determinar a confiança dos usuários da rede.

Os protocolos existentes na literatura de gerenciamento da confiança não levam em conta a relação social, que é um fator importante para o gerenciamento de confiança em DTNs com a proliferação de dispositivos móveis transportados e operados por humanos. Além disso, não consideram a questão do gerenciamento de confiança dinâmico, ou seja, como um protocolo de confiança pode melhor responder às mudanças das condições ambientais, como um crescente mau comportamento de nós ou desenvolvendo hostilidade ou relações sociais [Chen, 2014]. O modelo de confiança proposto neste trabalho é dinâmico com propagação por redes sociais em redes vDTN, que não dependem de caminhos fim-a-fim como redes *ad hoc.*

O modelo de segurança para a arquitetura DTN difere das redes tradicionais, pois o conjunto de participantes inclui os próprios roteadores [Fall, 2003]. Em MANET, os mecanismos de segurança são baseados na premissa de que existe uma ligação entre os nós de origem e destino (conexões fim-a-fim). Em geral, os métodos de segurança em redes são baseados em autenticar os usuários e a integridade das mensagens. No entanto os roteadores que encaminham as mensagens não são autenticados. Nas redes DTN os roteadores e *gateways* também têm que ser autenticados, conservando a rede, o mais cedo possível, de ficar trafegando informações não autorizadas.

Embora vários protocolos de segurança estejam propostos na literatura para prover autenticação e controle de acesso em pontos múltiplos de redes *ad hoc*, a maior parte deles não é tolerante a longas latências. Em particular, protocolos que requerem múltiplas trocas de informações ou múltiplas interações entre cliente e servidor para alcançar a segurança objetivada não serão apropriados para DTN [Seth, 2005]. Muitas vezes será impossível entrar em contato com o servidor de interesse ou ter conectividade por um período suficiente para transferir o material para a autenticação necessária [Portmann, 2008].

Seria interessante se a assinatura digital não exigisse a presença de uma autoridade confiável [Tanenbaum, 2011], visto que dificilmente alguma organização inspira total

confiança a todos os cidadãos. É necessário que autoridades certificadoras sejam consultadas para ter certeza da validade de um certificado, pois a revogação do certificado anula sua validade. Ter de lidar com a revogação (e talvez com a reabilitação) elimina uma das melhores propriedades dos certificados, ou seja, a possibilidade de usá-los sem ter de entrar em contato com uma autoridade certificadora [Tanenbaum, 2011].

A proposta de autenticação [Fernandes, 2008] prevê uma autoridade certificadora distribuída baseada em cadeias de confiança, que registra os endereços dos nós da rede *ad hoc*, associando a cada endereço uma chave pública, e emite certificados. A segurança baseia-se em testemunhas, que são nós escolhidos por meio de funções hash para monitorar um determinado nó. O funcionamento da rede depende inteiramente da cooperação e confiança entre os nós que possuem algum tipo de relação de confiança pré-estabelecida. Nesse caso, relações de confiança formadas a qualquer momento, a entidade autenticadora é distribuída e fica disponível em todos os momentos, permitindo o provimento de todos os serviços de uma autoridade certificadora ao longo do funcionamento da rede, tais como o registro de novos usuários, a emissão e a revogação de certificados [Fernandes, 2008].

Soluções projetadas para redes *ad hoc* não são apropriadas [Hui, 2005] [Jagadale, 2015]. As técnicas que dependem de acesso sob demanda a serviços centralizados não podem ser usadas, nem pode ser feita o pressuposto de que todos os nós intermediários são de confiança. Nesse caso como todos os nós de redes DTN são potencialmente maliciosos, o controle de acesso e a autenticação na rede, embora efetivos em outras situações, não são suficientes para proteger a DTN contra nós maliciosos [Hui, 2005].

Apesar de já existirem protocolos eficientes de autenticação e de controle de acesso, esses protocolos foram projetados para operar em redes *ad hoc* com pequenos atrasos e não apresentariam um desempenho aceitável em DTNs [Oliveira, 2007]. Em particular, a atualização de listas de controle de acesso e listas negras é especialmente difícil em ambientes com longos atrasos. Além disso, propostas que requerem frequentes acessos a servidores centralizados para completar a autenticação ou autorizar uma transação também não se mostrariam eficientes. Outras funções básicas de segurança tornam-se de difícil solução em redes DTNs. Sem um controle de integridade, por exemplo, não há como garantir que a carga útil dos agregados não seja corrompida enquanto estiver em trânsito e o destinatário pode não estar apto a detectar as alterações. Da mesma forma, a confidencialidade dos dados e o não-repúdio são difíceis de serem obtidos [Oliveira, 2007].

Os mecanismos de reputação propostos para redes DTN, como [Dini, 2012] [Paula, 2010], dependem de outras soluções para autenticação de mensagens. Assim como a Encriptação Baseada na Identidade teve sua aplicabilidade avaliada em DTN, permitindo melhores formas de prestação de confidencialidade, mas não foi considerada uma solução adequada e escalável para DTN [Farrel, 2006]. Segundo [Asokan, 2007], não há nenhuma vantagem significativa sobre a criptografia tradicional para autenticação e integridade. Afirma-se em [Wu, 2015] que a maior parte dos mecanismos usuais de autenticação requer alto custo de criptografia com premissa de uma autoridade centralizadora. Porções de uma rede DTN podem desprender-se do resto da DTN e voltar a conectar-se a um ponto da DTN diferente em um momento posterior.

Propostas existentes de reputação para VANETs [Daeinabi, 2013] [Li, 2012] centralizam as informações consultadas para o cálculo da reputação do sistema, que são armazenadas em um servidor. Quando um veículo é considerado malicioso, é retirado da lista branca de confiança e acrescentado na lista negra. Uma Autoridade Certificadora (AC) transmite periodicamente essas listas para os veículos da rede, o que não funciona em redes vDTN. O modelo de confiança deste trabalho propõe o uso de reputação descentralizada, visto que os usuários gerenciam e armazenam suas listas de usuários confiáveis.

Os sistemas propostos de reputação *ad hoc* [Li, 2012] [Paula, 2010] tem problemas de falhas devido ao uso de servidores em locais como postos de combustíveis e semáforos para armazenar a reputação dos veículos, o que inclui a coleta de relato de experiências para reputação e a propagação desta reputação na rede. Em RS4VANETs [Fernandes, 2015], a lista de reputação é propagada por RSUs (*roadside units*) para os veículos. Um esquema de votação proposto para reputação com uso de RSUs [Huang, 2014] cita como questão aberta o atraso nas transmissões que afeta a tomada de decisões. Este trabalho propõe um mecanismo de reputação distribuído independente da existência de infraestrutura ou servidores, com uso de redes DTN.

Mecanismos de reputação propostos para redes *ad hoc* 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 [Paula, 2010]. Assim, tornam-se possíveis soluções nas quais dados utilizados pelo mecanismo de reputação são armazenados de forma distribuída na rede 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,

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 mecanismo de reputação [Buchegger, 2004].

A aplicabilidade de mecanismos de reputação propostos para redes *ad hoc* e P2P no contexto das redes veiculares é bem restrita, haja vista que algumas considerações feitas nessas soluções, como citadas acima, não podem ser garantidas em redes veiculares, dadas as grandes velocidades de deslocamento dos veículos que compõem a rede [Paula, 2010]. Assim, surge a necessidade do desenvolvimento de soluções próprias para as redes veiculares DTN, nas quais suas características particulares são levadas em conta.

Os primeiros veículos a receber mensagens de reputação normalmente são aqueles mais próximos dos eventos de trânsito. Em situações nas quais a fonte de informação é desconhecida do receptor, não existe nenhuma base de confiança para o julgamento dos dados, haja vista que pouca ou nenhuma opinião foi adicionada à mensagem antes de seu recebimento [Paula, 2010]. Logo, nesses casos, mensagens geradas por veículos têm o mesmo peso que aquelas geradas por intrusos. Em redes *ad hoc*, o nó sempre está conectado a pelo menos um vizinho. Assim, ele pode escolher quando enviar os dados e, por exemplo, aproveitar um momento de canal livre. Por outro lado, na rede DTN, o nó se comunica quando há conexão. Assim, um nó que teve uma experiência na rede, boa ou ruim, pode ter somente uma ou mesmo nenhuma oportunidade de compartilhá-la na rede.

Uma comunicação confiável fim-a-fim dificilmente estará disponível entre os usuários e o centro de gerenciamento de chaves [Zhou, 2014], o que levaria a rede DTN a grande gasto de recursos e tempo de atraso. Mesmo que a comunicação seja possível, há casos em que a comunicação *ad hoc* é necessária devido à urgência. Por exemplo, acidentes serão evitados se sensores de um veículo gerarem evento para notificar os veículos mais próximos para acionar o freio com urgência. Nesse caso não haveria tempo de validação do emissor em uma autoridade centralizadora. Considera-se neste trabalho que a rede DTN provê entrega de mensagens sem infraestrutura de rede ou quando tal infraestrutura não estiver disponível.

Este trabalho propõe formas de diferenciar os certificados dos usuários atribuindo aos mesmos graus de confiança, tratando o aspecto da revogação de certificados em redes DTN. Se todos os usuários da rede veicular, legítimos ou não, possuem certificados oriundos da mesma autoridade certificadora, um usuário mal-intencionado ainda pode

interferir na rota de outro usuário ou restringir as informações recebidas a um determinado grupo de nós, pois não há distinção entre ele e os demais usuários. Tais questões são tratadas neste trabalho por meio de redes sociais e mecanismo de reputação.

Portanto, a certificação tradicional e mecanismos de gerenciamento de chaves anteriormente propostos não funcionam em redes vDTN. A certificação de todos os usuários da rede veicular pelas mesmas autoridades certificadoras atestaria a identidade de um motorista, mas não comprovaria sua confiança no caso dele trabalhar em posto de combustível, por exemplo. Assim como a certificação, o gerenciamento de chaves em DTN precisa ser executado de forma distribuída, como proposto neste trabalho.

3.4. Ataques de segurança em vDTN

Para construir uma arquitetura de segurança robusta para vDTN, é importante estudar as características dos ataques possíveis. O fato dessas redes ainda estarem em implementação faz com que a situação seja ainda mais complicada [Wangham, 2014]. Ataques contra a disponibilidade estão presentes nas diversas camadas de protocolos, especialmente pela facilidade de execução e pelo impacto sobre a aplicação, seja parcial ou totalmente inutilizada. Esses ataques são conhecidos por negação de serviço ou *Denial of Service* (DoS) [Hu, 2003].

Este trabalho permite que as redes veiculares continuem funcionando normalmente, mesmo sob a ação de um ataque do tipo *sybil* ou conluio (Seção 5.3), bem como alarmes trocados (Seção 7.2). Assim como ataques de negação de serviço distribuídos são ameaça para a Internet, a proteção e o controle de acesso à infraestrutura da rede é crítico em redes DTN, que tipicamente apresentam desafios em termos de recursos, sendo extremamente necessária a capacidade de manter a comunicação sofrendo esses ataques. Como essas redes sofrem impacto de altos tempos de resposta, baixa taxa de conexões e frequentes partições, eficiência é um fator importante em qualquer solução de segurança.

No modelo deste trabalho são possíveis a escuta e a criação de interferência, pois a comunicação é sem fio. Existem dois tipos de ataques contra a segurança de redes *ad hoc* móveis sem fio, passivos e ativos. O adversário descansa sem ser notado na rede enquanto promove um ataque passivo, sem perturbar as funções do protocolo, e escutando toda a informação útil sobre a rede e os nós participantes. Em ataques ativos, o adversário perturba o correto funcionamento do protocolo de roteamento, modificando alguma

informação ou promovendo ataques de negação de serviço. É importante utilizar mecanismos que permitam isolar esses nós detectados com comportamento indevido, como proposto no mecanismo de reputação deste trabalho.

Caso o adversário descubra as informações secretas da rede e insira essas informações em um nó estranho à rede, sendo aceito como nó da rede, é caracterizado um ataque interno. Já um ataque realizado por um computador portátil estranho à rede, é considerado um ataque externo. Nesse caso, ele não possui informações que são importantes para o funcionamento da rede, como as chaves e não consegue provar que é nó da rede, a comunicação será evitada pela utilização de certificados proposta.

A proteção para as redes *ad hoc* contra alguns tipos de ataques utiliza mecanismos preventivos. Para prevenir que nós adversários se façam passar por usuários legítimos de uma rede, por exemplo, são utilizados mecanismos de identificação baseados em métodos criptográficos como o proposto neste trabalho. Entretanto, existem ataques para os quais não são conhecidos mecanismos de prevenção, um exemplo é o ataque de canalização (*wormhole*). Para esses casos, a rede precisaria de um sistema de detecção de intrusos ou mecanismos para identificar adversários que fazem parte da rede veicular.

Neste trabalho é possível a captura de nós e inserção de nós adulterados, por ser ambiente aberto. Como o adversário tem acesso físico aos nós, eles podem ser violados fisicamente. A violação física (*tampering*) visa modificação, substituição ou destruição de hardware ou software. Assim, o adversário tem o intuito de obter informações secretas, como chaves criptográficas, ou de levar os protocolos a um comportamento anômalo, prejudicando a aplicação. Diversas formas de intrusão são documentadas na literatura [Engel, 2006] para redes móveis *ad hoc* e consideradas no contexto de redes veiculares.

Ataques contra disponibilidade

Uma classe de ataques é contra disponibilidade dos recursos da rede. Num ataque de exaustão (*exhaustion*), por exemplo, o adversário levaria um nó a fazer um número elevado de transmissões, desperdiçando recursos. Já a supressão de mensagens é um ataque que viola a integridade da mensagem: um atacante intercepta seletivamente pacotes da rede e suprime (bloqueia) esses pacotes que inclusive serão utilizados em outro momento [Wangham, 2014]. O objetivo nesse caso é impedir o aviso de congestionamento.

Ao promover um ataque de integridade, o nó malicioso perde mensagens, redireciona tráfego para um destino diferente, ou informa longas rotas com objetivo de aumentar o atraso na comunicação. O ataque mais famoso nesta categoria é a criação de um *blackhole*,

onde um adversário absorve todos os pacotes que passam por ele. As rotas são influenciadas pelo intruso, sendo um nó invasor ou um nó legítimo, já violado, no ataque buraco negro (*blackhole* ou *sinkhole*). Nesse caso, o adversário deseja obter informações da rede ou aplicar o ataque de negligência. Como uma forma de extensão, o adversário promove um ataque *greyhole*, permitindo alternar entre encaminhar pacotes ou descartá-los. Um ataque de temporização ocorre se um veículo malicioso recebe mensagem de emergência e não a transmite imediatamente aos seus vizinhos [Wangham, 2014].

Uma mensagem disponível num ponto da rede é enviada para outro ponto distante, com o estabelecimento de um túnel na rede entre dois ou mais nós que colaboram de forma que os intrusos sejam ligados por uma rede privada, assim o *wormhole* permite ao adversário interferir no fluxo normal dos pacotes. A canalização é uma manipulação de comunicação, pois leva uma mensagem a um ponto da rede aonde ela não chegaria, ou chegaria com uma latência maior. Assim, o adversário conseguiria influenciar rotas, e, em conjunto com outros ataques, omitir informações, prejudicando a aplicação. Após redirecionar os pacotes para outro ponto da rede veicular, o adversário os replica na rede.

Ataques do tipo *tampering* são baseados na distribuição de mensagens de roteamento falsas e são difíceis de identificar e rastrear. O ataque *rushing* é um exemplo de ação como um ataque efetivo de negação de serviço contra todos os protocolos de roteamento de redes *ad hoc* sob demanda propostos atualmente. Promovendo esse ataque, o adversário rapidamente espalha mensagens de roteamento por toda a rede, desabilitando mensagens de roteamento autorizadas com a consequência que outros nós as deletam como cópias replicadas. Obviamente, rotas computacionais para algum destino também são canceladas pela montagem de mensagens de erro de roteamento, afirmando que o vizinho não será alcançado. Logo, como difusão é mecanismo mais comum usado por protocolos de roteamento sob demanda para estabelecer rotas, perturbar a difusão é um ataque eficiente contra esse tipo de protocolo.

Ataques contra a autenticidade e a identificação

Outro tipo de ataque evitado com a utilização de certificados, proposta neste trabalho, é promovido quando o adversário tem objetivo de adotar alguma outra identidade na rede para parecer confiável. Consequentemente, ele opera como um nó da rede e divulga informações incorretas de roteamento, por exemplo. Um ataque perigoso é conhecido como *sybil* onde nós maliciosos não somente representam outros nós como multiplicam identidades falsas. Redes móveis que utilizam algum modelo de confiança são

particularmente vulneráveis a esse ataque, pois o intruso gera recomendações falsas sobre a confiança de um nó específico para atrair mais tráfego da rede para ele, o que oferece um ponto de partida ideal para ataques *wormhole*.

Ao simular várias identidades por meio de ataques de *sybil*, seria possível atrapalhar os protocolos de roteamento e, assim, prejudicar o envio de mensagens. Outras formas de ataques são possíveis se o intruso conseguir inserir-se na rede, fazendo se passar por um nó legítimo. Seria possível, por exemplo, comprometer o roteamento das mensagens por meio de ataques de negligência (*neglect and greed*) ou retransmissão seletiva (*selective forwarding*). O adversário ignoraria seu papel de roteador, deixando de retransmitir algumas mensagens.

Ataques contra a integridade e confiança dos dados

Na modificação de mensagem (*man in the middle*) nas redes veiculares, o atacante é um veículo que está inserido entre dois veículos que se comunicam. O atacante intermedia a comunicação das duas vítimas e modifica suas mensagens, interceptando as mensagens enquanto os usuários acreditam que estão se comunicando diretamente [Wangham, 2014]. Injeção de informação falsa (*bogus information*) ocorre quando um atacante, um intruso ou um usuário legítimo, transmite informações falsas na rede veicular para obter vantagens ou afetar a decisão de outros veículos [Wangham, 2014].

Num ataque de conluio, um atacante forma alianças com outros nós da rede para alcançar um objetivo comum, como vandalismo ou terrorismo na rede. Esse ataque resulta na indisponibilidade da rede ou de uma aplicação ou denegrir a reputação (confiança) de um veículo [Zhang, 2011]. Ataques contra a privacidade representam a violação da privacidade dos condutores e usuários em VANETs. Como exemplo, tem-se o rastreamento de um veículo durante a sua viagem [Wangham, 2014].

Alguns desses ataques são prevenidos por meio do uso de protocolos criptográficos bem projetados, tais como: injeção de mensagens maliciosas, replicação de mensagens antigas e modificação do conteúdo de mensagens válidas. Entretanto, existem ataques que são difíceis de serem prevenidos; para esses casos e para os casos onde os mecanismos de prevenção forem comprometidos, a utilização de um sistema de detecção de intrusos torna-se primordial.

3.5. Segurança na arquitetura WAVE

A arquitetura WAVE (*Wireless Access in the Vehicular Environment*) [IEEE, 2010] é o padrão de acesso sem fio definido para ambientes veiculares. O padrão IEEE 802.11p foi definido por um grupo de trabalho do IEEE para facilitar a implantação de redes veiculares em ambientes de alta velocidade (comunicação V2V e V2I). Sua descrição é composta por doze documentos, sendo que o documento 1609.2 [IEEE, 2013] especifica um conjunto de serviços para prover segurança às mensagens WAVE contra análise de tráfego (*eavesdroping*), forjamento (*spoofing*) e outros tipos de ataques em ambientes de redes veiculares [Wangham, 2014]. O padrão IEEE 1609.2 envolve basicamente de três componentes [Schütze, 2011]:

- Algoritmos de assinaturas digitais usando criptografia de curvas elípticas (ECC), especificamente o padrão ECDSA (*Elliptic Curve Digital Signature Standard*);
- Esquema híbrido de cifragem assimétrica com ECC, especificamente o esquema ECIES (*Elliptic Curve Integrated Encryption Scheme*). A criptografia assimétrica é utilizada apenas para o transporte da chave simétrica;
- Esquema puramente simétrico para cifragem autenticada é utilizado para garantir a integridade de forma eficiente e, opcionalmente, para trocas cifradas com menos sobrecarga. O CBC-MAC com AES (AES-CCM) é um exemplo de esquema suportado.

O padrão IEEE 1609.2 define uma forma compacta de certificado digital, chamada de certificado WAVE, e define a existência de autoridades certificadoras [Wangham, 2014]. O padrão descreve uma aplicação denominada entidade de gerenciamento de certificados, responsável por gerenciar o certificado raiz e armazenar as listas de certificados revogados [Schütze, 2011]. Os serviços de segurança WAVE definidos na IEEE 1609.2 consistem em [IEEE, 2013]:

- Serviços de processamento de segurança: oferecem mecanismos para estabelecer comunicações seguras com o objetivo de proteger os dados e prover segurança para os anúncios de serviços WAVE (*WSAs - WAVE Service Advertisements*).
- Serviços de gerenciamento de segurança: Serviços de gestão de certificados são serviços providos pela Entidade de Gerenciamento de Certificados (*CME - Certificate Management Entity*), as quais gerenciam informações relacionadas à validade de todos os certificados; Serviços de gerenciamento de segurança de

provedores de serviços são providos pela Entidade de Gerenciamento de Provedores de Serviços (*PSSME - Provider Service Security Management Entity),* gerenciam as informações relacionadas aos certificados e às chaves privadas que são usados no envio seguro dos anúncios de serviços WAVE (WSAs).

Com a norma IEEE 1609.2, tem-se uma base criptográfica sólida para a concepção de sistemas de transportes inteligentes seguros. Porém, isto dependerá dos fabricantes e fornecedores que precisam implementar este padrão em sua forma completa [Schütze, 2011]. Além disso, de acordo com o autor, a implementação da norma IEEE 1609.2 em software não é uma solução muito realista, devido às limitações de desempenho e conectividade. Além do problema de desempenho, os processadores automotivos atuais não têm proteção suficiente contra manipulações maliciosas [Wangham, 2014].

A norma IEEE 1609.2 especifica apenas os formatos e como ocorrem os processamentos para prover segurança criptográfica [Wangham, 2014]. Porém, a privacidade e o anonimato são questões consideradas fora do escopo, já que requerem atenção por parte dos desenvolvedores das diferentes partes de um dispositivo WAVE [IEEE 2013]. A arquitetura não considera tolerância a interrupções e demanda novas soluções de criptografia para redes veiculares.

Este trabalho utiliza algoritmos de criptografia de curvas elípticas e o formato de certificado WAVE, definido no padrão IEEE 1609.2 como uma forma compacta de certificado digital [IEEE, 2013]. O padrão define, por exemplo, como a chave pública de um usuário é usada para criptografar uma mensagem ou como é realizada a autenticação do usuário. Diferentemente desse padrão, neste trabalho não há um gerente de segurança e o próprio usuário é responsável pela criação, validação e revogação dos certificados.

3.6. Conclusão

Neste capítulo, foram apresentados os aspectos relativos à segurança em redes veiculares tolerantes a interrupções. Baseado em uma revisão da literatura, foi possível listar os principais requisitos de segurança, que foram considerados no modelo de confiança proposto. Também foram identificados os principais mecanismos de segurança existentes para redes veiculares.

As possíveis utilizações de mecanismos de segurança na arquitetura WAVE e em redes vDTN foram analisadas, mostrando questões em aberto existentes quando considera-se a tolerância a interrupções na comunicação entre veículos. Foi abordada a necessidade de uma alternativa para prover autenticação e confiança em redes vDTN, pois mecanismos tradicionais de redes *ad hoc* não funcionam nessas redes. Por fim, foram listados ataques de segurança a que estão sujeitas as redes veiculares.

Capítulo 4

Trabalhos Relacionados

Nesta seção, são descritos e revisados os trabalhos publicados no IEEE, ACM e *Elsevier Science Direct* entre 2005 e 2015, que abordam segurança em redes veiculares, redes sociais ou redes DTN. Foram comparados 46 artigos publicados em congressos e revistas, com objetivo de identificar as soluções propostas por meio de uma revisão sistemática da literatura, relacionando-as com o mecanismo proposto neste trabalho.

Estudos foram coletados em bases de dados eletrônicas com os seguintes critérios: artigos revisados; acesso completo aos artigos; motor de busca por palavras-chave por campo; e reconhecida reputação na publicação de conteúdo de alta qualidade. Na lista de bancos de dados selecionados tem-se: *ACM Digital Library* (http://portal.acm.org/); IEEExplore (http://www.ieeexplore.ieee.org/); *Elsevier Science Direct* (http://www.sciencedirect.com/). Foi realizada uma revisão de investigação em dois passos: pesquisa através do *Google Scholar* (http://scholar.google.com) e inspeção manual da bibliografia dos artigos selecionados entre 2012 e 2015.

As propostas estudadas neste capítulo foram classificadas segundo os critérios: Rede social ou DTN, assim como três possíveis abordagens para segurança – Confiança, Reputação ou Autenticação. Tal classificação é mostrada de forma gráfica em uma taxonomia ao final desta seção.

A estrutura deste capítulo é composta por trabalhos relacionados à confiança em redes veiculares na Seção 4.1, os relacionados às redes sociais veiculares na Seção 4.2 e aqueles relacionados a redes DTN e infraestrutura na Seção 4.3, seguidos da taxonomia das propostas e conclusão do capítulo.

4.1. Confiança em VANETs

Veículos que recebem informações de outros veículos ou entidades da rede precisam saber a confiança de quem gerou aquela informação [Karagiannis, 2011]. Os autores propõem que o nível de privacidade seja ajustado pelo usuário, considerando ainda aberta a pesquisa na área de anonimicidade e privacidade adaptativa, onde usuários selecionariam a privacidade que desejam ter. Tais questões são abordadas neste trabalho tratando usuários em uma rede social, que permite ao usuário definir quais usuários são confiáveis.

Um estudo quantitativo sobre modelos de confiança e protocolos de gerenciamento de confiança em redes sociais baseadas em redes móveis sem fio foi realizado em [Malhotra, 2014]. Segundo o autor, a confiança direta entre dois nós representa avaliação baseada em observação direta ou experiência em relação a um nó, enquanto a confiança indireta considera evidências como recomendações de outros nós vizinhos. Este trabalho propõe graus de confiança semelhantes por meio de relacionamentos de amizade entre nós.

Uma abordagem de rede social para gerenciamento de confiança em VANETs foi proposta em [Huang, 2014]. Os autores apresentam várias limitações dos sistemas atuais de gerenciamento de confiança em VANETs e argumentam que a sua natureza efêmera as torna inúteis em situações práticas. Foi identificado em [Huang, 2011] um problema causado devido à votação simples para a tomada de decisão, que geralmente surge em redes sociais e também afeta negativamente esquemas de gerenciamento de confiança em VANETs. Um novo esquema de votação foi proposto onde cada veículo tem peso diferente na votação de acordo com a distância do evento, com preferência para veículos mais próximos aos eventos. Uma questão aberta citada em [Huang, 2014] é o atraso nas transmissões que afeta a tomada de decisões, tal questão é tratada neste trabalho com atribuição de graus de confiança aos diferentes usuários da rede vDTN.

O modelo TRIP (*Trust and Reputation Infrastructure-based Proposal*) foi proposto em [Marmol, 2012] para decidir quando aceitar ou não um aviso de tráfego proveniente de outro veículo por meio de avaliação da confiança do emitente da mensagem. Os autores propõem que a infraestrutura de segurança seja capaz de tomar decisões rápidas para lidar com a topologia em constante mudança e de comutação rápida de vizinhos; caso contrário, a comunicação torna-se muito ineficiente. A rede também seria resiliente a ameaças de segurança e privacidade, como nós maliciosos que tentam dirigir a reputação de um nó para baixo confiável. Finalmente, a segurança também é independente de padrões de mobilidade, mantendo a precisão em todos os cenários de tráfego possível. Este trabalho

aborda aspectos de confiança e reputação para evitar conluio sem utilização de infraestrutura nas vias como se baseia o TRIP; o modelo proposto trata ainda autenticação e DTN para lidar com a alta mobilidade dos usuários.

Em [Raya, 2007], os autores apresentam uma arquitetura de segurança e descrevem algumas das principais decisões de projeto ainda a serem feitas, que tem mais do que meras implicações técnicas. A preocupação com a privacidade dos usuários inclui o potencial de o monitoramento do trânsito resultar em taxas de cobrança aos motoristas. Segundo os autores, a segurança em redes veiculares é um desafio crucial e a confiança é um elemento chave nesse aspecto, devido ao grande número de nós independentes envolvidos e presença de fatores humanos na rede que aumentam a tendência de mau comportamento. Neste trabalho é utilizado o conhecimento prévio entre os usuários para estabelecer confiança, que assim escolhem com quem compartilham informações e atribuem reputação a eles.

O modelo de confiança HIT para redes *ad hoc* [Velloso, 2008] simula as relações humanas de confiança e baseia-se no aprendizado dos nós. A abordagem do modelo difere de outros trabalhos preocupados apenas com aspectos convencionais de segurança da rede, como a detecção de nós maliciosos, entre outros. O principal objetivo foi proporcionar aos nós de uma rede *ad hoc* uma maneira de avaliar e manter uma opinião sobre seus vizinhos, que servirá de base para a interação e a tomada de decisões entre eles. Assim, proporcionar um ambiente confiável não é um dos objetivos, mas sim capacitar os nós a reconhecer o ambiente ao qual pertencem. Este trabalho também propõe graus de confiança baseados nas experiências anteriores e na contribuição dos nós da rede veicular DTN, diferente das redes *ad hoc* que dependem de um caminho entre origem e destino, nesse caso vizinhos.

Seguindo o modelo humano, [Velloso, 2010] constrói uma relação de confiança entre os nós de uma rede *ad hoc*. A confiança é baseada em experiências individuais anteriores e nas recomendações dos outros, que permite aos nós trocar recomendações sobre os seus vizinhos. A proposta não requer divulgação das informações a confiança de toda a rede, o nó só precisa manter e trocar informações de confiança sobre nós dentro do alcance do rádio. A maturidade de relacionamento é apresentada como conceito para melhorar a eficiência do modelo de confiança proposto. Este trabalho também propõe um modelo de confiança com propagação sobre usuários confiáveis para a rede social do usuário, assim os relacionamentos previamente existentes entre usuários agregam maturidade ao modelo.

SG-PKM [Nogueira, 2011] é uma infraestrutura de chave pública de sobrevivência para redes *ad hoc* sem fio, que utiliza grupos com base em relacionamentos dos usuários para aumentar a capacidade de sobrevivência na presença de diferentes tipos de ataques,

como *Sybil* e a falta de cooperação. SG-PKM consiste de pequenos grupos chamados iniciadores, que são compostos de nós cujos usuários têm uma relação de amigo entre eles. Os grupos são essenciais para ligação de um novo nó ao sistema, emissão de certificados e renovação de chaves. Nós em um grupo emitem certificados de chaves públicas reciprocamente entre eles. SG-PKM trabalha com dois tipos de certificados: certificados de nó vinculam chaves públicas do usuário com suas identidades; e certificados de grupo vinculam as chaves públicas do grupo com a identificação do grupo. Certificados de nós são assinados com a chave privada do grupo que participam e certificados de grupo são assinados com a chave privada de outros grupos. As relações de amizade propagadas neste trabalho por meio de certificados em redes sociais não utilizam grupos, o que possibilita a certificação entre dois usuários mesmo sem conexão entre origem e destino (Seção 3.3).

A proposta de autenticação [Fernandes, 2008] prevê uma autoridade certificadora distribuída baseada em cadeias de confiança, que registra os endereços dos nós da rede *ad hoc*, associando a cada endereço uma chave pública, e emite certificados. A segurança baseia-se em testemunhas, que são nós escolhidos por meio de funções hash para monitorar um determinado nó. Considera-se a entidade autenticadora distribuída como disponível em todos os momentos, para permitir o provimento de todos os serviços de uma autoridade certificadora ao longo do funcionamento da rede, tais como o registro de novos usuários, a emissão e a revogação de certificados; no entanto essa entidade pode não estar disponível.

PGP-like [Capkun, 2003] é uma das iniciativas de gerenciamento de chaves para redes *ad hoc,* que lida com o problema de gerenciamento de chave pública e propõe uma infraestrutura de gerenciamento totalmente distribuído auto-organizado de chave pública. PGP-like baseia-se na funcionalidade de PGP (*Pretty Good Privacy*) [Zimmerman, 1995] e cada nó é responsável por criar as suas chaves públicas e privadas. Ao contrário do PGP, onde os certificados são armazenados principalmente em repositórios de certificados centralizados, os certificados no PGP-like são armazenados, distribuídos e gerenciados pelos nós de uma maneira totalmente auto-organizado. Neste trabalho, a autenticação de chaves também é realizada por cadeias de certificados de chave pública, porém considera tolerância a interrupções e falta de conexão entre usuários que diferencia de redes *ad hoc*.

RS4VANETs [Fernandes, 2015] foi proposto para analisar a confiança dos veículos em VANETs infraestruturadas, onde a lista de reputação é propagada pelas RSUs (*roadside units*) para os veículos. Cada veículo recebe as últimas experiências passadas quando o veículo está muito perto do local de um evento, usando-as para calcular a reputação direta. Calcula-se também a reputação agregada (indireta) no RS4VANETs, com

base em informações de terceiros para calcular a reputação de veículos desconhecidos. Como se baseia em redes veiculares infraestruturadas, esse mecanismo de reputação não funcionaria em vDTN. Este trabalho propaga a reputação atribuída apenas por usuários confiáveis, de modo que a reputação indireta tem um grau de confiança que não depende de usuários desconhecidos, que poderiam atribuir reputação a outro usuário desconhecido.

A maioria das propostas para redes veiculares trata de problemas específicos, como a autenticação e a privacidade dos nós da rede. Em [Paula, 2010] foi proposto um mecanismo de reputação para redes veiculares considerando tolerância a atrasos e desconexões, mas assume que todos os veículos são certificados. Nesse mecanismo denominado RMDTV (*Reputation Mechanism for Delay Tolerant Vehicular Networks*), os membros da rede qualificam outros membros responsáveis pelo envio de informações corretas. A comparação do RMDTV com este trabalho será apresentada na Seção 7.

Em um protocolo baseado em reputação para buracos negros contrastantes em DTN [Dini, 2012], cada nó mantém localmente a reputação de nós encaminhada em contatos, para aprender gradualmente a identificar aqueles que têm a mais alta reputação. Assim como existem algumas propostas de arquiteturas de segurança DTN mais genéricas [Papadimitratos, 2008], que dependem de outras soluções de criptografia. Este trabalho se diferencia ao propor um modelo de confiança que utiliza certificação em redes sociais para atender os requisitos de segurança das redes veiculares tolerantes a interrupções.

A proposta de [Xu, 2011] toma vantagem da confiança entre os usuários na vida real para formar redes sociais baseadas na confiança, bem como possibilitar criptografia e assim gerar um novo tipo de sistemas complexos. Os autores introduziram e analisaram a ideia de explorar redes sociais baseadas na confiança para a proteção distribuída de dados sensíveis, especialmente chaves criptográficas. A exploração é focada no caso de confiança da vida real, ou seja, que cada usuário saiba quantos amigos humanos tem na vida real. Segundo os autores, muitas questões interessantes foram deixadas em aberto, como ao estender o esquema para acomodar relações de confiança da vida virtual, por exemplo, pessoas que nunca se encontraram, será necessário tomar cuidado especial para lidar com o ataque *Sybil*. Este trabalho inclui outras propostas que independem de relações virtuais.

Um módulo de confiança utilizando técnicas de teoria dos jogos foi apresentado por [Raya, 2010], com dois tipos de jogos em redes *ad hoc*: um entre o grupo de bons nós e o grupo de nós adversários, e outro entre os nós do mesmo tipo. A cada nó é atribuído benefício se ele se comporta bem e uma punição, se ele se comporta mal. Nós observando mau comportamentos podem votar ou abster-se de votar. Este trabalho também utiliza

reputação com o compartilhamento de opiniões propagado na rede social do usuário, que na rede DTN pode incluir usuários sem conexão naquele momento e sem uso de grupos.

Um modelo de confiança é apresentado em [Minhas, 2010] com introdução de dois novos elementos no modelo proposto: distinguem relatos diretos e indiretos que são compartilhados; empregam como recurso uma penalidade a relatos enganosos, para promover a honestidade. Os autores apresentam um *framework* para o compartilhamento de informações segundo o modelo de confiança em várias dimensões, para ajudar os motoristas na tomada de decisões em VANETs. A mobilidade ou mudanças na topologia da rede veicular DTN podem atrapalhar esse compartilhamento. Assim, neste trabalho são abordados tais aspectos de confiança e reputação propagados em redes sociais.

A arquitetura e modelos para redes sociais móveis, onde usuários com *smartphones* obtem informações desejadas de vizinhos, são apresentados em [Liang, 2014] com desafios e soluções de segurança infraestruturadas. Os autores fornecem desafios de pesquisa promissores ao considerar que a comunidade social implica relações de confiança nessas redes. Quando dois usuários participam de uma comunidade social, cada um tem a sensação de que o outro é mais confiável, e as opiniões compartilhadas são mais confiáveis [Liang, 2014]. O compartilhamento de informações de modo confiável é abordado neste trabalho em redes sociais sem a necessidade de infraestrutura ou utilizar Internet, que podem não estar disponíveis.

Considerando inadequada a utilização de uma PKI centralizada em redes DTN, [Djamaludin, 2013] propõe estabelecer confiança com sistemas distribuídos como o *Pretty Good Privacy* (PGP) [Zimmermann, 1995]. A proposta utiliza um modelo de distribuição de chaves baseado no princípio da Teia de Confiança (*Web of Trust*), empregando uma influência simples dos amigos em comum para estabelecer a confiança inicial em DTN autônomas. Há ainda referência a mecanismos de reputação como trabalhos futuros, o que é abordado neste trabalho que utiliza a interação dos usuários para definição dos amigos.

Em [Rivas, 2011], foram discutidos o uso da Infraestrutura de Chave Pública (PKI) e certificados de revogação, privacidade de localização, anonimato e assinaturas de grupo para VANETs. Os autores compararam várias propostas para identificar e expulsar nós com mau comportamento ou falhas. A utilização de PKI ainda tem várias questões em aberto, como revogação de nós (e tamanho da lista) e privacidade. Propõe-se empregar chave pública e certificados neste trabalho de forma distribuída em redes vDTN.

No mecanismo DMV (*Detection of Malicious Vehicles*) [Daeinabi, 2013], cada veículo é monitorado por vizinhos confiáveis da VANET para isolar nós maliciosos que

rejeitam ou duplicam pacotes recebidos dos nós considerados honestos. Cada agrupamento possui um líder para um conjunto de veículos e representa uma Autoridade Certificadora (CA), uma terceira parte confiável que gerencia as identidades, as chaves criptográficas e as credenciais dos veículos dentro de sua região. Como os grupos que são dinâmicos em vDTN, este trabalho propõe um mecanismo baseado nas escolhas do usuário.

DMV é um sistema para monitorar nós maliciosos de forma a isolá-los dos nós considerados honestos com duas listas para cada veículo: lista branca e lista negra [Daeinabi, 2013]. Um nó é considerado malicioso quando caso seu valor de desconfiança está superior a um *threshold* mínimo. Quando isto ocorre, esse veículo é retirado da lista branca e é acrescentado na lista negra. Uma Autoridade Certificadora (AC) transmite periodicamente essas listas para os veículos da rede, ou seja, são centralizadas as informações consultadas para o cálculo da reputação desse sistema e armazenadas em um servidor. Como a revogação deveria ser distribuída, este trabalho propõe descentralizar para que os usuários gerenciem e armazenem suas listas de usuários confiáveis.

Sistemas veiculares cientes de contexto são abordados em [Wan, 2014], com análise de dois componentes cruciais de serviço: redes sociais veiculares e segurança veicular ciente de contexto. Segundo os autores, com o crescimento das redes sociais veiculares, o contexto será incorporado em vários serviços de segurança, tais como controle de acesso, criptografia e autenticação; o que ocorrerá de diferentes maneiras, como completando ou substituindo atributos de usuário. No *framework* proposto, a unidade de gerenciamento de confiança avaliaria a confiança de cada veículo [Wan, 2014]. Esses componentes cruciais são abordados de forma integrada e totalmente distribuída neste trabalho.

Foram abordados aspectos de redes veiculares e o futuro da Internet móvel em [Gerla, 2011], que identifica o papel da infraestrutura urbana no apoio a aplicações veiculares emergentes. Quanto à segurança, duas tendências são apontadas: a necessidade de uma Autoridade Certificadora (CA) exigiria conexão eficiente a servidores de Internet; ao mesmo tempo, para lidar com proteção a ataques em situações quando os nós estão desconectados da Internet, ou será muito demorado para consultar o CA quando houver Internet, ou os usuários móveis organizam-se em comunidades para utilizar as regras de maioria e/ou eleger CAs móveis para resolver questões de segurança. Este trabalho propõe formas de viabilizar essa certificação mesmo sem conexão com a Internet ao utilizar DTN.

Aspectos de segurança em redes veiculares orientadas a serviço são apresentados em [Zhu, 2009]; uma série de requisitos de segurança tem de ser satisfeitos: autenticação, confidencialidade, privacidade e faturamento. Um protocolo de troca de chaves [Li, 2008]

manipula a disponibilidade de certos recursos, garantindo que a sessão vai realmente ser estabelecida. Para preservar a privacidade, tem-se adotado a técnica de pseudônimos baseados no tempo, e no caso da anonimicidade a alternativa é uso de assinaturas de grupo [Zhu, 2013]. Neste trabalho são adotados mecanismos baseados em reputação entre amigos para estimular o encaminhamento de informações nessas redes veiculares, de forma que os usuários escolhem com quem compartilharão seus dados.

Uma rede social móvel emergente orientada a multimídia [Zhang, 2014] ajuda os usuários a receber serviços de multimídia, não só de suas comunidades sociais *online*, mas também de seus vizinhos; são investigadas as questões de segurança e privacidade de serviços multimídia que dificultam o crescimento desses serviços. Segundo os autores, o maior desafio de confiança é como construir relações de confiança entre os usuários móveis e fornecer conteúdos confiáveis a eles, aspectos tratados neste trabalho com comunicação entre usuários previamente conhecidos em redes vDTN.

4.2. Redes sociais veiculares

O uso de conceitos *"Small World"* para criar redes *mesh* sem fio foi proposto em [Verma, 2011]. Em [Guidoni, 2012] é proposta a aplicação de conceitos *"Small World"* no projeto de topologias para redes de sensores sem fio heterogêneas. Em [Liu, 2012], que cita várias leis universais de redes sociais que ocorrem em redes veiculares, são abordados os encontros entre veículos como relacionamentos sociais e redes veiculares como grafos sociais para explorar as propriedades de rede social, seus experimentos mostram a ocorrência do fenômeno "*Small World*".

As rotinas dos motoristas foram objeto de estudo de mobilidade sob uma perspectiva social em [Cunha, 2013] para investigar quanto efetivo é explorar interações sociais em VANETs. Uma análise social de *traces* reais com cálculo de métricas sociais é apresentada em [Cunha, 2014], demonstrando que *traces* de redes veiculares possuem comportamento "*Small World"*. O problema da divulgação dos dados em sistemas veiculares sociais foi abordado em [Maaroufi, 2014], com questões que desafiam o propósito de um novo campo de pesquisa crescente de VSNs (*Vehicular Social Networks*), apresentando uma estratégia social *on-line* para os veículos que transitam em pelotões.

Os limites assintóticos de desempenho em redes veiculares de proximidade social foram investigados em [Lu, 2014], ou seja, capacidade de transferência e atraso médio de

pacotes entre veículos deslocando-se em uma região de mobilidade restrita em torno de um ponto social (*spot*) específico, que transmitem através de um fluxo único (*unicast)* para um veículo de destino que está associado ao mesmo ponto social. Neste trabalho tais métricas são tratadas por redes DTN em mensagens para as redes sociais de cada veículo.

Uma rede social de veículos para permitir comunicações sociais e interações entre usuários na estrada durante suas viagens foi proposta em [Luan, 2015]. Motivado pela conexão limitada a conteúdos e serviços de Internet, seu objetivo essencial é incentivar os usuários distribuídos na estrada a contribuir espontaneamente com informações, de modo a proporcionar troca de mensagens oportunas e localizadas entre si por meio de comunicação de baixo custo entre veículos. Para evitar que essas comunicações sejam frequentemente interrompidas pela mobilidade diversificada dos veículos e conexões intermitentes, o que irritaria os usuários, foi adotado um mecanismo pró-ativo de estimativa do tempo de conexão entre os pares de veículos, e recomendando veículos com conexões relativamente duradouras e estáveis para as comunicações sociais. Segundo [Luan, 2015], os usuários estranhos uns aos outros ficam relutantes em divulgar informações pessoais a terceiros. Tais questões foram tratadas sobre outras perspectivas com redes DTN neste trabalho.

Em [Wu, 2015] foram investigadas redes sociais móveis oportunísticas como um novo paradigma de comunicação, explorando encontros oportunísticos entre dispositivos carregados por humanos e redes sociais móveis para disseminação de conteúdo colaborativo. Os autores propõem aplicações de redes oportunísticas estritamente direcionadas a redes sociais no contexto de redes veiculares, considerando mobilidade real e interações sociais de usuários e discutindo questões de segurança para proteger a identidade do usuário e privacidade da localização. Este trabalho propõe alternativas à afirmação de [Wu, 2015] que a maior parte dos mecanismos de autenticação usualmente requer alto custo de criptografia com premissa de uma autoridade centralizadora.

Um sistema confiável de avaliação de serviços foi proposto em [Liang, 2013] para permitir que os usuários compartilhem comentários de serviços em redes sociais móveis orientadas a serviços. Cada provedor de serviços mantém de forma independente um sistema particular, que coleta e armazena comentários dos usuários sobre seus serviços sem necessidade de qualquer terceira autoridade confiável. Os comentários são então disponibilizados para os usuários interessados na tomada de decisões sobre o serviço.

Os deslocamentos diários dos motoristas são altamente previsíveis e regulares, fornecendo uma grande oportunidade para formar comunidades móveis virtuais com nós fisicamente presentes na mesma localização [Smaldone, 2008]. *RoadSpeak* conecta

usuários veiculares de forma distribuída por meio da infraestrutura de Internet para formar grupos de bate-papo de voz com base em suas localizações e interesses. Usuários de um mesmo grupo são capazes de se comunicar na estrada por meio de mensagens de bate-papo de voz. Este trabalho forma redes sociais veiculares independentes da localização.

Em [Cutillo, 2009], *Safebook* explora as relações de confiança entre os usuários para facilitar o compartilhamento de conteúdo em uma rede social descentralizada, sugerindo uma nova abordagem para resolver problemas de segurança e privacidade com ênfase especial sobre a privacidade dos usuários com relação ao fornecedor da aplicação para defesa contra intrusos ou usuários mal-intencionados, já que muitos conteúdos entregues são de estranhos em vez de amigos sociais. Os aspectos estudados pelos autores para redes sociais *online* fazem parte da proposta deste trabalho para redes sociais veiculares.

Drive and share [Lequerica, 2010] é uma aplicação social veicular instalada nos telefones celulares dos usuários a bordo de veículos. Usando conexões ubíquas de redes celulares, o aplicativo auxilia motoristas e passageiros para troca de informações baseadas na localização na estrada, como informações sobre o tráfego e entretenimento social. Redes sociais em cenários veiculares também são abordadas neste trabalho para compartilhamento de informações entre usuários confiáveis.

4.3. Redes DTN e infraestrutura

Um método foi proposto em [Jiang, 2009] para construir "*Small Worlds*" em redes sem fio usando *data mules*, como empregados em redes DTN. Os dados são enviados entre os nós da rede que não tem comunicação sem fio diretamente, os *data mules* imitam atalhos em "*Small World*". De forma semelhante, este trabalho utiliza redes sociais para prover segurança em redes DTN veiculares.

Segundo [Bhutta, 2014], DTN exige a definição de novos protocolos de segurança e gerenciamento de chaves, pois protocolos tradicionais de segurança fim-a-fim não funcionam com DTN. Para este problema, foi proposto um esquema de transporte de chaves para transportar a chave simétrica gerada em um nó DTN para outro nó comunicar de forma segura usando criptografia de chave pública e assinaturas de *proxy*. Projetado de acordo com a arquitetura DTN, o esquema visa garantir a autenticação e a confidencialidade na comunicação de forma alternativa como proposto neste trabalho.

Ao abordar redes DTN espaciais, [Zhou, 2014] evita gastar grande quantidade de energia e tempo de atraso com uma comunicação confiável fim-a-fim que dificilmente estará disponível entre os usuários e o centro de gerenciamento de chaves. Para tanto, é proposto de um esquema autonômico de gerenciamento de chave em grupos para DTN com uso de uma árvore de chaves lógicas. No esquema proposto, cada nó legítimo tem a mesma capacidade de modificar a chave pública de encriptação com sua chave de decodificação que o centro de gerenciamento de chaves. Este trabalho também propõe uma alternativa para a rede DTN não depender de uma autoridade centralizadora.

Segundo [Lv, 2014], a especificação de redes DTN deixa o gerenciamento de chaves como um problema em aberto, para garantir a autenticidade, integridade e confidencialidade dos pacotes. Ao abordar a questão de estabelecimento de chaves, os autores propõem um modelo de topologia em evolução do tempo e criptografia de dois canais para projetar um protocolo de troca de chaves não-interativo. Assim, um nó programa quando e para quem ele envia a sua chave pública. O esquema permite entre nós DTN a troca de suas chaves públicas ou informações de status de revogação, o que também é tratado neste trabalho com uma alternativa ao gerenciamento de chaves.

Um gerenciamento de confiança dinâmico para DTN e sua aplicação para roteamento seguro são mostrados em [Chen, 2014] para lidar com nós egoístas e mal-intencionados. Foram abordadas a determinação e aplicação dos melhores parâmetros operacionais em tempo de execução em resposta às mudanças das condições da rede de forma dinâmica para minimizar o viés confiança e para maximizar o desempenho do aplicativo de roteamento. Em [Trifunovic, 2010] é abordada a avaliação se um usuário é genuíno com intenções honestas, propondo duas abordagens complementares para o estabelecimento de confiança social: a confiança social explícita e implícita. A confiança é abordada neste trabalho utilizando redes sociais para prover segurança em redes veiculares DTN.

Segundo [Hui, 2008], é possível detectar propriedades características de um agrupamento social de forma descentralizada a partir de um conjunto diversificado de vestígios do mundo real, e aplicar tais características nas decisões de encaminhamento de pacotes em DTN. Os autores propõem um algoritmo social de encaminhamento (BUBBLE) para redes oportunísticas, que melhora significativamente a eficiência de encaminhamento de acordo com os resultados. No entanto, questões de segurança e preservação de privacidade não foram discutidas no BUBBLE. Este trabalho utiliza relações de amizade em redes sociais para prover segurança em redes DTN veiculares.

Um protocolo para encaminhamento de pacotes preservando a privacidade (SPRING) foi proposto em [Lu, 2010] para DTNs veiculares. Com base na implantação de infraestrutura com base social, o protocolo objetiva melhorar a confiabilidade nas comunicações V2V e V2I, também a preservação da privacidade em encaminhamento de pacotes. Contudo, o foco dos autores é a melhor eficiência em termos da taxa de entrega em redes vDTN, utilizando grau de interseções sociais para implantar infraestrutura nas vias. Este trabalho utiliza redes sociais para encaminhamento e análise de confiança das mensagens V2V em vDTN.

Uma melhor eficiência na comunicação em redes veiculares é alcançada sacrificando a segurança e vice-versa, mas VANETs não são inicializadas sem ambas. Assim, [Raya, 2006] propõe um conjunto de mecanismos para reconciliar esses dois requisitos contraditórios, usando agregação de mensagens e comunicação em grupos. Uma heurística probabilística foi proposta em [Silva, 2014] para projetar a infraestrutura fixa necessária para disseminação de informações em redes veiculares (V2I), o que diminui o custo de implementação dessa infraestrutura nas rodovias.

Com a utilização de redes veiculares heterogêneas, a segurança da rede se torna um ponto delicado, uma vez que cada tecnologia de rede é mais vulnerável a determinados ataques [Zou, 2010]. Os autores investigam os efeitos adversos de ataques à taxa de transferência de canal e taxa de entrega, propondo uma abordagem para detectar as mensagens de controle fabricadas para fazer falsas alegações de reserva de canal. Com a ajuda das informações de vizinhança de dois saltos, a técnica permite a detecção de interferência e permite ao nó alvo enviar uma mensagem, que instrui nós vizinhos a ignorar a mensagem de controle fabricada. Este trabalho trata a característica heterogênea da rede partindo da confiança que existe entre os usuários para definir aspectos de segurança. O mecanismo proposto neste trabalho é uma alternativa para troca de chaves em redes veiculares por meio da rede social.

Um sistema centralizado de reputação para redes veiculares foi proposto em [Li, 2012] para avaliar a confiança da mensagem recebida de acordo com a reputação do veículo gerador da mensagem. O sistema proposto tem problemas de falhas devido ao uso de servidores em locais como postos de combustíveis e semáforos para armazenar a reputação dos veículos, o que inclui a coleta de relato de experiências para reputação e a propagação desta reputação na rede. Este trabalho propõe mecanismos distribuídos independentes da existência de infraestrutura ou servidores com uso de redes DTN.

Em [Pereira, 2012] foram abordadas as redes veiculares DTN (vDTN), desde aspectos da tolerância a interrupções até discussão de desafios de pesquisa, como a falta de um método tolerante a atraso para o gerenciamento de chaves. Entre os projetos descritos por esses autores, apenas o *KioskNet* [Guo, 2007] trata questões de segurança, utilizando infraestrutura de chave pública (PKI) para assinar e criptografar dados transmitidos. Neste trabalho é proposto um mecanismo alternativo ao gerenciamento de chaves em vDTN.

O modelo de segurança para a arquitetura DTN difere das redes tradicionais, pois o conjunto de participantes inclui os próprios roteadores [Fall, 2003]. A maior parte das técnicas de segurança envolve a autenticação mútua e a troca de dados restrita entre dois usuários da rede, deixando o restante da rede sem participação nesse processo. Várias das propostas de segurança existentes requerem numerosas trocas de informações entre partes e envolvimento de um terceiro elemento confiável, ou requerem que sejam trocadas credenciais de autenticação relativamente grandes antes de se iniciar a comunicação [Seth, 2005].

Soluções originais da comunidade de pesquisa de redes tolerantes a atrasos e desconexões incluem o uso da encriptação baseada na identidade (IBC – *Identity-Based Cryptography*) [Seth, 2005] [Kate, 2007], que permite aos nós receber informação criptografada com seu identificador público. A aplicabilidade da IBC em redes DTN foi analisada em [Asokan, 2007], concluindo que IBC não tem nenhuma vantagem significativa sobre a criptografia tradicional para autenticação e integridade, mas permite melhores formas de prestação de confidencialidade. Em geral, soluções de redes móveis *ad hoc* vêm sendo alteradas para adaptação a redes DTN e existem pesquisas de segurança distribuída, como o uso de autoridades certificadoras distribuídas [Burgess, 2007]. Segundo os autores, há várias razões para evitar esquemas de autenticação para DTNs, pois tais mecanismos implicam registro administrativo e distribuição de chave à frente de implantação; uma autoridade administrativa comum seria de difícil controle.

Um modelo para gerenciamento de segurança no cenário de redes de emergência foi proposto em [Oliveira, 2010], considerando aspectos das redes DTN e a integração de redes de sensores sem fio (RSSF), com uso do gerenciamento de segurança proposto em [Oliveira, 2008] e suas definições para os sensores. Este trabalho propõe um modelo de confiança para redes DTN veiculares independente de outras soluções de criptografia como controle de acesso ou gerenciamento de chaves.

Para utilizar redes veiculares DTN, é necessário haver alternativa que torne viável a autenticação. Entre as propostas relativas à segurança em redes DTN, em [Symington,

2011] foram apresentadas algumas ideias preliminares sobre a distribuição e gerenciamento de chaves para DTN, mas percebe-se que tais questões ainda estão em aberto. Tais propostas não foram reconhecidas como soluções definitivas ou dependem da existência de alternativas para gerenciamento de chaves, como apresentado neste trabalho.

Um dos desafios relativos à segurança em redes DTN é estabelecer o contexto inicial seguro, sendo irreal assumir que PKI esteja sempre presente e globalmente disponível, portanto um problema aberto nessas redes [Jia, 2012]. Assim, foi proposto um modelo dígrafo virtual dinâmico para estudo da distribuição de chaves públicas [Jia, 2012], estendendo a teoria dos grafos e baseando-se na criptografia em dois canais para redes oportunísticas (*pockets* DTN). Este trabalho também utiliza conceitos de grafos "*Small World*" para possibilitar a criptografia com certificados e chaves públicas em redes vDTN.

4.4. Taxonomia

As propostas estudadas neste trabalho foram categorizadas de acordo com a abordagem de seus autores. Foram adotados como critérios o uso de redes DTN, aspectos de redes sociais, mecanismos relacionados à segurança: confiança, reputação ou autenticação. Esse último critério inclui soluções relacionadas ao gerenciamento de chaves, problema abordado neste trabalho como desafio em redes veiculares DTN. O modelo de confiança proposto nesta tese utiliza redes sociais para prover confiança, reputação e autenticação, sendo a certificação SNVC uma alternativa ao gerenciamento de chaves tradicional.

Como observa-se na Tabela 4.1, iniciativas existentes para redes veiculares são direcionadas para um ou outro cenário, muitas vezes restringindo o acesso ou sem considerar tolerância a interrupções. Tanto quanto sabemos, não existe na literatura alguma proposta para segurança em redes veiculares que viabilize a participação de todos os veículos com mecanismos de segurança, considerando as restrições de recursos dessas redes como a conectividade intermitente.

Tabela 4.1. Comparativo de propostas em relação aos temas abordados.

Proposta - Autor	Redes DTN	Redes sociais	Confiança	Reputação	Autenticação
SNVC 2016	X	X	X	X	X
[Djamaludin, 2013]	X	X			X
[Jia, 2012]	X	X			X
[Lu, 2010]	X	X	X		
[Hui, 2008]	X	X			
[Cunha, 2014]	X	X			
[Jiang, 2009]	X	X			
[Wu, 2015]	X	X			
[Lu, 2014]	X	X			
[Chen, 2014]	X		X		
[Oliveira, 2010]	X		X		
[Trifunovic, 2010]	X		X		
[Dini, 2012]	X			X	
[Paula, 2010]	X			X	
[Symington, 2011]	X				X
[Bhutta, 2014]	X				X
[Zhou, 2014]	X				X
[Lv, 2014]	X				X
[Burgess, 2007]	X				X
[Seth, 2005]	X				X
[Kate, 2007]	X				X
[Pereira, 2012]	X				X
[Guo, 2007]	X				X
[Raya, 2010]				X	
[Li, 2012]				X	
[Marmol, 2012]			X	X	
[Fernandes, 2015]			X	X	
[Velloso, 2010]			X	X	
[Minhas, 2010]			X		
[Fernandes, 2008]			X		X
[Karagiannis, 2011]			X		X
[Gerla, 2011]					X
[Raya, 2006]					X
[Zhu, 2013]					X
[Zou, 2010]					X
[Rivas, 2011]					X
[Daeinabi, 2013]		X			X
[Nogueira, 2011]		X	X		X
[Cutillo, 2009]		X	X		X
[Huang, 2014]		X	X	X	
[Liang, 2013]		X	X	X	
[Xu, 2011]		X	X		
[Liang, 2014]		X	X		
[Wan, 2014]		X	X		
[Maaroufi, 2014]		X	X		
[Malhotra, 2014]		X	X		
[Zhang, 2014]		X	X		
[Luan, 2015]		X	X		
[Lequerica, 2010]		X			
[Smaldone, 2008]		X			
[Liu, 2012]		X			
[Guidoni, 2012]		X			

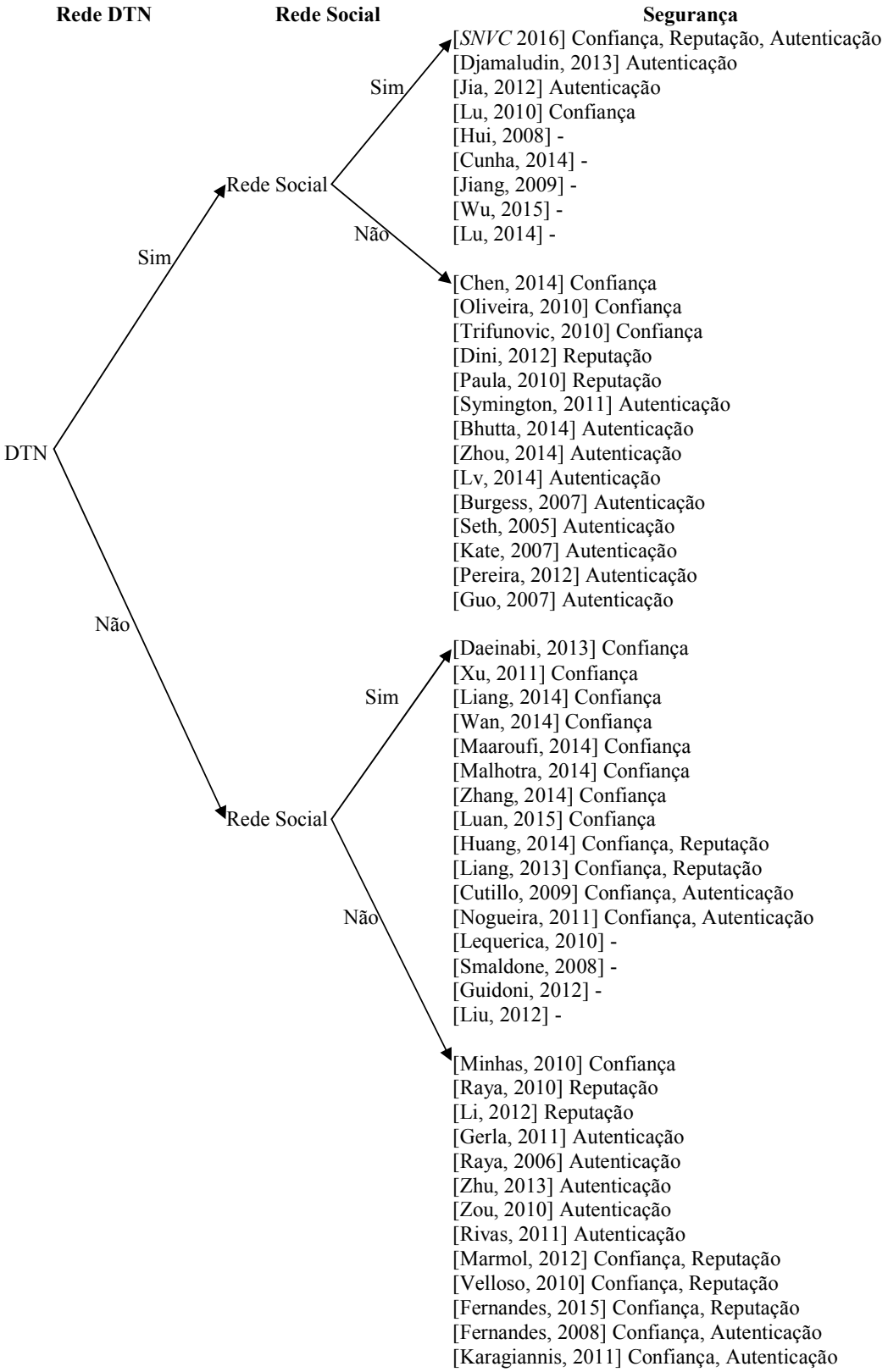

Figura 4.1. Taxonomia de propostas em relação aos temas abordados.

A Figura 4.1 mostra de forma gráfica a categorização das propostas relacionadas a este trabalho segundo os critérios: redes DTN, redes sociais e segurança. No aspecto de segurança são listados os temas abordados: Confiança, Reputação ou Autenticação; quando for o caso, já que há propostas sem relação com segurança. Percebe-se que o modelo de confiança proposto neste trabalho, representado pelo SNVC, é o único que atua em todos os critérios abordados de segurança, assim como utiliza redes sociais e DTN.

4.5. Conclusão

Neste capítulo, foi possível identificar a abordagem de outros autores em relação às redes veiculares ou DTN, particularmente no que se refere à segurança dessas redes. Em geral, os trabalhos relacionados abordam especificamente um tipo de rede, assumindo premissas fortes sobre a conectividade em redes veiculares ou sem considerar desafios específicos da comunicação entre veículos nas pesquisas sobre DTN. No aspecto de segurança, há necessidade de maior pesquisa em ambos cenários citados.

A comparação entre as propostas analisadas na revisão da literatura possibilitou definir categorias para cada proposta, desde o tipo de rede abordado se redes sociais ou DTN, aos critérios de segurança utilizados. Na taxonomia foi mostrado que este trabalho aborda ao mesmo tempo redes sociais e DTN, sendo o único trabalho a abordar aspectos de autenticação, confiança e reputação em redes veiculares tolerantes a interrupções.

Capítulo 5

Redes Sociais para Confiança

Este capítulo apresenta o modelo de confiança proposto neste trabalho, que utiliza redes sociais para segurança em redes veiculares tolerantes a interrupções. O objetivo é prover comunicação para a troca de informações confiáveis entre os veículos e as entidades responsáveis por organizar o trânsito. Entre diversas aplicações dessas redes, será possível fornecer informações confiáveis ao usuário e seus sistemas de navegação, para que ele possa decidir qual a melhor rota a tomar para cumprir determinado trajeto.

5.1. Modelo de rede veicular

No modelo deste trabalho, as redes veiculares são compostas de veículos e dispositivos dos próprios usuários, portanto possibilitam uma variedade muito grande de configurações. Cada nó da rede corresponde a um par veículo-motorista. A ampla diversidade de possíveis nós participantes, que vão desde nós sensores a robustos servidores de controle de tráfego, a mobilidade e as aplicações impedem que o problema de provimento de segurança seja abordado de forma única nas soluções existentes na literatura. Dessa forma, é necessário especificar o escopo da solução de segurança proposta para redes veiculares:

- **Heterogeneidade:** redes veiculares são heterogêneas em *hardware* para estimular todos os usuários a participarem por meio da utilização de seus próprios *notebooks*, *palmtops*, *tablets e smartphones,* com várias tecnologias de rede para comunicação entre esses nós [Macedo, 2012];
- **Ausência de hierarquia:** não existe hierarquia entre os nós das redes veiculares tratadas neste trabalho, caracterizados como um par veículo-motorista;
- **Ausência de infraestrutura:** neste trabalho não é considerada a existência de infraestrutura nas vias, o que difere a rede veicular de redes tradicionais. A possível

utilização de servidores de controle de tráfego e o eventual acesso de nós às redes metropolitanas não garantem requisitos de segurança em tempo real [Zhou, 2014]. As redes devem ser tolerantes a interrupções com conectividade parcial, portanto, não contam com acesso constante a servidores e autoridades certificadoras;

- **Conectividade parcial:** alguns dos nós da rede estão conectados entre si, enquanto os demais não tem conectividade. As conexões são perdidas a qualquer momento, devido a falhas, deslocamentos, conexão limitada das operadoras ou outros tipos de eventos. Nós começam a participar ou deixam a rede dinamicamente, de forma que a rede necessita da arquitetura DTN para comunicação;
- **Comunicação *ad hoc:*** a comunicação ocorre de modo *ad hoc* (V2V). Como a rede não conta com infraestrutura física para conectividade, a comunicação precisa de tolerância a interrupções para entrega de mensagens de nós desconectados. Comunicação *ad hoc* entre os veículos é fundamental, pois neste trabalho utiliza-se a arquitetura de rede DTN. Dessa forma, não é necessário haver conexão constante com equipamentos de uma rede metropolitana sem fio (WMAN), em estradas longe das cidades, disponibilizadas pelo poder público ou via redes celulares 3G/4G;
- **Interação direta:** a interação entre os usuários ocorre de forma direta, como *Bluetooth*. A tecnologia a ser empregada quando os carros tiverem sistemas embarcados compatíveis é o padrão IEEE 802.11p, implementação de rede sem fio para ambientes veiculares WAVE (*Wireless Access in Vehicular Environments*) [IEEE 2013][Jiang, 2008], que padroniza a comunicação em redes veiculares;
- **Topologia desconhecida:** não existe conhecimento prévio de topologia de roteamento e localização de vizinhos, devido à distribuição aleatória dos nós;
- **Escalabilidade:** a rede é de larga escala, considerando redes veiculares com centenas ou milhares de nós.

Formalmente, o modelo de rede considera um conjunto $\mathcal{N}$ de nós usuários e o grafo de topologia da rede $G = (V_t, E_t)$, onde $V_t \subseteq \mathcal{N}$ é o conjunto de vértices e E_t é o conjunto de arestas que representam os contatos oportunísticos entre pares de nós no tempo *t.* Um contato ocorre quando dois nós da rede estão dentro do raio de transmissão um do outro.

Sejam $\mathcal{P}_t \subseteq \mathcal{N}$ os nós sem conexão a quaisquer nós da rede num determinado tempo *t*, conforme o modelo de rede definido, tal que $\mathcal{P}_t \cup V_t = \mathcal{N}$. A comunicação vDTN ocorre quando mensagens de um nó $p \in \mathcal{P}_t$ são encaminhadas para $n \in V_t$, por meio de um

contato e_t = (n, p) em um posterior instante de tempo *t'*. Os nós sem contatos no instante *t,* p ∈ $\mathcal{P}_t$ terão contato com outros nós num instante posterior *t'*, quando se torna p ∈ $\mathcal{V}_{t'}$.

5.2. Modelo de relacionamentos

As redes veiculares abordadas neste trabalho utilizam um modelo de relacionamentos proposto para estabelecer comunicação segura entre os usuários. As entidades que integram a rede social proposta neste trabalho são:

- **Usuário:** representa um nó da rede veicular que tem relacionamentos de amizade com outros usuários;
- **Amigo:** usuário que possui um relacionamento direto de prévia confiança com um determinado usuário;
- **Amigo de amigo:** usuário que possui relacionamento indireto com um determinado usuário por meio de um amigo em comum;
- **Amigo por reputação:** usuário que possui relacionamento indireto com outro usuário por meio de reputações enviadas para rede social, logo é considerado confiável por reputação;
- **Usuário beneficiado:** amigo ou amigo de amigo que foi favorecido por uma informação útil repassada por outro usuário da sua rede social e deseja recompensá-lo com atribuição de reputação.

O modelo de relacionamento que existe entre os usuários da rede é uma importante definição diretamente ligada ao modelo de confiança proposto para troca de mensagens por meio da rede social. Como utilizam a comunicação sem fio entre veículos, as redes veiculares são modeladas como redes sociais, no campo de pesquisa das redes complexas [Almiron, 2010]. A utilização de técnicas de análise de redes sociais para transmitir dados em redes *ad hoc* tolerantes a desconexões foi proposta em [Daly, 2007].

Uma análise social de *traces* reais com cálculo de métricas sociais [Cunha, 2014] demonstrou que *traces* de redes veiculares possuem comportamento *"Small World"*. As características do modelo *Small World* são utilizadas em [Guidoni, 2012] para criar uma rede de sensores sem fio para melhorar a comunicação de dados, já que o grafo dessa rede tende a apresentar maior agrupamento que redes aleatórias e características de alto caminho médio.

Tabela 5.1. Modelo de relacionamento entre usuários no grafo da rede social.

Usuários	Amigos	Amigos de Amigos	Amigo por reputação
Relacionamento no grafo	Direto	Indireto por um nó	Indireto por dois nós

Formalmente, o modelo de confiança proposto neste trabalho considera um conjunto $\mathcal{N}$ de usuários e o grafo da rede social $C^{\bullet} = (\mathcal{N}, C_t)$, onde $\mathcal{N}$ é o conjunto de vértices e C_t é o conjunto de arestas que representam relacionamentos entre pares de usuários no tempo t. Sejam $A_n \subseteq \mathcal{N}$ os amigos do usuário n por meio da rede social e $\Gamma_n \subseteq \mathcal{N}$ são os amigos desses amigos que representam o conjunto de amigos dos amigos desse usuário n. Segundo o modelo, tais usuários ainda podem atribuir reputação a outros usuários de suas redes sociais (Seção 5.3.4). Seja $\Omega_n \subseteq \mathcal{N}$ os usuários que tem histórico de reputação salvo por n, que representa um princípio de reconhecimento público do comportamento do usuário, pois a reputação é utilizada para recompensar usuários que se comportam bem na divulgação e repasse de informações verdadeiras.

A Tabela 5.1 mostra o modelo de relacionamentos possíveis entre os usuários em sua rede social. Dois usuários que se relacionam como amigos possuem relacionamento direto entre eles no grafo da rede social, representado por uma aresta entre esses usuários da rede. Para que um desses usuários possua relacionamento com um amigo do outro usuário, depende-se então de duas arestas relacionando os usuários envolvidos indiretamente. No caso da reputação, somente haverá caminho entre dois usuários se um amigo em comum atribuir reputação positiva para alguma informação útil enviada por um desses usuários.

5.3. Modelo de confiança

A proposta deste trabalho é estabelecer a confiança por meio de uma rede social, utilizando a troca direta de material criptográfico em relacionamentos cotidianos para certificação (*SNVC – Social Networks for Vehicular Certification)*, como encontro com amigos ou ajuda a outros usuários. Um amigo é um usuário de prévia confiança que assina o certificado do outro usuário. Por meio de amigos em comum na rede social, é possível receber informações úteis e atribuir reputação ao usuário que enviou a mensagem. É necessário propor novos mecanismos para que os veículos consigam atender aos requisitos de segurança discutidos na Seção 3.1, pois no modelo de rede deste trabalho as redes

veiculares não contam com acesso a servidores de autenticação e os usuários da rede não possuem certificados oficiais.

O modelo de confiança considera um conjunto $\mathcal{N}$ de usuários e o grafo $C^{\cdot} = (\mathcal{N}, C_t)$, onde $\mathcal{N}$ é o conjunto de vértices e C_t é o conjunto de arestas que representam os relacionamentos entre pares de usuários no tempo t. Sejam $T_n \subseteq \mathcal{N}$ todos os usuários confiáveis, capazes de se comunicar com o usuário n por meio da rede social proposta, ou seja, a união dos conjuntos definidos no modelo de relacionamento da seção anterior (seção 5.2): $T_n = A_n \cup \Gamma_n \cup \Omega_n$.

Sejam dois usuários A e B que já se conhecem e se encontram, eles adicionam-se como amigos na rede social para tornarem-se mutuamente confiáveis de acordo com o modelo de confiança proposto. Nesse caso, cada usuário adiciona o outro em sua lista de amigos por meio de emparelhamento de seus equipamentos. Em seguida, o nó A recebe a lista de amigos de B, o que lhe possibilita trocar mensagens confiáveis com todos os amigos de B. Da mesma forma, o nó B reconhece como confiáveis também as mensagens dos amigos de A.

A Figura 5.1 ilustra a situação de A e B se adicionarem como amigos, tal operação será detalhada na Seção 5.3.2. Se B já possuía como amigos os usuários C e D, então esses usuários também participarão do novo relacionamento ao reconhecerem A como amigo de amigo para a troca de mensagens segundo o modelo de confiança. Na Tabela 5.2 são mostradas as consequências de A e B tornarem-se amigos, o que aumenta o número de usuários confiáveis também por incluir os amigos do amigo.

Os parâmetros para distinguir mensagens que são confiáveis são estabelecidos sobre algum tipo de informação comum que os usuários da rede compartilhem. Mesmo que essa distinção se baseasse em algum tipo de prioridade, como preferência por mensagens de ônibus ou entidades responsáveis pelo trânsito, ainda seria necessário o conhecimento prévio de material criptográfico para garantir o reconhecimento desses veículos. O modelo de confiança propõe que o reconhecimento de usuários utilize material criptográfico trocado de forma direta entre motoristas previamente conhecidos.

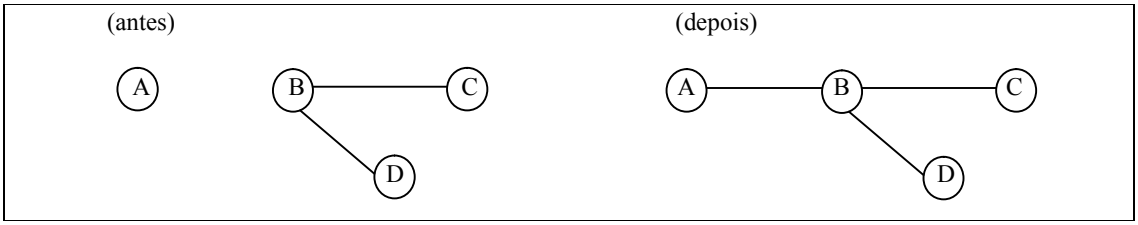

Figura 5.1. Relacionamentos de A antes e depois de adicionar B como amigo.

Tabela 5.2. Lista de amigos e usuários confiáveis após A adicionar B.

Usuário	Amigos Antes	Amigos Depois	Usuários Confiáveis
A	-	B	B, C, D
B	C, D	A, C, D	A, C, D

Propõe-se que os usuários das redes veiculares determinem seus amigos com base no conhecimento prévio e contato direto com o outro usuário, reconhecendo-se mutuamente como usuários confiáveis. O material criptográfico (certificados e chaves) é armazenado por ambos e divulgado em mensagem assinada aos outros usuários de suas redes sociais, para que se estabeleça um grau de confiança. Baseado nos relacionamentos entre os usuários é proposto um mecanismo de reputação, pelo qual os usuários beneficiados podem atribuir uma assinatura para o certificado de quem o ajudou, incluindo uma pontuação positiva pela informação útil repassada (Seção 5.3.4). Essa pontuação é utilizada para determinar se um usuário é confiável e mesmo reconhecer usuários que enviam informações falsas ou imprecisas para a rede, possibilitando um histórico de reputação.

Na Figura 5.2 observa-se a alteração no grafo proposto pelo modelo de confiança quando o usuário A adiciona como amigo o usuário E. Os usuários então reconhecem a lista de amigos do amigo adicionado como usuários confiáveis, sendo amigos de amigo. Após A se tornar amigo de E, essa situação permite a A trocar mensagens com o nó F como amigo de amigo, mas só é possível A comunicar com o nó G se ele possuir reputação positiva.

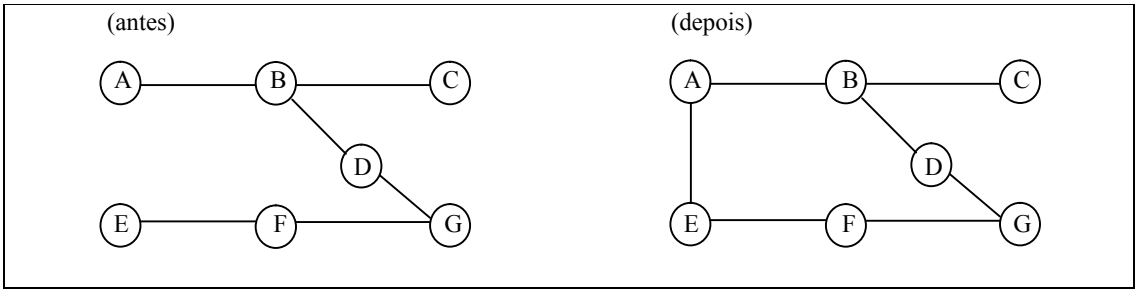

Figura 5.2. Relacionamentos antes e depois de A adicionar o usuário E como amigo.

Tabela 5.3. Lista de amigos e usuários confiáveis após A adicionar E.

Usuário	Usuários confiáveis antes	Amigos antes	Amigos depois	Usuários confiáveis depois
A	B, C, D	B	B, E	B, C, D, E, F; G (reputação)
B	A, C, D, G	A, C, D	A, C, D	A, C, D, E, G
E	F, G	F	A, F	A, B, F, G
F	E, G, D	E, G	E, G	A, E, G, D

A Tabela 5.3 mostra os amigos e usuários confiáveis depois que A adiciona E como amigo, o que aumenta as possibilidades de troca de mensagens confiáveis para esses usuários e também para seus amigos B e F. Ainda é possível por meio do mecanismo de reputação que o usuário F atribua reputação positiva ao usuário G, por exemplo. Essa reputação seria reconhecida pelo usuário A, então as mensagens do usuário G seriam consideradas confiáveis pelo nó A devido à reputação positiva atribuída pelo nó F ou outros usuários que façam parte da rede social de A nesse caso.

Uma mensagem de reputação é validada com as chaves que o usuário armazena dos seus amigos e dos amigos de amigos. Ao vincular a reputação à rede social do usuário, previne-se contra o conluio de usuários mal-intencionados que criam reputações mútuas. Tal medida também previne o mecanismo de reputação de usuários falsos como ataques *sybil*. Somente assinaturas de reputação atribuídas por amigos ou amigos de amigos do usuário são consideradas para analisar a confiança das mensagens.

A assinatura de reputação é mais uma possibilidade de reconhecimento do usuário, ao indicar que alguém da rede social deu crédito à sua informação e isso lhe foi útil. No grafo proposto pelo modelo de confiança $C' = (N, E_t)$, se um usuário com reputação positiva deseja se comunicar com outro usuário, esse último é capaz de validar a reputação por meio do certificado se for amigo ou amigo de amigo do usuário beneficiado que atribuiu reputação. Então há caminho no grafo entre esse usuário e o amigo por reputação.

Assim, o modelo de confiança propõe utilizar redes sociais para aumentar as possibilidades de comunicação confiável em redes veiculares. Os usuários compartilham chaves de amigos reconhecidos como confiáveis, sendo que o maior número de amigos possibilitará mais caminhos no grafo da rede social. Os certificados são assinados por amigos em contato direto ou por meio de reputação atribuída por usuários beneficiados por alguma mensagem. Existem diferentes caminhos entre dois usuários confiáveis, mas sempre há um amigo em cada caminho no grafo da rede social proposta.

5.3.1. Graus de confiança

O modelo de confiança proposto neste trabalho está diretamente ligado ao modelo de relacionamento apresentado na Tabela 5.1 (Seção 5.2), por meio dos graus de confiança atribuídos aos possíveis relacionamentos entre os usuários da rede social. O grau de confiança é uma medida da confiança de um usuário em relação ao outro.

Tabela 5.4. Graus de confiança segundo modelo proposto.

Grau de Confiança	**ALTO**	**MÉDIO**	**BAIXO**	**NULO**
Usuário	Amigo	Amigo de Amigos	Amigo por Reputação	Sem relacionamento

Os graus de confiança apresentados na Tabela 5.4 são utilizados pela certificação SNVC (Seção 5.3.3) e aplicações que farão a interação entre usuários. Assim, ao ouvir uma mensagem recebida de sua rede social, o usuário saberá o grau de confiança associado e considerará essa informação para tomar alguma decisão sobre sua rota. Veículos que recebem informações de outros usuários precisam saber a confiança de quem gerou aquela informação [Karagiannis, 2011].

A escolha de usuários confiáveis define quanto os demais usuários da rede confiam no emissor de uma mensagem. Um amigo do usuário tem o grau de confiança "ALTO", que representa o maior grau de confiança possível. Os amigos de um amigo da rede social do usuário têm grau de confiança "MÉDIO", portanto abaixo dos amigos desse usuário. Para os amigos de amigos, o usuário sempre guarda a informação do amigo que os relaciona indiretamente.

Um mecanismo de reputação indica a confiança ao permitir os usuários beneficiados por informações de sua rede social que manifestem aos demais qual usuário merece ser distinguido por sua reputação. Para isso, o modelo atribui a esse amigo por reputação um grau de confiança "BAIXO", o que possibilita que ele troque mensagens com a rede social do usuário beneficiado pela informação. Por incluir as reputações atribuídas por amigos de amigos, esse grau de confiança relaciona os usuários indiretamente por dois nós, que são o amigo em comum e o usuário beneficiado. Dois usuários que não tiverem nenhum desses relacionamentos não se comunicarão por terem grau de confiança "NULO".

Os graus de confiança foram definidos de forma hierárquica para atribuir maior confiança aos amigos que possuem contato direto com o usuário. Os amigos de amigos são confiáveis com grau de confiança menor, pois representa a relação de confiança com algum amigo desse usuário com quem teve contato direto. Dessa forma é possível armazenar o amigo em comum que os relaciona indiretamente no grafo da rede social. Para tal controle considera-se apenas um amigo em comum, o que evita problemas de armazenamento e restringe a confiança a contatos diretos dos amigos do usuário.

O modelo *"Small World"* indica que quase todos os elementos do grafo são alcançáveis com até seis saltos [Gakenheimer, 1999]. Em geral, redes sociais são

aplicações do conceito *"Small World"*, usado para modelagem de redes sem fio [Verma, 2011]. Em [Liu, 2012], que cita várias leis universais de redes sociais que ocorrem em redes veiculares, são abordados os encontros entre veículos como relacionamentos sociais e redes veiculares como grafos sociais para explorar as propriedades de rede social, seus experimentos mostram a ocorrência do fenômeno *"Small World"*. Uma análise social de *traces* reais com cálculo de métricas sociais [Cunha, 2014] demonstrou que *traces* de redes veiculares possuem comportamento *"Small World"*.

O modelo de confiança deste trabalho permite o relacionamento até três saltos no caso da reputação, pois é necessário rastrear as informações recebidas relacionando os amigos ou amigo de amigos que possibilitam a comunicação confiável por um caminho no grafo. Assim, os amigos tem relacionamento direto de um salto que representa conhecimento prévio entre eles. Os amigos desses amigos são considerados confiáveis por relacionamento indireto de dois saltos (Seção 5.2), sendo que houve contato direto entre dois dos três usuários envolvidos nesse caminho no grafo. Se fosse considerado outro nível de amigos de amigos dos amigos, seria inviável rastrear o amigo do usuário como intermediário de confiança de outro usuário com quem não teve contato direto.

A reputação apresenta o grau de confiança mais baixo, pois não representa necessariamente contatos diretos entre usuários. É possível atribuir reputação a qualquer informação recebida pela rede social, seja de um amigo ou amigo de amigo. Quando um usuário beneficiado por uma informação útil propaga para sua rede social a reputação que atribui, os amigos de seus amigos tornam-se amigos por reputação do usuário que originou a informação. Trata-se de um relacionamento direcional (Seção 5.3.4) e indireto por três saltos (Seção 5.2) entre usuários que não possuem um amigo em comum, porém houve colaboração com sua rede social que gerou atribuição de reputação.

5.3.2. Visão geral

O modelo de confiança proposto se baseia inicialmente nos contatos diretos entre dois usuários num mesmo ambiente que emparelham seus equipamentos, por exemplo, veículos parados lado a lado ou em um estacionamento. A troca de material criptográfico de forma direta possibilitará a comunicação quando não houver conectividade na rede vDTN. É possível estabelecer uma senha temporária [Xu, 2011] para garantir que não existe um intruso nessa comunicação por entrega direta, que será digitada por ambos os usuários nesse contato inicial.

Esse contato direto entre amigos, que são pessoas que se conhecem e garantem sua identidade, possibilita que um assine o certificado do outro. Assinar o certificado de modo recíproco e compartilhar suas chaves públicas possibilita uma rede de relacionamento social, então todos os usuários que possuam amigos em comum conseguem validar seus certificados usando as chaves desse amigo. Isto ocorre porque os usuários armazenam a chave pública do amigo quando assinam o certificado do amigo e a utilizam para verificar a assinatura que o amigo emitiu para outros certificados.

Os usuários validam todos os certificados assinados com as chaves de seus amigos ou amigos de amigos, pois armazenam as chaves públicas de usuários da sua rede social. Supondo que os usuários conhecem centenas de amigos e consequentemente milhares de chaves, aumenta-se a probabilidade de encontrar uma chave em comum com os outros usuários que desejam validar os requisitos de segurança para comunicação confiável.

A título de ilustração, uma centena de amigos envolveria, com os amigos dos amigos, até 10.000 usuários. Mas como sempre existem amigos em comum, esse número tende a cair consideravelmente [Gakenheimer, 1999]. Como descrito na Seção 3.5, são utilizados mecanismos de chave pública curtas de curva elíptica e resumos das chaves de 20 bits permitem localizar chaves em comum. O tamanho das mensagens e certificados é minimizado por não ser necessário enviar as assinaturas de cada certificado. Ao encontrar as chaves em comum da rede social, os certificados são validados.

O funcionamento, baseado no PGP (*Pretty Good Privacy*) [Zimmermann, 1995] [RNP, 2014], ocorre da seguinte forma:

1. O usuário gera um certificado auto-assinado;
2. O certificado é assinado por outros usuários em contatos diretos, tornando-se amigos. A geração das assinaturas dos certificados é iniciada ao aproximar os dispositivos dos usuários, por meio do compartilhamento de uma senha gerada no momento e trocada entre os amigos;
3. O dispositivo de cada usuário armazena por contato direto as assinaturas do amigo adicionado e as chaves públicas de todos os amigos desse amigo. As chaves dos amigos armazenadas são usadas para validar o certificado e as assinaturas desses usuários. Informações de amigos de amigos armazenadas incluirão também o certificado do amigo que os relaciona indiretamente no grafo da rede social (Seção 5.2), pois é possível ter mais de um amigo em comum entre os usuários.
4. O certificado do amigo é compartilhado com os amigos do usuário para que atualizem as listas de amigos de amigos. Os amigos dos amigos reconhecem o

certificado, assinado por um amigo, e passam a trocar mensagens confiáveis, compartilhando a convicção do amigo de que é um usuário confiável.

5. A comunicação entre usuários se inicia pela pesquisa de um amigo ou amigo de amigos. O vínculo de um amigo em comum permite confirmar a assinatura do remetente da mensagem por meio das chaves públicas armazenadas. Se houver restrições de memória do dispositivo do usuário ou caso seja rompido o vínculo com algum usuário, é possível removê-lo da lista de amigos.
6. Caso não esteja disponível alguma assinatura da rede social do usuário, é possível buscar uma assinatura conhecida originária de reputação. Essa assinatura será armazenada se o usuário beneficiado que a emitiu estiver na rede social do usuário que verifica o certificado. A reputação aumenta as chances de reconhecimento, indicando que alguém da sua rede social foi beneficiado por um usuário e o mesmo foi recompensado com uma assinatura de reputação, tornando-se reconhecido como amigo por reputação.

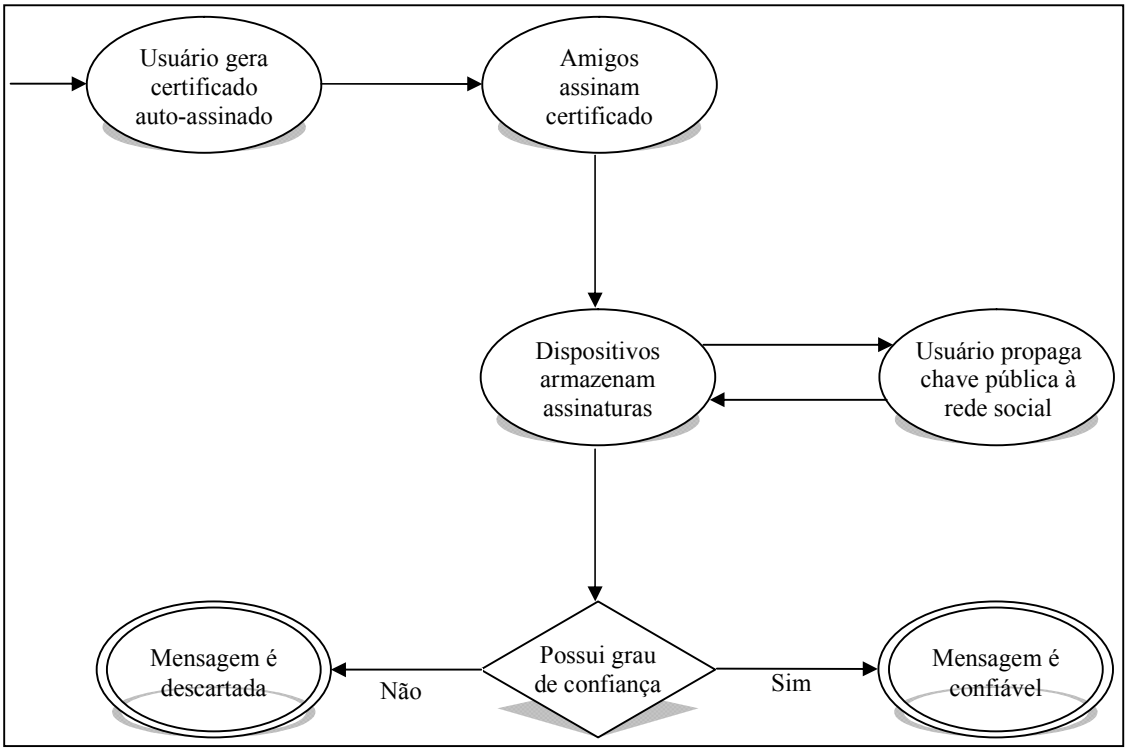

Figura 5.3. Diagrama de participação de usuários.

```
1:  algoritmo principal()
2:    certificado ← geraCertificado()                    // gera certificado auto-assinado do usuário
3:    enquanto (¬Sair)
4:      mensagem ← recebeMensagem()
5:       se mensagem = [T_EncontrouAmigo, amigo] então
6:         adicionarAmigo(amigo)                         // adiciona usuário à lista de amigos como confiável
7:       senão se (mensagem.possuiCertificado() ∧ validarMensagem() ≠ NULO) então
8:         se mensagem = [T_novo, amigo] então           // processa mensagens recebidas da sua rede social
9:           adicionarConhecido(amigo)                   // salva informações de amigo dos amigos
10:        senão se mensagem = [T_remover, amigo] então
11:          removerConhecido(amigo)                     // exclui chave pública de amigo dos amigos
12:        senão se mensagem = [T_bonus, amigo] então
13:          adicionarReputacao(amigo)                   // salva reputação recebida de sua rede social
14:      fim se                                          // caso contrário aplicativo mostrará mensagem ao usuário
15:      se Mensagem = RemoverAmigo então
16:        removerAmigo(amigo)                           // remove usuário da lista de amigos (confiáveis)
17:      senão se Mensagem = Reputacao então
18:        atribuirReputacao(usuario, tipo)              // atribui reputação ao usuário e envia para rede social
19:    fim enquanto                                      // sai da repetição e desliga aplicativo comunicação V2V
```

Figura 5.4. Algoritmo principal.

Na Figura 5.3 são exibidos os eventos que determinam a participação de um usuário na rede social proposta. As mensagens recebidas por esse usuário são validadas por meio das chaves públicas armazenadas no dispositivo do usuário, que são utilizadas diretamente se a mensagem for de sua rede social ou, caso contrário, se alguém de sua rede social gerou uma assinatura de reputação para o emissor da mensagem. Se não houver vínculo algum com os amigos do usuário, a mensagem é descartada por não ser confiável.

Na Figura 5.4 é apresentado o algoritmo principal que determina o funcionamento da rede social proposta e aciona os algoritmos relacionados para: adicionar amigos, remover amigo, validar mensagem, atribuir reputação. As mensagens recebidas pelo usuário são processadas por esse algoritmo para adicionar ou remover chaves públicas de amigos de amigos ou armazenar assinaturas de reputação atribuídas por sua rede social. Da mesma forma, é processada a comunicação com aplicações que utilizam a rede social quando o usuário encontra um amigo.

Na Figura 5.5 são mostradas as situações possíveis em que a mensagem é confiável. No caso de verificação da reputação do remetente de uma mensagem, somente são válidas reputações atribuídas pela rede social do usuário que a recebe, seus amigos ou amigos de

amigos. Dessa forma, a chave pública da assinatura de reputação é reconhecida e as indicações positivas precisam superar em número as indicações negativas.

As assinaturas propostas neste trabalho são validadas de acordo com o certificado e as respectivas assinaturas do usuário que envia as mensagens. A mensagem é definida como confiável com base no grau de confiança de quem a enviou, o que considera também o cálculo da sua reputação. Os graus de confiança utilizados para validação de mensagens recebidas foram apresentados na Seção 5.3.1.

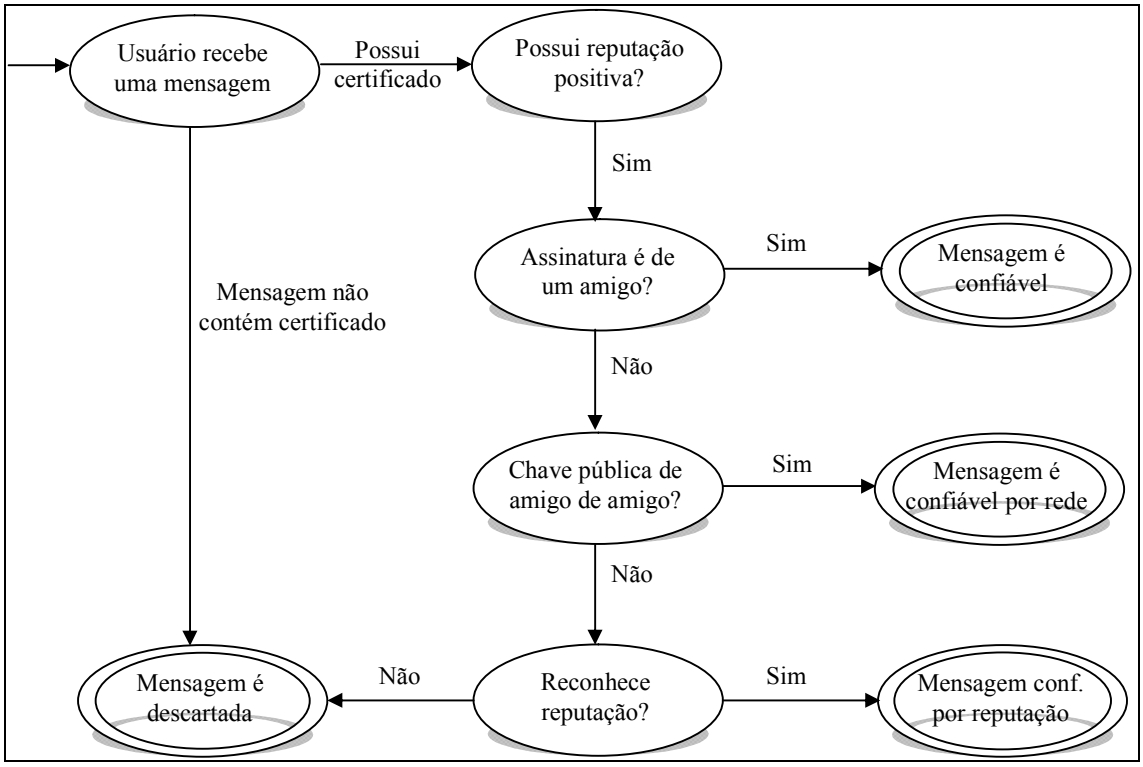

Figura 5.5. Diagrama de reconhecimento de mensagens confiáveis.

```
1:  algoritmo validarMensagem(usuario)                    // obter grau de confiança do remetente da mensagem
2:    GrauConfianca confianca ← NULL;                     // usuários inicialmente são não-confiáveis
3:    se usuario ∈ listaAmigos ∧ calcularReputacao(usuario) ≥ 0 então
4:      confianca = ALTO                                  // reconhece chave pública de amigo
5:    senão se usuario ∈ listaConhecidos ∧ calcularReputacao(usuario) ≥ 0 então
6:      confianca = MEDIO                                 // se usuário for amigo de amigos da sua rede social
7:    senão se calcularReputacao(usuario) ≥ 0 então
8:      confianca = BAIXO                                 // se reputação for positiva, é confiável por reputação
9:    retorna confianca                                   // mensagens de grau de confiança NULO serão descartadas
```

Figura 5.6. Algoritmo para validar mensagens por grau de confiança.

A Figura 5.6 mostra o algoritmo utilizado para validar as mensagens por meio da obtenção do grau de confiança do usuário que a enviou. Inicialmente o grau de confiança é "NULO" e caso o usuário em questão não possua assinaturas válidas para o seu certificado, a mensagem será descartada. As mensagens de amigos são reconhecidas diretamente como confiáveis, com grau de confiança "Alto". Se o grau de confiança do usuário for "Médio" ou "Baixo", a mensagem é considerada confiável e o grau de confiança obtido será informado ao usuário juntamente com a leitura do conteúdo da mensagem.

O algoritmo ainda valida a reputação de um usuário da rede social dentro dos limites aceitos para confiança, o que permite restringir mensagens de usuários com reputação negativa mesmo que sejam amigos ou amigos de amigos. Se um amigo tiver reputação negativa ou um amigo de amigo tiver alguma indicação negativa de reputação, esse usuário não possuirá grau de confiança e suas mensagens serão não confiáveis. Tais limites serão definidos pelas aplicações que utilizem a rede social proposta de acordo com os graus de confiança aceitáveis pela aplicação, que serão informados aos usuários juntamente com as mensagens consideradas confiáveis.

5.3.3. Certificação SNVC

A certificação tradicional baseia seu funcionamento em um modelo de árvore. Propõe-se expandir o modelo para um grafo, em que todos os usuários de rede capazes de se comunicar usando certificação são nós do grafo. Os certificados são validados se existe um caminho entre os dois usuários que querem se comunicar no grafo da rede social. Tal caminho tem tamanho máximo igual a três quando for atribuída reputação a um usuário, ou seja, o caminho inclui o amigo do usuário, amigo do amigo e o amigo por reputação, como descrito na seção 5.3.1. O tamanho máximo é definido porque apenas usuários da rede social terão suas mensagens recebidas e consideradas úteis para atribuição de reputação pelo usuário beneficiado, que será então um amigo ou amigo de amigo.

No modelo PKI convencional, como todos os nós da rede possuem a chave pública do nó raiz, basta que um nó possua uma cadeia de certificação que chegue até uma raiz conhecida para que ele seja validado por outro. Ao considerarmos o grafo da rede social proposto neste trabalho, se existir uma cadeia de certificação que ligue dois nós dessa rede, eles também validarão suas chaves. Ou seja, sob um grafo denso de uma rede social, se forem estabelecidas arestas seguras entre dois nós quaisquer com os amigos e amigos de amigos, será possível validar os respectivos certificados.

O modelo de confiança propõe três tipos de assinaturas emitidas para os certificados dos usuários que os credenciam para garantir a segurança em uma comunicação: assinaturas dos amigos, assinaturas de amigos dos amigos e assinaturas de reputação. A certificação SNVC propaga essas assinaturas com baixo *overhead* já que inicialmente houve a troca direta de material criptográfico. As assinaturas dos amigos são obtidas por contato direto e, por isso, implicam em uma relação próxima de conhecimento. As assinaturas de amigos dos amigos, sempre acompanhadas dos certificados dos respectivos amigos em comum, são obtidas por meio de interações entre usuários que compartilham suas listas de amigos. As assinaturas de reputação representam uma recompensa a usuários que colaboram positivamente com a rede veicular.

A segurança das mensagens na rede veicular proposta neste trabalho depende de ambos: do amigo em comum e do amigo de amigo. Quando um usuário adiciona um novo amigo, ele envia para seus amigos a chave pública do amigo recentemente adicionado. De forma complementar, a assinatura de reputação é validada se o usuário beneficiado fizer parte de sua rede social, caso tenha sido beneficiado pela ação do usuário que se torna amigo por reputação. A certificação SNVC ainda operaria em conjunto com entidades responsáveis pelo trânsito, que atuariam como fontes confiáveis certificadas pela rede, no entanto as limitações da certificação tradicional já foram discutidas na Seção 3.3.

A Figura 5.7 apresenta o algoritmo para um usuário adicionar outro usuário como amigo. De forma recíproca, o novo amigo também adiciona o usuário como amigo e executa o mesmo algoritmo, que verifica se um usuário já está na lista do outro devido ao algoritmo ser utilizado bidirecionalmente. As listas de amigos de cada usuário são enviadas para que o novo amigo reconheça os amigos do usuário como amigos de amigo, que são denominados conhecidos. Para que esses últimos reconheçam o novo amigo, é enviada uma mensagem aos amigos de cada usuário para que eles salvem a chave pública recebida com a mensagem como sendo de um conhecido (amigo de amigo).

```
1:  algoritmo adicionarAmigo(amigo)
2:    se amigo ∉ listaAmigos então
3:      listaAmigos ← listaAmigos ∪ amigo              // adiciona usuário à lista de amigos como confiável
4:      listaConhecidos ← listaConhecidos ∪ amigo.listaAmigos          // conhecidos = amigos de amigos
5:
6:      para cada conhecido em listaAmigos
7:        enviaMensagem([T_novo, amigo], conhecido)      // propaga novo relacionamento aos seus amigos
```

Figura 5.7. Algoritmo de adição de amigos.

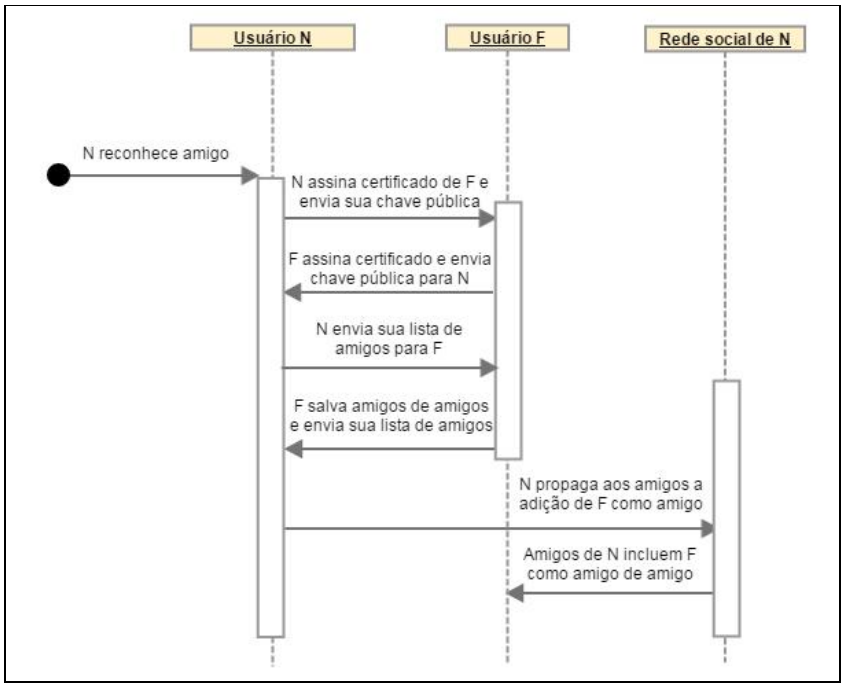

Figura 5.8. Diagrama de eventos da adição de amigos.

A Figura 5.8 mostra a interação entre um usuário N que adiciona um usuário F como amigo para compartilhar as suas chaves públicas. Após tornarem-se amigos, ambos N e F enviam mensagem à sua rede social informando que há um novo usuário confiável. Por isso, os amigos de F passam a reconhecer as mensagens de N como confiáveis, o mesmo para os amigos de N reconhecendo F. Outros amigos de N reconhecem F e assinam seu certificado quando ambos estiverem conectados.

Quando um usuário N adiciona como amigo um usuário F, ele salva as chaves públicas da lista de amigos de F e envia mensagem para seus amigos também incluírem F como nó confiável. Da mesma forma, F salva a lista de amigos desse usuário como amigos de amigos para troca de mensagens confiáveis. Além de F salvar a chave do novo amigo N, ele envia mensagem com a chave desse usuário para seus amigos. Quando algum desses amigos receber uma mensagem de N, então ela é reconhecida como confiável.

A certificação SNVC utiliza algoritmos de criptografia de curvas elípticas e o formato de certificado WAVE descrito na Seção 3.5, que foi definido no padrão IEEE 1609.2 como uma forma compacta de certificado digital [IEEE, 2013]. Contudo, a norma IEEE 1609.2 especifica apenas os formatos e como ocorrem os processamentos para prover segurança criptográfica [Wangham, 2014]. O padrão define, por exemplo, como a chave pública de um usuário é usada para criptografar uma mensagem ou como é realizada a autenticação do usuário. Diferentemente desse padrão, neste trabalho não há um gerente

de segurança e o próprio usuário é responsável pela criação, validação e revogação dos certificados.

5.3.4. Reputação certificada

Um mecanismo de reputação também é usado para confirmar que os usuários estão agindo em benefício da rede social. A reputação tem efeito semelhante às assinaturas dos certificados, diferenciando-se apenas por um indicativo do certificado, que é bonificação positiva quando emitida por usuários beneficiados por informações recebidas de outro usuário. Por exemplo, um usuário que identifica um acidente e manifesta essa informação para a rede social poderá receber uma bonificação de reputação positiva, se sua informação for útil a outro usuário. A assinatura de reputação precisa ser validada com a chave pública do usuário beneficiado e possibilita que a mensagem seja reconhecida como confiável.

Reputações negativas são atribuídas a algum usuário e enviadas para a rede em caso de informações erradas, pois usuários podem ser adversários de outros no intuito de interromper ou escutar a comunicação. O princípio de reputação é uma recompensa para os usuários que se comportam bem na divulgação de informações do trânsito e repassam informações verdadeiras. Os comportamentos detectados como negativos ou egoístas são punidos, restringindo a participação desses usuários na rede social. O conhecimento sobre usuários com esse tipo de comportamento também é compartilhado na rede social por meio da utilização de sistemas baseados em reputação.

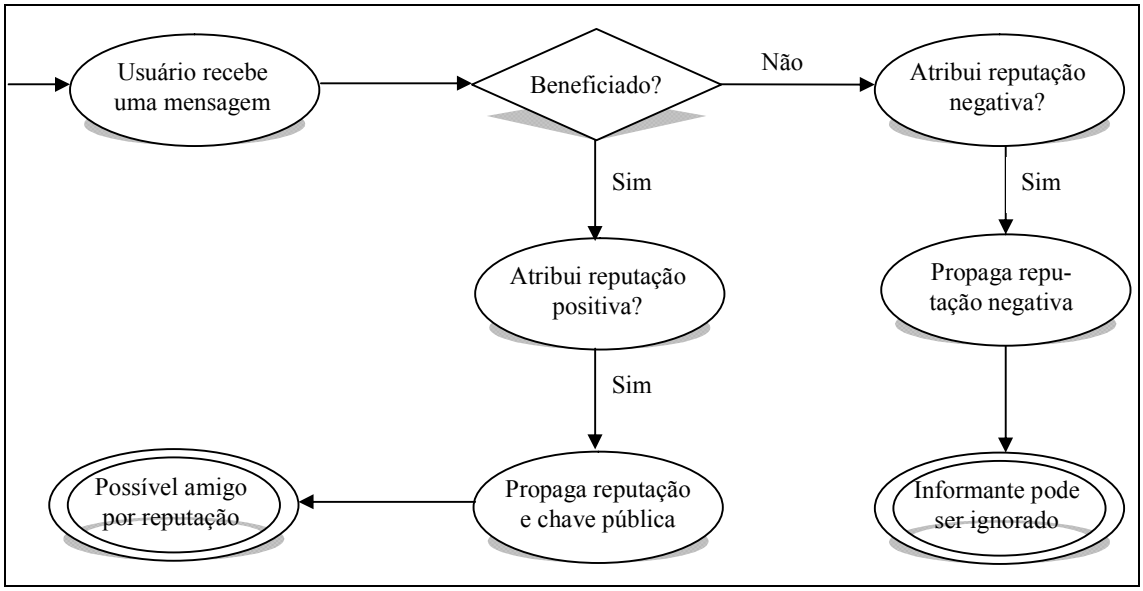

Figura 5.9. Diagrama de participação de usuários no mecanismo de reputação.

```
1:  algoritmo atribuirReputacao(usuario, tipo)
2:    se usuario ∈ listaAmigos ∨ usuario ∈ listaConhecidos então     // usuário é amigo ou amigo de amigos
3:      reputacao ← novaReputacao(usuario, tipo)                    // tipo determina reputação positiva ou negativa
4:      listaReputacao ← listaReputacao ∪ reputacao                 // adiciona à sua lista de amigos por reputação
5:      para cada amigo em listaAmigos                              // usuários armazenarão reputação e chave do usuário
6:        enviaMensagem([T_bonus, reputacao], amigo)                // propaga a reputação atribuída aos seus amigos
7:      para cada conhecido em listaConhecidos
8:        enviaMensagem([T_bonus, reputacao], conhecido)            // propaga a reputação a todos amigos de amigos
9:    fim se
```

Figura 5.10. Algoritmo de atribuição e propagação de bônus de reputação.

Um certificado acumula várias assinaturas indicando sua reputação e é válido se as bonificações positivas de **amigos e amigos de amigos** forem em maior número que reputações negativas. Assim, restringe-se a participação de usuários desconhecidos, que poderiam atribuir reputação a outro usuário desconhecido ou afetar negativamente a reputação de usuários confiáveis por meio de conluio. Entre as propostas do modelo de confiança deste trabalho, inclui-se a utilização do histórico de reputação para armazenar os as reputações propagadas por amigos e amigos de amigos, que atribuem reputação positiva ou negativa a um usuário. Os usuários são confiáveis se possuem um número maior de bonificações positivas em relação a reputações negativas.

A Figura 5.9 mostra a participação de usuários no mecanismo de reputação. A geração de uma informação útil por um usuário da rede social pode agregar assinaturas que facilitem o seu reconhecimento por outros usuários. Os usuários beneficiados atribuem reputação positiva para informações consideradas corretas que, propagada para sua rede social, representa consequência positiva na identificação de usuários confiáveis que se tornam amigos por reputação.

O usuário que recebe a reputação também faz parte da rede social do usuário beneficiado, visto que o recebimento da mensagem e o reconhecimento do seu certificado foram necessários para o usuário avaliar se a informação trouxe benefício. Da mesma forma, o usuário ainda pode atribuir reputação negativa a um usuário que gerou informação incorreta, para que as mensagens desse usuário sejam ignoradas por possuir reputação negativa.

Na Figura 5.10 é observado o algoritmo que permite a atribuição de bônus de reputação a usuários que são recompensados pelo seu comportamento, o que aumenta as possibilidades de comunicação em sua rede social. Para receber o bônus, o usuário faz

parte da rede social do usuário beneficiado, pois foi esse último quem recebeu a informação considerada útil. Um usuário não pode atribuir reputação a si mesmo, pois não faz parte da própria rede social. O usuário beneficiado propaga a reputação à sua rede social, assim ela reconhece a reputação na troca de mensagens futuras, por meio da chave pública armazenada junto com a reputação. Todos os usuários que tiverem acesso à chave pública do usuário beneficiado são capazes de validar a reputação.

Na Figura 5.11 apresenta-se um exemplo de atribuição de bônus de reputação do usuário beneficiado D ao usuário G, o qual se torna amigo por reputação para a rede social de D. A propagação da reputação atribuída por D na sua rede social possibilita a G ser reconhecido como confiável pelos usuários A e C, o que antes não ocorria. A atribuição de reputação é uma operação direcional, que parte do usuário beneficiado para o amigo por reputação. Dessa forma, um amigo de G apenas que não esteja na rede social de D não receberia mensagem sobre tal reputação, então não haveria um caminho para comunicação confiável entre esse usuário e D.

Como mostrado na Figura 5.12, o bônus é assinado com o certificado do usuário N beneficiado pela informação enviada à rede pelo usuário R. Então todos os usuários com acesso à chave pública desse veículo N conseguem validar o bônus, uma vez que é enviada mensagem a amigos e amigos de amigos de N informando sobre o bônus de reputação para que eles também armazenem a chave pública de R. O mesmo processo acontece para publicar o mau comportamento de um usuário. Por exemplo, se há alguma informação errada sobre o tráfego, um usuário atribui uma recomendação negativa para o usuário que enviou a informação. Essa indicação é enviada para todos os usuários que reconhecem o seu certificado, os seus amigos e amigos de amigos.

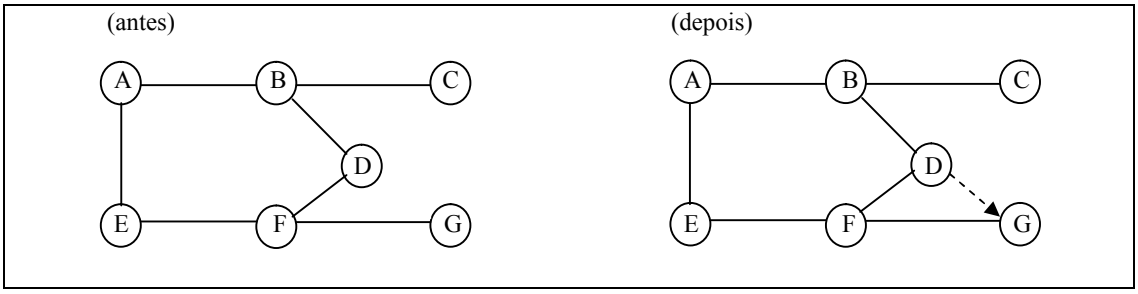

Figura 5.11. Relacionamentos antes e depois de D atribuir bônus de reputação a G.

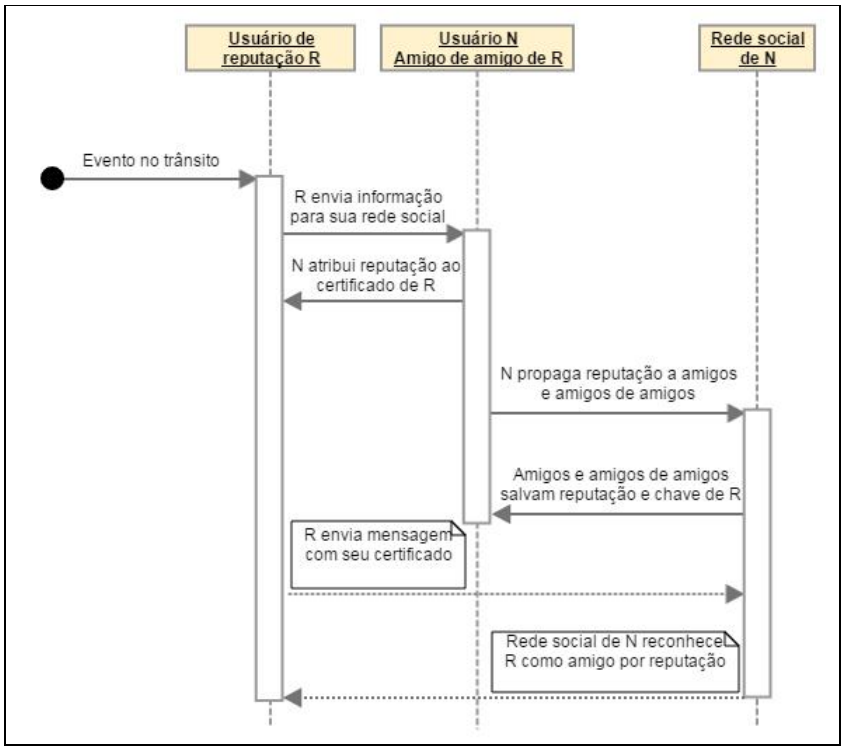

Figura 5.12. Diagrama de eventos da reputação de usuários.

```
1:  algoritmo calcularReputacao(usuario)
2:    reputacao ← 0;                                  // calcula reputação do usuário em questão
3:    se usuario ∈ listaReputacao então               // se existir reputação gravada para esse usuário
4:      para cada bonus em listaReputacao             // lista de reputações armazenadas, se for desse usuário
5:        se bonus.usuario = usuario ∧ bonus.indicacao = true então     // verifica tipo de bônus atribuído
6:          reputacao ← reputacao + 1                 // se há reputação positiva, usuário favoreceu a rede
7:        senão se bonus.usuario = usuario ∧ bonus.indicacao = false então
8:          reputacao ← reputacao - 1                 // se não favoreceu a rede, reputação é decrementada
9:    retorna reputacao                               // se reputação for positiva, usuário será considerado confiável
```

Figura 5.13. Algoritmo de cômputo da reputação.

A Figura 5.13 mostra o algoritmo de cômputo da reputação de um usuário, pontuando as reputações atribuídas e obtendo como resultado o histórico de reputação, prevalecendo as reputações em maior número positivas ou não. São incluídas no cálculo todas as reputações recebidas por meio da rede social do usuário, enviadas por seus amigos ou amigos de amigos. Se o cálculo da reputação resultar positivo, esse usuário é considerado confiável por reputação, ou seja, amigo por reputação.

A reputação ainda é utilizada para validar mensagens de amigos ou amigos de amigos que, mesmo sendo parte da rede social do usuário, podem ter reputação negativa e

suas mensagens serem consideradas não confiáveis. Assim, um *threshold* é definido para amigos ou amigos de amigos serem confiáveis. A confiança em um usuário da rede social diminui caso um amigo obtenha reputação negativa inferior ao limite estabelecido, o mesmo ocorre para amigos de amigos com reputação negativa. Definidos os valores iniciais como máximo para confiança, os limites são representados no grafo da rede social por valores de *threshold* para amigos e amigos de amigos. Tais limites serão determinados mediante avaliação conforme a Seção 6.4.

O vínculo da reputação com a rede social do usuário representa também um incentivo para que os usuários beneficiados atribuam reputação ao usuário que originou a informação considerada útil, assim ele será reconhecido como amigo por reputação. Recompensar um amigo ou amigo de amigo por uma mensagem recebida seria então mais comum que atribuir reputação negativa, caso haja alguma informação errada. Em redes sociais, considera-se mais comum "curtir" (avaliar positivamente) mensagens de amigos do que criticá-los com reações negativas, diferentemente de quando não há vínculo entre usuários e não haveria motivo para um motorista elogiar o outro.

5.3.5. Remoção de amigos

As assinaturas dos certificados dos usuários propostas neste trabalho e as listas de chaves públicas de amigos dos amigos são atualizadas quando um usuário é removido ou adicionado como amigo. As listas de amigos são compartilhadas quando um usuário adiciona outro como amigo, então esse usuário divulga a chave pública do amigo e recebe a lista de amigos do amigo.

A Figura 5.14 mostra o algoritmo para remover um amigo da rede social do usuário. Toda remoção de amigos ocorre de forma bidirecional para estabilidade do relacionamento entre os usuários, o que acontece por meio de mensagem para que o outro usuário também execute o algoritmo. Se algum usuário decide remover um amigo, essa mensagem é assinada com a chave pública do amigo removido, então ele usará sua chave privada para também atualizar suas listas de amigos e amigos de amigos. Ao remover um amigo, o usuário propaga aos seus amigos essa informação para que eles retirem a chave pública do amigo removido de suas listas de amigos de amigos, pois foi removido o caminho entre esses usuários no grafo da rede social.

Quando os caminhos envolvendo o usuário removido no grafo proposto pelo modelo de confiança são atualizados, então arestas entre os amigos removidos deixam de

existir. Toda remoção de amigos do usuário é realizada com a assinatura do usuário para evitar falsas remoções, portanto apenas os usuários que conhecem a chave pública desse usuário executam a operação.

A Figura 5.15 mostra os eventos relacionados à remoção de um amigo, realizada de forma recíproca e propagada aos amigos dos usuários envolvidos para atualização das suas listas de amigos dos amigos. É necessário propagar essa remoção para todos os amigos de ambos os usuários envolvidos para que eles removam a chave pública da lista de amigos dos amigos de cada nó, assim como são excluídas as reputações atribuídas a tal usuário.

```
1:  algoritmo removerAmigo(usuario)
2:    se usuario ∈ listaAmigos então
3:      listaAmigos ← listaAmigos – usuario                    // remove usuário da sua rede social
4:      listaReputacao ← listaReputacao – usuario              // exclui reputações desse usuário
5:      para cada amigo em listaAmigos
6:        enviaMensagem([T_remover, usuario], amigo)           // propaga a remoção aos seus amigos
7:    fim se      // ao receber mensagem de remoção, usuários excluirão chave da lista de amigos de amigos
```

Figura 5.14. Algoritmo para remoção de amigos.

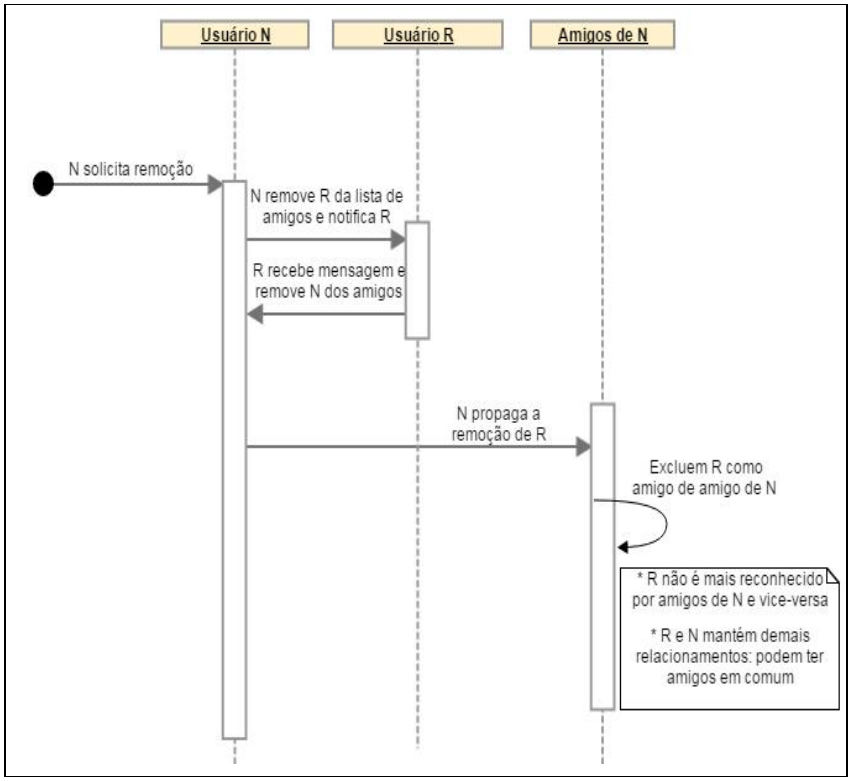

Figura 5.15. Diagrama de eventos da remoção de amigos.

Vale ressaltar que podem existir outros caminhos no grafo da rede social que relacionem os usuários, portanto ao retirar a chave pública do usuário removido da lista de amigos de amigos, é removida apenas a entrada referente ao amigo que comunicou a remoção. Se houver nessa lista outro usuário que indique o usuário removido como amigo, esse último continuará sendo confiável como amigo de amigo. O usuário removido ainda mantém os demais amigos com mesmo grau de confiança, pois as listas de amigos de seus amigos não são afetadas.

Devido às características DTN das redes veiculares, as mensagens são recebidas por usuários com atraso ou até mesmo ocorre uma falha no envio. No caso da remoção de amigos, se houver atraso na mensagem propagada aos amigos para que excluam a chave pública do usuário removido da sua lista de amigos dos amigos, esse usuário ainda é considerado como amigo do amigo ao tentar se comunicar. Se houver outras assinaturas que relacionem o usuário removido ao amigo do amigo que recebe a sua mensagem, ambos comunicam-se como amigos ou por terem outro amigo em comum. Porém, se a única assinatura válida para esse usuário for aquela excluída, a comunicação entre eles ocorre de maneira indevida. Para evitar tal situação, a rede social atualiza as listas de amigos de amigos sempre que usuários se encontrem.

A Figura 5.16 exemplifica a remoção do amigo B pelo usuário D, o que torna as mensagens do usuário A não confiáveis para D. Os usuários atualizam em cada encontro as suas listas de amigos de amigos, visto que as listas de amigos são atualizadas quando o usuário adiciona ou remove um amigo. Se um usuário tem a informação mais recente que B e D não são amigos em relação à informação do usuário A, que ainda contém em sua lista de amigos de amigos o relacionamento entre ambos, ao encontrá-lo o usuário A atualiza sua lista removendo a informação que B é amigo de D.

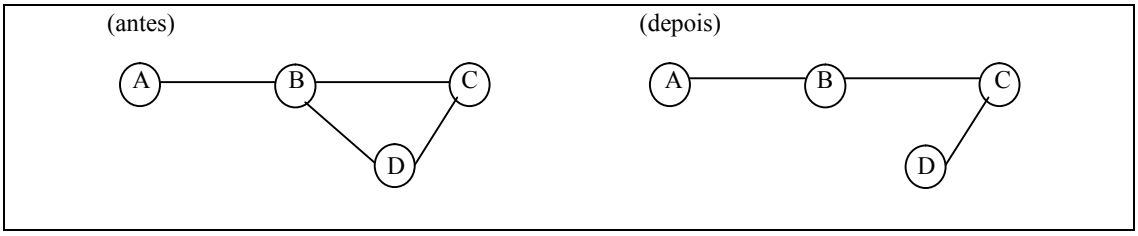

Figura 5.16. Usuário D antes e depois de remover o usuário B como amigo.

5.3.6. Ataques evitados

Mensagens não confiáveis também podem ser geradas intencionalmente [Li, 2012]. Por exemplo, alguns veículos podem gerar e transmitir mensagens falsas de congestionamento rodoviário com a intenção de enganar outros veículos para evitar certas rotas. No caso extremo, a mensagem não confiável pode levar a lesões e até mortes. Por isso, é importante a avaliação da confiança de mensagens geradas pelos veículos.

Em um ambiente amplo, os veículos são assumidos como tendo uma relação de confiança fraca (ou não) com os outros [Li, 2012]. Isso levanta a questão: como os veículos decidem se confiam em uma mensagem? Minimizar os ataques e as consequências de comportamentos maliciosos é muito importante em soluções que necessitam da cooperação e da honestidade dos nós, tais como as aplicações de Alerta de Perigo Local [Fernandes, 2015]. Tais aplicações podem ser muito úteis para prover segurança do trânsito nas rodovias, porém, a confiança nos nós que propagam e difundem os alertas precisa ser avaliada.

Restringir as mensagens a usuários confiáveis evita ataques do tipo supressão usando rede social. A finalidade do ataque de supressão é bloquear um aviso de congestionamento, por exemplo, impedindo veículos de procurar caminhos alternativos, forçando-os a entrar no congestionamento. Como o modelo de confiança proposto propaga as mensagens para a rede social, um intruso não consegue impedir a entrega de cópias da mensagem.

O uso de criptografia evita ataques de negação de serviço e também a análise de tráfego, pois um atacante com acesso à rede poderia interceptar o tráfego de pacotes e coletar dados transmitidos de forma passiva sem conhecimento de chaves. O modelo de confiança proposto reduz o impacto de ataques como *blackhole*, *grayhole* e *wormhole*. Nesse tipo de intrusão, veículos maliciosos se recusam a transmitir mensagens enviadas sobre um acidente e que deveriam ser direcionadas para outros veículos. Eles podem transmitir apenas parte das mensagens ou redirecioná-las para outros pontos da rede para dificultar a sua entrega. A propagação de mensagens por usuários confiáveis evita intrusos na troca de mensagens autenticadas, replicadas aos amigos da rede social o que diminui a incidência dos ataques citados.

A reputação baseada em redes sociais como aqui proposta evita ataques como falsas informações (*bogus*) e conluio. Um intruso ou um usuário legítimo poderia transmitir informação falsa na rede para obter vantagens ou afetar a decisão de outros veículos. Em caso de conluio, um atacante forma alianças com outros nós da rede para atingir um

objetivo comum, como prejudicar a aplicação ou denegrir a reputação de algum usuário. Algumas propostas de reputação [Li, 2012] não previnem contra ataques de conluio.

Uma mensagem é validada por reputação usando as chaves que o usuário armazena de seus amigos e amigos de amigos. Ao vincular a reputação à rede social do usuário, previne-se contra o conluio de usuários mal-intencionados, criado com reputação mútua. Tal ação também previne o mecanismo de reputação de falsos usuários como ataques *Sybil*. Apenas reputação atribuída por amigos ou amigos de amigos do usuário é considerada para analisar a confiança de mensagens.

Ataques do tipo supressão ou *tampering* podem ocorrer mesmo com utilização do modelo de confiança proposto. A replicação de mensagens poderia levar os usuários à exaustão de recursos e também retransmitir mensagens reais da rede, dificultando sua detecção. A violação física dos nós a fim de obter informações e segredos, além de também comprometer o nó, insere códigos maliciosos ou ainda troca partes do *hardware* [Fernandes, 2006]. Segundo os autores, a maioria dos protocolos desenvolvidos para prover segurança falha em ambientes onde é possível ocorrer a violação. Nesse caso, a atribuição de reputação negativa visa evitar que nós violados repitam ataques.

No forjamento de dados de posição do GPS (*GPS spoofing*), o satélite GPS mantém uma tabela com a localização geográfica e a identidade do veículo na rede, mas os atacantes usam um simulador de satélite GPS para gerar sinais mais fortes do que aqueles gerados pelo satélite real de forma a enganar os veículos, introduzindo uma localização falsa [Rawat, 2012]. O modelo de confiança proposto não atua sobre informações relativas aos veículos dos usuários.

Ilusão é uma nova ameaça de segurança em aplicações VANET na qual o atacante engana ou interfere intencionalmente nos sensores do seu próprio veículo para produzir leituras erradas. Como resultado, mensagens de aviso de tráfego incorretas são transmitidas para os nós vizinhos, criando uma condição de ilusão em VANET [Wangham, 2014]. As mensagens geradas por usuários confiáveis serão propagadas e outros usuários podem atribuir reputação negativa para quem enviou essas informações erradas.

5.3.7. Aplicações *versus* privacidade

O escopo deste trabalho delimita-se pelo estudo relativo à confiança para troca de informações por meio de uma rede social entre veículos, para que tomem decisões mais precisas no trânsito. O modelo de confiança proposto permite a troca de mensagens

autenticadas entre amigos sobre suas experiências durante seus deslocamentos. A definição de rotas de trânsito é um exemplo de aplicação, entre outras como gerenciamento de ônibus, otimização de horários de deslocamentos e compartilhamento de veículos.

As aplicações deste trabalho são em geral de gerenciamento e eficiência de tráfego para melhorar o fluxo, a coordenação e a assistência do tráfego, e também, em prover a atualização das informações locais, como mapas e mensagens de relevância delimitadas no espaço ou no tempo. Aplicações de *Infotainment* ainda oferecem, entre outras coisas, informação e entretenimento para o conforto dos motoristas e passageiros.

O funcionamento de uma aplicação com a rede social proposta parte do contato pessoalmente entre dois amigos que pareiam seus dispositivos para assinar seus certificados ao adicionar o amigo. Assim, é possível receber informações desse amigo e dos seus amigos, da mesma forma que poderá enviar mensagens a eles. Para cada informação recebida, o usuário pode atribuir reputação positiva ou negativa para quem enviou a mensagem. A atribuição de reputação também é autenticada e propagada para rede social do usuário beneficiado pela informação útil, assim como no caso de reputação negativa. Para cada mensagem recebida, a aplicação verifica o grau de confiança segundo o modelo proposto para decisão sobre informar ou não ao usuário. Somente mensagens de usuários confiáveis são mostradas pela aplicação com o grau de confiança do usuário que enviou a informação. Em geral, as aplicações devem permitir mensagens de áudio para que os motoristas não sejam distraídos digitando ou lendo mensagens enquanto dirigem.

Como exemplo de aplicação que utilize o modelo de confiança proposto, deve-se oferecer opções aos usuários para enviar áudios com informações para que sua rede social possa ouvir a mensagem de voz acompanhada do seu grau de confiança. A aplicação não deve depender de processamento do usuário para evitar sobrecarga de mensagens e atraso na tomada de decisões. Quando o veículo estiver parado ou num congestionamento, o motorista pode informar num mapa detalhes do evento e situação atual no local onde se encontra. Além disso, o motorista pode atribuir reputação para qualificar informações recebidas e sensores podem enviar mensagens automáticas sobre seu deslocamento.

Suponha um usuário que deseja saber se existem buracos ou desvios na rota até a sua casa. Um posto de combustíveis pode colocar alarmes falsos em uma avenida, para fazer com que os usuários mudem o seu trajeto para direcionar-se ao posto. Com o modelo de confiança proposto, os usuários receberiam a informação do posto apenas se o mesmo fizer parte da rede social e ainda marcariam tal informação como falsa, assim a reputação do posto rapidamente se tornaria negativa.

O modelo de confiança ainda permite aplicações específicas para troca de informações entre taxistas ou motoristas de ônibus, por exemplo. Tanto em aplicações de definição de rotas de trânsito quanto em uma de *Infotainment*, o usuário tende a ter na rede social deste trabalho pessoas que convivem no mesmo ambiente em parte do dia ou deslocam-se para lugares próximos. Os usuários variam de acordo com as aplicações, que podem utilizar o mesmo modelo de confiança deste trabalho. Assim, se uma pessoa mal intencionada enviar um alerta falso de acidente de trânsito mesmo que de um dispositivo roubado, apenas seus amigos irão recebê-lo e poderão remover esse amigo ou atribuir reputação negativa para que esse usuário não seja mais considerado confiável.

As vantagens do uso de redes sociais para prover confiança em redes veiculares incluem os aspectos de autenticação e reputação por meio de certificados. O modelo de confiança integra esses aspectos em graus de confiança obtidos nas interações entre os usuários, o que diferencia as mensagens recebidas pela confiança no usuário que enviou a mensagem. A restrição de mensagens apenas de usuários confiáveis é considerada vantajosa, pois representa maior segurança para tomada de decisões, embora seja necessário que o usuário participe da rede social e adicione amigos para aumentar a probabilidade de ser informado sobre eventos do trânsito.

Como desvantagem do modelo proposto tem-se a anonimicidade: autenticação de usuários e veículos versus a privacidade dos dados. Um usuário quer ter certeza que pode confiar na fonte da informação. Entretanto, ter acesso à identidade do informante pode contradizer os requisitos de privacidade desse usuário [Wangham, 2014]. Com o envio de mensagens autenticadas, o modelo propôs graus de confiança para fomentar as decisões sobre mensagens recebidas. Este trabalho propõe que cada usuário conheça apenas as chaves públicas da sua rede social, pois essa seria o único meio de compartilhamento das chaves entre os usuários.

A privacidade e o anonimato são questões que requerem atenção por parte dos desenvolvedores das diferentes partes de um dispositivo WAVE [IEEE 2013]. Os mecanismos de segurança devem fornecer privacidade para os veículos, mas também devem ser capazes de monitorar o comportamento desses veículos para poder identificar um veículo se o mesmo assumir um comportamento inadequado (malicioso). Os veículos precisam ter uma privacidade condicional em redes veiculares [Huang, 2014]. Em outras palavras, a privacidade dos veículos será garantida se eles se comportarem de forma adequada na rede [Wangham, 2014].

Na rede social proposta, os usuários selecionam a privacidade que desejam ter, assim como [Karagiannis, 2011] propõe que o nível de privacidade seja ajustado pelo usuário, considerando ainda aberta a pesquisa na área de anonimicidade e privacidade adaptativa. A escolha de usuários confiáveis reflete então a diminuição de privacidade para compartilhar informações de seus deslocamentos, o que poderia ser desvantagem em relação à anonimicidade, mas as mensagens são autenticadas e propagadas apenas para rede social do usuário.

Como exemplo prático de ataques contra a privacidade, tem-se: rastreamento, a busca de um veículo durante a sua viagem; engenharia social, se um veículo em um determinado momento está na garagem ou em circulação [Wangham, 2014]. O usuário das aplicações que utilizam o modelo de confiança proposto definirá quais informações deseja enviar e com quem compartilhará essas mensagens, ou seja, usuários que ele escolheu como confiáveis para fazer parte de sua rede social e seus respectivos amigos.

No modelo de confiança deste trabalho, a escolha de amigos define o nível de privacidade desejada na comunicação com os usuários. Usuários com nível de confiança que estão se comunicando salvam as respectivas chaves públicas, enquanto um intruso dificilmente saberia qual chave foi usada. Um requisito de alto nível de privacidade geralmente resulta em um aumento na sobrecarga computacional e de comunicação, o que não pode ocorrer em redes vDTN. A privacidade adaptativa é uma questão em aberto, assim como a construção de sistemas de gerenciamento de identidades projetados particularmente para o ambiente altamente dinâmico das redes veiculares. Para manter o anonimato nessas redes, pesquisadores consideram consenso o uso de criptografia de curvas elípticas (ECC) [Wangham, 2014].

5.4. Conclusão

Neste capítulo foi apresentado o modelo de confiança proposto para redes veiculares tolerantes a interrupções, com objetivo de prover comunicação segura entre os usuários e possibilitar a troca de informações confiáveis entre eles. Por meio do uso de certificados por usuários da rede social, é possível o compartilhamento de chaves por contato direto, entre duas pessoas que se conhecem e garantem sua identidade, então assinam o certificado do outro mutuamente. As assinaturas desses certificados por usuários não reconhecidos

como autoridades certificadoras oficiais são validadas por amigos e amigos de amigos que tem armazenada a chave pública do usuário.

Além disso, o mecanismo de reputação possibilita também que usuários beneficiados possam emitir uma assinatura de reputação positiva, para identificar o outro certificado como um usuário confiável, ou identifiquem usuários com mau comportamento com atribuição de reputação negativa. A atribuição de reputação, assim como a adição de amigos, é informada para a rede social do usuário de forma que passa a existir um novo caminho no grafo do modelo de confiança proposto. No caso da remoção de amigos, deixa de existir um caminho nesse grafo.

Capítulo 6

Avaliação

Este capítulo apresenta a avaliação por meio de simulações e utilização de *traces* reais de mobilidade de redes veiculares. O funcionamento dos mecanismos de segurança propostos paras redes vDTN é verificado, de maneira que os usuários apresentem comportamento adequado e não seja afetado o desempenho da rede. O estabelecimento de confiança por meio da utilização de rede social não representa alteração significativa em relação à taxa de entrega de mensagens da rede, visto que são necessárias apenas poucas mensagens para assinatura dos certificados.

As avaliações realizadas incluem *traces* reais de mobilidade e mostram o comportamento de uma rede veicular com a utilização de certificados em redes sociais para estabelecer confiança entre os usuários. As simulações indicam a probabilidade das mensagens recebidas serem de um amigo, ou amigo de amigos em comum, bem como de existir uma assinatura de reputação que possibilite o reconhecimento como confiável.

O objetivo das avaliações deste capítulo é verificar o comportamento da rede, em função do número de nós da rede e do número médio de usuários diretamente alcançáveis. As avaliações indicam o percentual de comunicações estabelecidas em enlaces seguros, usando certificados reconhecidos por sua rede social. Um modelo de simulação foi utilizado para calcular a probabilidade de estabelecer o enlace seguro para dois nós quaisquer que se encontram no trânsito a partir de um determinado perfil de tráfego, pois os nós tendem a estabelecer os mesmos trajetos de forma repetitiva. Nesse cenário, um nó tende a repetir os encontros com determinada frequência, o que aumenta as chances de relacionamento próximo pelo mecanismo de reputação.

Este capítulo é composto em sua primeira parte da metodologia aplicada; e cenário das simulações na Seção 6.2. A Seção 6.3 apresenta os resultados e discussão da simulação com modelo de mobilidade sintético. Na Seção 6.4 apresenta-se a avaliação realizada com uso de *traces* de mobilidade, seguida da conclusão deste capítulo na Seção 6.5.

6.1. Metodologia aplicada

Para validar o modelo de confiança aqui apresentado, um conjunto de simulações foi realizado para verificar o comportamento da rede, em função do número de nós da rede e do número médio de usuários diretamente alcançáveis. O objetivo é mostrar o comportamento da rede veicular com utilização dos certificados auto-assinados à medida que os usuários passam a participar e serem autenticados pelos outros usuários, considerando os aspectos da tolerância a interrupções.

Foram utilizados também *traces* de redes com dados reais de contatos entre dispositivos móveis para ter menos controle sob o cenário e parâmetros de simulação. O desempenho das abordagens em redes veiculares de acordo com o número de nós na rede é considerado um fator importante, pois esse tipo de rede tende a ser composta por uma grande quantidade e diversidade de nós.

Aplicações, protocolos e algoritmos não são escolhidos considerando apenas sua "elegância" e capacidade, assim os impactos da solução proposta neste trabalho são avaliados bem como o desempenho e funcionalidade alcançados. Soluções de segurança em redes DTN são validadas em relação a alguns aspectos importantes como consumo de recursos e sobrecarga de mensagens na rede; duas métricas críticas que são comumente utilizadas para avaliar redes DTN são a porcentagem de pacotes entregues e a latência da entrega [Oliveira, 2010]. Como usuários entram ou deixam as redes veiculares a qualquer momento, alguns pacotes nunca são entregues mesmo quando adversários não estão presentes.

Além da avaliação de desempenho com objetivo de avaliar a escalabilidade, é analisado o impacto das funcionalidades. Deve-se verificar que mensagens somente são enviadas quando for realmente necessário assinar ou validar um certificado. Isso economiza recursos da rede, tanto em processamento quanto em comunicação, e será observado o número de mensagens relacionadas aos certificados. Foram utilizadas as seguintes métricas na avaliação apresentada neste capítulo:

- Percentual médio de usuários confiáveis por cada nó da rede veicular;
- Mensagens confiáveis em relação a recebidas por nós da rede;
- Impacto de amigos de amigos e reputação na seleção de mensagens confiáveis;
- Impacto de intrusos e reputação negativa no modelo de confiança;
- Média de atraso na entrega das mensagens;
- *Overhead* de mensagens utilizadas na certificação SNVC.

O percentual médio de usuários confiáveis por cada nó da rede veicular indica o número médio de usuários diretamente alcançáveis que fazem parte da rede social daquele nó como amigos ou amigos de amigos. Um valor percentual baixo para essa métrica indica dificuldade de comunicação com outros nós da rede veicular, enquanto um percentual alto indica comunicação confiável com a maior parte dessa rede.

Da mesma forma, o percentual de mensagens confiáveis em relação a recebidas por nós da rede indica a restrição aplicada pela validação de mensagens do modelo de confiança proposto. Tal métrica é relacionada ao percentual de usuários confiáveis, pois o maior valor desse percentual representa maior número de mensagens consideradas confiáveis. Se o percentual de mensagens confiáveis for baixo, o modelo de confiança torna-se inviável por ser muito restritivo.

O impacto de amigos de amigos e reputação na seleção de mensagens confiáveis indica o ganho de se considerar outros usuários confiáveis além dos amigos. A utilização de apenas amigos como usuários confiáveis pode restringir a comunicação entre nós da rede veicular, representando percentuais baixos de mensagens confiáveis. Dessa forma, são avaliados os graus de confiança propostos neste trabalho.

A presença de intrusos e o impacto de reputação negativa no modelo de confiança avaliam como a reputação será utilizada para descartar mensagens, mesmo que enviadas pela rede social do usuário se a reputação de quem enviou a mensagem for negativa. Essa métrica indica o comportamento da rede veicular em uma situação com atribuição de mais reputações negativas que bonificações positivas, obtendo o percentual de mensagens ignoradas que não são consideradas confiáveis pelo modelo proposto.

A média de atraso na entrega das mensagens é uma métrica comumente avaliada em redes DTN como as redes veiculares deste trabalho. Nesse caso, compara-se a média de atraso com utilização do modelo de confiança proposto com um cenário em que todos os nós da rede são considerados confiáveis, ou seja, sem aspectos de segurança e restrições a mensagens recebidas.

O *overhead* de mensagens utilizadas na certificação SNVC representa o impacto para estabelecer confiança entre os usuários da rede social. Em razão dos recursos limitados em redes DTN, evita-se sobrecarregar a rede com alto número de mensagens para mecanismos de segurança. Essa métrica indica o percentual de mensagens geradas pelo modelo de confiança proposto em relação ao total de mensagens recebidas pelos usuários.

Para avaliar tais métricas, a variação do número de nós da rede e do percentual de amigos de cada nó será observada. A geração de mensagens permanecerá na mesma

quantidade, pois considera-se mais importante obter os valores percentuais das mensagens confiáveis que o número total de mensagens geradas. De acordo com o modelo de rede vDTN deste trabalho, não foi avaliada a presença de infraestrutura de rede nas vias.

A partir da rede social proposta pelo modelo de confiança deste trabalho, realizou-se a implementação dos aspectos relacionados aos certificados de amigos, bem como consequências em relação à validação e aceitação de mensagens como confiáveis. Para tanto, procurou-se o ambiente mais adequado para simulação das características das redes veiculares DTN.

Utilizou-se o simulador The ONE (*Opportunistic Networking Evaluator*) [Keranen, 2009], que simula um modelo de comunicação tolerante a interrupções, no qual os nós seguem o paradigma guardar-carregar-repassar mensagens (*store-carry-forward*), ao mantê-las em um buffer caso o nó não tenha conexão direta com o destino. Cada teste foi executado repetidamente, sendo alterada a semente geradora do padrão de mobilidade.

The ONE é um simulador desenvolvido em Java, projetado e implementado por Ari Keränen, *download* disponível na Internet (http://www.netlab.tkk.fi/tutkimus/dtn/theone/). O ambiente de simulação tem sido utilizado em vários trabalhos relativos a redes tolerantes a interrupções [Doering, 2010], sendo capaz de:

- gerar movimento do nó usando diferentes modelos;
- visualizar mobilidade e envio de mensagem em tempo real na interface gráfica;
- rotear mensagens entre nós usando diferentes modelos;
- executar os protocolos de roteamento já implementados: *Direct Delivery, Epidemic, Spray and Wait* e *PRopHet*.

6.2. Cenário

Como é esperada diversidade de usuários participando das redes veiculares, as simulações inicialmente consideraram uma rede móvel heterogênea, com o número total de nós variando entre 50 e 600 nós com velocidades que variam entre 20 e 60 km/h [Teixeira, 2014]. Os nós são distribuídos pela rede de forma aleatória e deslocam-se de acordo com probabilidades definidas entre as regiões de um cenário urbano. Os pontos de interesse foram definidos como regiões centro, universidade e bairro. Os nós se deslocam entre as regiões pelas vias de uma cidade, como é visualizado na Figura 6.1.

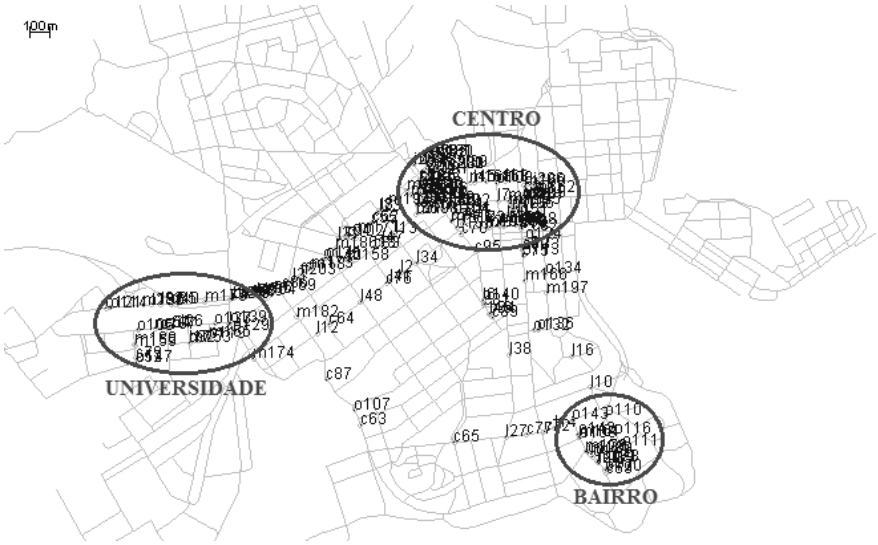

Figura 6.1. Cenário das simulações com modelo sintético.

Cada nó corresponde a um par veículo-motorista. Por considerar o deslocamento em uma região urbana, o cenário utiliza um mapa e as rotas procuram obter o menor caminho possível para o destino dos nós. Foi utilizado o padrão de mobilidade "*Shortest Path Map Based Movement*" [Ekman, 2008], que é uma derivação do "*Random Waypoint*", onde os nós usam o algoritmo de *Dijkstra* para o menor caminho para definir a rota do local atual até um destino selecionado de maneira randômica, por meio dos caminhos disponíveis.

Os nós se movimentam dentro da região abrangida pela rede, que possui tamanho de 4500 x 3400 metros. No entanto, há regiões nessa área onde os nós não possuem conectividade. Não existe infraestrutura nas vias para comunicação com os nós. Somente existe conexão *ad hoc* entre quaisquer dois nós quando ambos estão dentro do respectivo raio de transmissão. Considerando o padrão IEEE 802.11p [IEEE 2010] para redes veiculares, esse raio foi definido como 100m para os nós, enquanto a velocidade de transmissão dos dados foi 2 Mbps e o buffer de mensagens 10MB para cada nó.

A Tabela 6.1 apresenta os aspectos do cenário utilizado na avaliação. Para o roteamento, foi utilizado o protocolo *Spray and Wait* no modo binário [Spyropoulos, 2005]. Tal protocolo foi escolhido porque a melhor defesa em redes DTN contra ataques de perda de pacotes é o uso de caminhos múltiplos [Burgess, 2007]. Cada teste foi executado repetidamente, no mínimo oito vezes, sendo alterada a semente geradora do padrão de mobilidade. Mensagens são geradas a cada 30-45 segundos por algum usuário da rede seguindo uma distribuição uniforme e os períodos observados para avaliação foram de 24 horas, gerando-se assim mais de 2000 mensagens em cada simulação.

Tabela 6.1. Características do cenário da avaliação.

Área simulada	4500 x 3400 metros
Tempo de simulação	24 horas
Número de nós	50 a 600 nós
Velocidade dos nós	20 a 60 km/h [Teixeira, 2014]
Modelo de mobilidade	*Shortest Path Map Based Movement* [Ekman, 2008]
Raio de alcance dos nós	100m (IEEE 802.11p)
Taxa de transmissão	2 Mbps
Nó da rede	Representa par veículo-motorista
Geração de mensagens	30 a 45 segundos
Protocolo de roteamento	*Spray and Wait*

6.3. Resultados e discussão

Inicialmente, foi verificado o impacto da utilização do modelo de confiança por meio da rede social proposta na rede veicular, calculando o número médio de usuários considerados confiáveis, ou seja, amigos ou amigos dos amigos. Logo após, foi analisado o comportamento da rede veicular à medida que os usuários passam a participar e as mensagens serem autenticadas pelos outros usuários, considerando os aspectos da tolerância a interrupções. Os resultados são apresentados nos gráficos a seguir com 95% para o intervalo de confiança.

Os primeiros resultados dos dados coletados corresponderam à média de usuários confiáveis na rede veicular de acordo com o modelo de confiança proposto. O percentual de amigos que cada nó da rede veicular possui foi parametrizado entre 1% e 25% dos nós da rede.

Na Figura 6.2 observa-se que o percentual estipulado como número de amigos na simulação interfere diretamente na média de usuários confiáveis, que considera também os amigos dos amigos. O aumento no percentual de amigos incrementa o percentual de usuários confiáveis em aproximadamente 20 a 30% dos nós da rede, pois o maior número de amigos agrega outros usuários confiáveis. Com 25% de amigos na rede, quase todos os nós da rede são considerados usuários confiáveis. À medida que o número de nós da rede aumenta, há um incremento proporcional na média de usuários confiáveis.

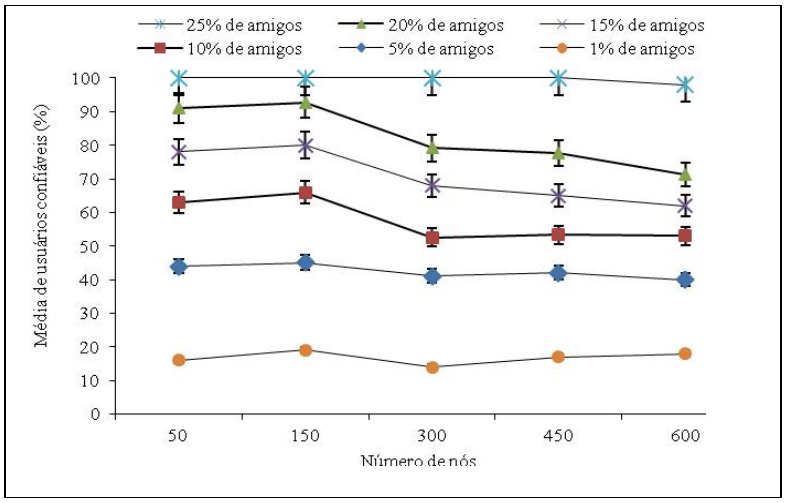

Figura 6.2. Percentual médio de usuários confiáveis por cada nó da rede veicular.

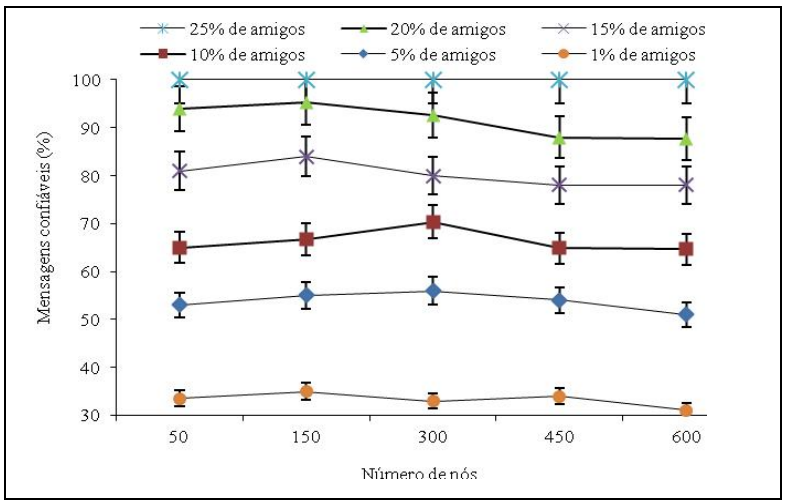

Figura 6.3. Mensagens confiáveis em relação a recebidas por nós da rede.

A Figura 6.3 mostra o impacto da utilização dos graus de confiança como critério na seleção de mensagens recebidas por usuários da rede veicular DTN, visto que o percentual de mensagens confiáveis representa mais segurança na comunicação. Com apenas 1% de amigos na rede, a seleção de mensagens é restritiva e limita a utilização do modelo de confiança proposto. O percentual de mensagens confiáveis com 5% ou 10% de amigos foi considerado viável como superior a 50%, atingindo percentuais próximos ou superiores a 80% em relação às mensagens entregues nos cenários com 15% ou mais de amigos.

As mensagens recebidas por usuários da rede social foram analisadas para decidir sobre sua confiança, o que não representou restrição no cenário com 25% de amigos. O aumento do percentual de amigos de cada nó representou até 20% de acréscimo no percentual de mensagens confiáveis, ou seja, enviadas por amigos ou amigos de amigos.

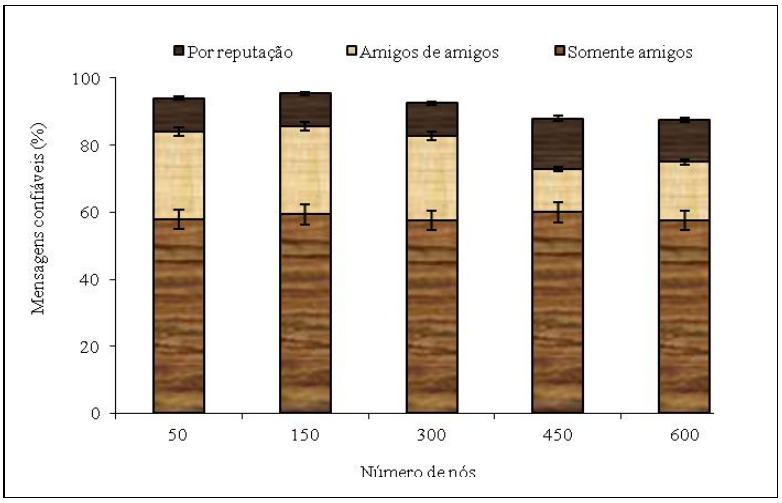

Figura 6.4. Impacto da reputação e de amigos de amigos com 20% de amigos na rede.

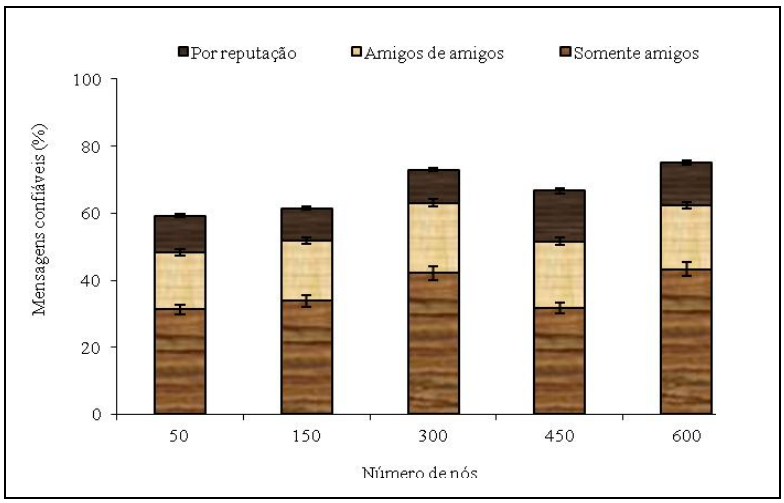

Figura 6.5. Impacto da reputação e amigos de amigos na seleção de mensagens confiáveis.

A Figura 6.4 mostra a análise com 20% de amigos dos percentuais de mensagens confiáveis com apenas mensagens de amigos, mensagens de amigos dos amigos ou reconhecidas por reputação. O impacto das mensagens recebidas de amigos de amigos é visto pelo aumento considerável no percentual de mensagens confiáveis, que representa variação entre 15% e 30% das mensagens confiáveis.

Estipulando-se 10% de amigos para cada nó da rede, na Figura 6.5 também foi analisado o impacto de utilizar a reputação e incluir também mensagens de amigos dos amigos na seleção de mensagens confiáveis. Incluir certificados de reputação é vantajoso, pois aumenta o percentual de mensagens confiáveis em cerca de 10%. Algum amigo de amigo pode atribuir reputação a um usuário que torna-se amigo por reputação, assim esse usuário será confiável para quem receber a propagação dessa reputação.

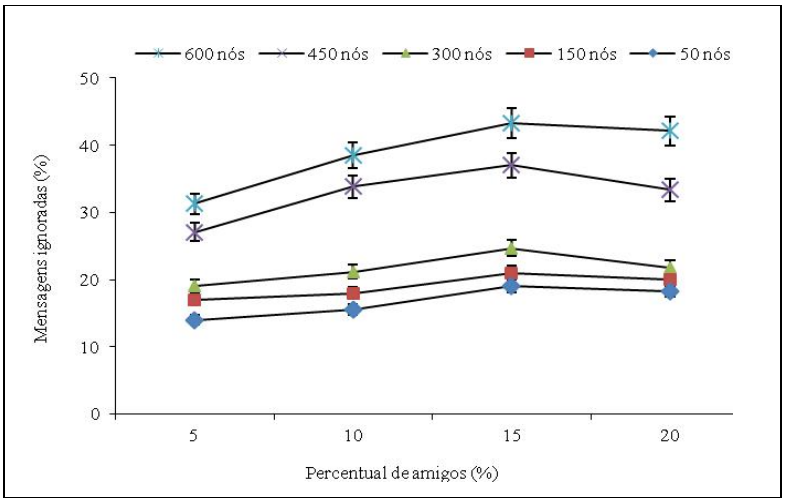

Figura 6.6. Impacto de intrusos e reputação negativa no modelo de confiança.

A Figura 6.6 apresenta a simulação de uma situação extrema com número de reputações negativas superior às bonificações positivas, obtendo o percentual de mensagens ignoradas pelo modelo de confiança proposto. Percebe-se que a reputação negativa possibilita uma forma de desconsiderar mensagens de usuários da rede social que tiveram avaliações negativas em suas contribuições anteriores, com aproximadamente 20% a 30% das mensagens recebidas.

A validação da reputação de um usuário da rede social dentro dos limites aceitos para confiança resulta no percentual de mensagens ignoradas, o que permite restringir mensagens de usuários com reputação negativa mesmo que sejam amigos ou amigos de amigos. Um usuário ignora mensagens de um amigo que tenha reputação negativa em 5 (cinco) unidades ou um amigo de amigo com reputação menor que 2 (duas) unidades negativas, portanto não possuem grau de confiança. Definidos os valores iniciais como máximo para confiança em 10, os limites foram avaliados no grafo da rede social por valores de *threshold*: 5 a 10 para amigos e 5 a 7,5 para amigos de amigos.

A Figura 6.7 mostra a variação do atraso médio das mensagens entregues na rede veicular DTN com o modelo de confiança e sem a utilização do mesmo. A comparação da utilização do modelo de confiança com um cenário em que todos os nós da rede são confiáveis não apresentou variação significativa no atraso das mensagens. Ao possuir mais amigos e consequentemente mais usuários confiáveis, as mensagens alcançam o nó mais rápido por meio de outros caminhos no grafo da rede social. O número de caminhos possíveis no modelo de confiança proposto cresce também devido ao maior número de amigos dos amigos, assim a média de atraso diminui com maior percentual de amigos.

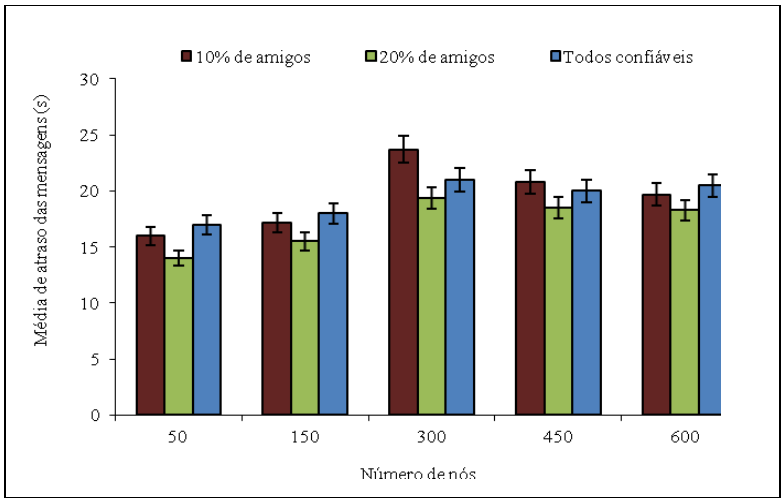

Figura 6.7. Média de atraso na entrega das mensagens.

Analisando os resultados, inicialmente verificou-se o impacto da variação do número de amigos na rede veicular com percentual estipulado e usuários adicionando outros usuários como amigos. O número de amigos interfere diretamente na seleção de mensagens confiáveis, que considera envio de amigos ou amigos de amigos. Quanto maior o número de amigos que um usuário da rede possuir, maior a possibilidade de que uma mensagem recebida por ele seja reconhecida como confiável.

Quando um usuário adiciona um novo amigo, ele recebe as chaves públicas dos amigos desse amigo que se tornam também usuários confiáveis, que serão capazes de trocar mensagens confiáveis. O aumento no número de amigos provoca um aumento igual ou maior no número de usuários confiáveis. Portanto, a inclusão de amigos dos amigos na seleção de mensagens aumenta o percentual de mensagens consideradas confiáveis.

No grafo da rede social proposta, há caminhos para comunicação confiável entre amigos e amigos de amigos. A reputação também representa um novo caminho, pois algum amigo de amigo pode atribuir um bônus de reputação para o certificado de um usuário e propagar à sua rede social que ele também é considerado confiável, tornando-se amigo por reputação. Os bônus de reputação recompensam informações úteis dos usuários, que dessa forma obtém outro caminho no grafo da rede social.

O número de caminhos do nó para recebimento de mensagens confiáveis cresce também com a obtenção de mais bônus de reputação. Assim, a inclusão da reputação como critério na seleção de mensagens foi considerada vantajosa, pois representou aumento no percentual de mensagens confiáveis e ainda valida se os usuários estão agindo em benefício da rede social.

Tabela 6.2. Métricas e resultados sumarizados da avaliação.

Métricas	Resultados sumarizados
Média de usuários confiáveis	40% dos usuários com 5% de amigos 50% a 100% dos usuários acima de 5% de amigos
Mensagens confiáveis	35% das mensagens recebidas com 1% de amigos 50% a 100% das mensagens entre 5% e 25% de amigos
Impacto da reputação	Aumento de 10% a 15% das mensagens confiáveis
Impacto de amigos de amigos	Aumento de 15% a 25% das mensagens confiáveis
Intrusos e reputação negativa	20 a 30% de mensagens ignoradas
Média de atraso da entrega	Aproximadamente igual com todos os nós confiáveis
***Overhead* de mensagens**	10% das mensagens recebidas

O maior número de usuários confiáveis representa mais caminhos possíveis no grafo da rede social para a entrega de mensagens confiáveis. Portanto, o atraso das mensagens entregues considerando aspectos da rede veicular DTN diminui à medida que torna-se maior o número de amigos e consequentemente amigos de amigos, bem como os bônus de reputação também auxiliam na entrega de mensagens confiáveis. O modelo de confiança apresentou *overhead* de aproximadamente 10% das mensagens recebidas na simulação, o que representa um baixo impacto para estabelecer confiança entre os usuários.

A Tabela 6.2 apresenta as métricas e resultados sumarizados da avaliação realizada. Foi possível verificar nas simulações que a utilização da rede social resulta em vantagens independente do número de nós da rede veicular, pois representa maior segurança para os usuários em relação à confiança e legitimidade da rede. O número de mensagens entregues diminui, pois se restringe aos usuários confiáveis. Como inicialmente não existiam chaves para autenticação das mensagens, a certificação proposta pelo modelo de confiança representa uma alternativa ao gerenciamento de chaves baseando-se em uma rede social.

6.4. Avaliação com *traces* de mobilidade

Ao utilizar *traces* de redes com dados reais de contatos entre dispositivos móveis, tende-se a ter menos controle sob o cenário e parâmetros de simulação. Dessa forma, o modelo de confiança proposto foi avaliado com utilização de três *traces* com mobilidade dos nós em

redes vDTN: DieselNet [Burgess, 2006], Chicago [CTA, 2010] e Seattle [Jetcheva, 2003]. Vários trabalhos relacionados já utilizaram esses conjuntos de dados, tais como [Burgess, 2007], [Liu, 2012], [Pereira, 2012], [Doering, 2010], [Uppoor, 2014] e [Zhang, 2010].

O conjunto de registros reais de mobilidade DieselNet é resultado de um experimento realizado pela Universidade de Massachusetts, que implantou uma plataforma de testes para redes DTN usando seus ônibus [Burgess, 2006]. Os registros do conjunto DieselNet utilizados neste trabalho compreendem aproximadamente 30 ônibus que circulam nos arredores do campus *Amherst* da *University of Massachusetts* (UMass). Cada ônibus está equipado com um ponto de acesso e uma interface *wireless* IEEE 802.11b, um dispositivo *Global Positioning System* (GPS) e um computador com o sistema operacional Linux. Os dados foram pré-processados para exclusão dos contatos entre ônibus e pontos de acesso, visando considerar somente as conexões entre os nós móveis da rede.

Seattle fornece um ambiente de roteamento topograficamente desafiador, composto por um lago de mais de 90 quilômetros quadrados no meio da cidade. Os *traces* [Jetcheva, 2003] fornecem dados de movimento real da frota de ônibus urbanos em Seattle, área metropolitana de Washington, em suas rotas normais fornecendo serviço a passageiros de toda a cidade. O número de nós móveis da rede obtida por meio do *trace* Seattle, presente nas simulações deste trabalho varia entre 50 e 130 ônibus, em uma área de aproximadamente 5.000 quilômetros quadrados.

Os traces de mobilidade de Chicago [CTA, 2010] foram obtidos a partir da *API Bus Tracker* do *Chicago Transport Authority* (CTA) por meio do rastreio dos ônibus, o qual está disponível e documentado publicamente. Sistemas de localização de veículos automatizados nos ônibus enviam atualizações de posição para um servidor central no CTA. Durante 18 dias em novembro de 2009, um script foi usado para armazenar posições de veículos identificados e temporizados em um banco de dados. Esses *traces* foram comparados com os *traces* de Seattle em [Doering, 2010].

Na Tabela 6.3 são mostradas as características dos *traces* utilizados e parâmetros das simulações. Cada nó da rede corresponde a um par veículo-motorista e envia mensagens para rede social. A análise dos dados dos *traces,* disponíveis em [Corner, 2011] [Crawdad 2015], tem dois objetivos: verificar a viabilidade do modelo de confiança proposto e definir os parâmetros ideais para que a solução proposta apresente os melhores resultados. Para realizar essa análise, inicialmente os *traces* foram convertidos para o formato de entrada do simulador *The ONE* [Keranen, 2009] para redes DTN. A mesma implementação foi avaliada sob as diferentes características dos três *traces*: DieselNet, Chicago e Seattle.

Tabela 6.3. Características dos *traces* utilizados na avaliação.

Trace	DieselNet	Chicago	Seattle
Área aproximada	241 km^2	606 km^2	5.100 km^2
Tempo de duração	60 dias	13 dias	18 dias
Número de nós	30 nós	1648 nós	50 a 130 nós
Nó da rede	Representa par veículo-motorista		
Raio de alcance dos nós	100m (IEEE 802.11p)		
Taxa de transmissão	2 Mbps		
Geração de mensagens	30 a 45 segundos		
Protocolo de roteamento	*Spray and Wait*		

Na Figura 6.8 são mostrados os resultados da aplicação do modelo de confiança em quatorze dias do *trace* DieselNet, variando-se o percentual de amigos de cada nó desde 1 a 20% dos nós da rede. O percentual de usuários confiáveis, que inclui amigos e amigos de amigos, é inicialmente baixo com 1% de amigos e aumenta consideravelmente com 5% de amigos na rede. O percentual de 5% de amigos obtém valores próximos de 40% de usuários confiáveis da rede, o que viabiliza a troca de mensagens. O percentual de usuários confiáveis aumenta mais com 10% de amigos na rede, da mesma forma que a presença de 15% ou 20% de amigos representa resultados próximos da totalidade de nós confiáveis. Ao longo do dia, os usuários passam a reconhecer outros como usuários confiáveis, o que aumenta o percentual analisado com a propagação de amigos de amigos.

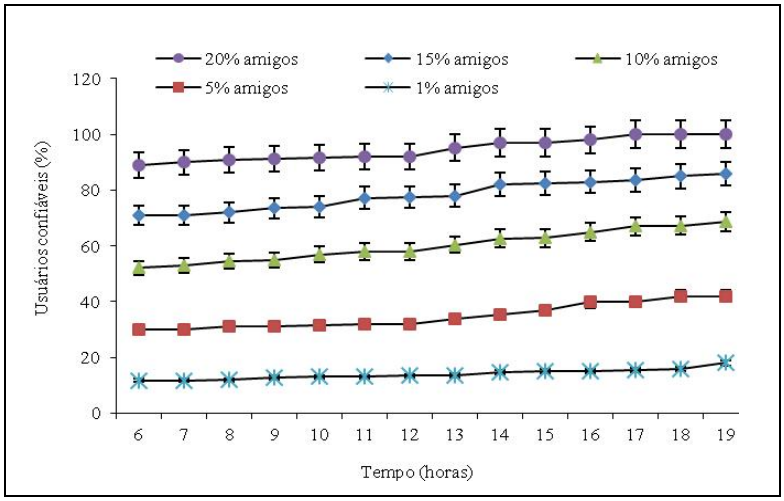

Figura 6.8. Percentual de usuários confiáveis (DieselNet).

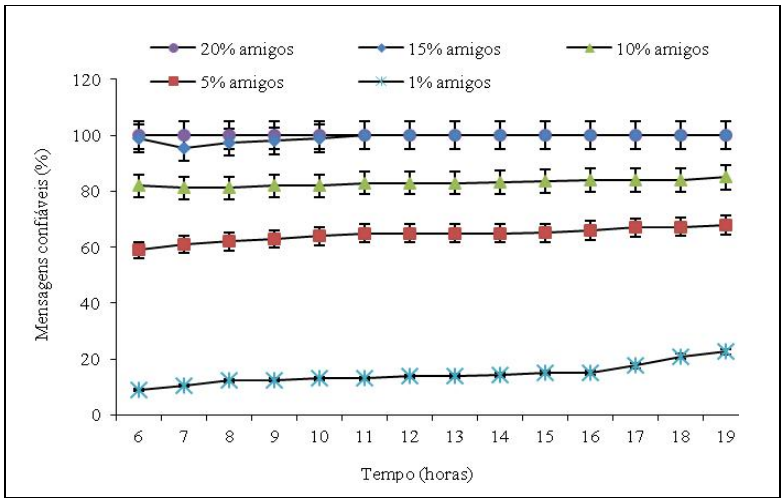

Figura 6.9. Percentual de mensagens confiáveis em relação a entregues (DieselNet).

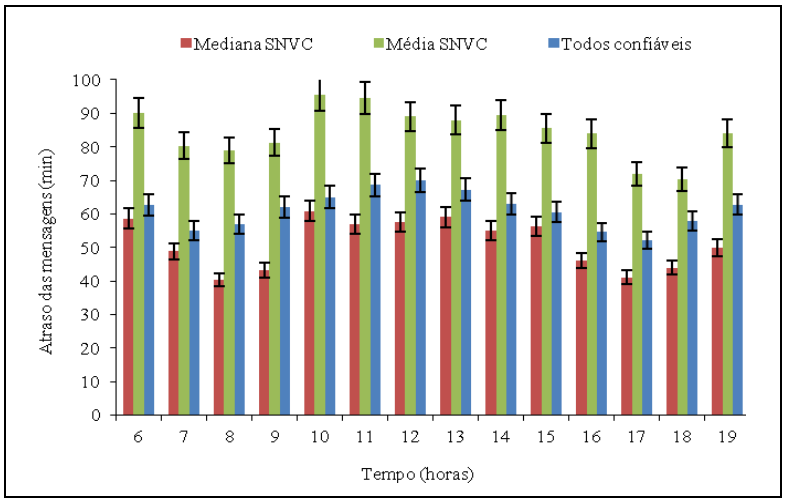

Figura 6.10. Mediana e média do atraso das mensagens entregues (DieselNet).

A Figura 6.9 apresenta os reflexos do percentual de usuários confiáveis no percentual de mensagens confiáveis recebidas pelos usuários no mesmo período do *trace* DieselNet com variação do percentual de amigos na rede. Com apenas 1% de amigos para cada nó, a seleção de mensagens confiáveis torna-se restritiva em valores próximos a 20% das mensagens entregues. A partir de 5% de amigos, com cerca de 60% mensagens confiáveis, os percentuais são suficientes para comunicação segura por meio da rede social, chegando a 100% de mensagens confiáveis com a presença de 15% ou 20% de amigos na rede.

Durante a avaliação do modelo de confiança no *trace* DieselNet, foi verificado o atraso das mensagens entregues como mostrado na Figura 6.10. De forma geral, não houve alteração no atraso das mensagens com utilização do modelo de confiança e variação do percentual de amigos na rede social em relação ao cenário com todos os usuários

confiáveis, que não utilizaria o SNVC e apresenta valores semelhantes para média e mediana do atraso das mensagens. Foi observado que os valores da média de atraso foram consideravelmente maiores à mediana do atraso em cada dia analisado, portanto a maior parte das mensagens da rede foi entregue em tempos inferiores aos resultados da mediana e apenas parte das mensagens com atraso elevado em relação às demais causou aumento na média de atraso da rede com utilização do modelo de confiança.

A comparação dos resultados obtidos com os *traces* DieselNet, Chicago e Seattle mediante aplicação do modelo de confiança é mostrada a partir da Figura 6.11, variando-se o percentual de amigos na rede de 5% a 20% dos nós. O percentual de usuários confiáveis aumentou nos três *traces* analisados, representando quase a totalidade dos usuários da rede com 20% de amigos na rede, ocorrendo o menor crescimento percentual no DieselNet. A maior variação no *trace* de Chicago está relacionada à presença de maior número de nós.

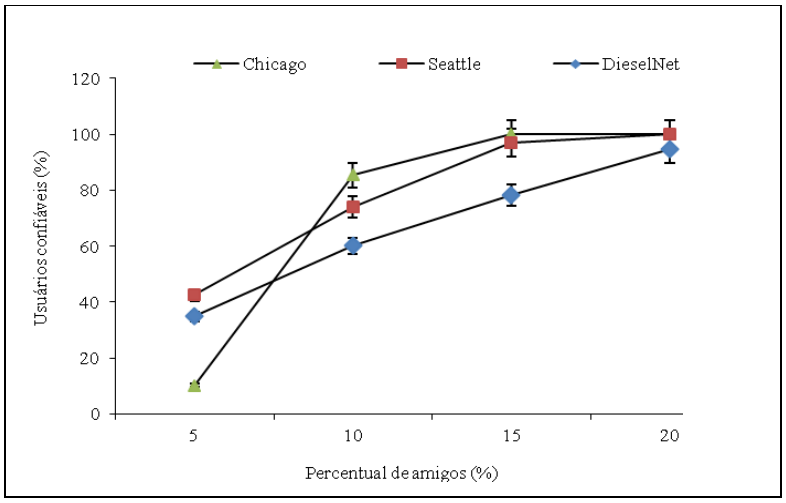

Figura 6.11. Percentual de usuários confiáveis nos *traces*.

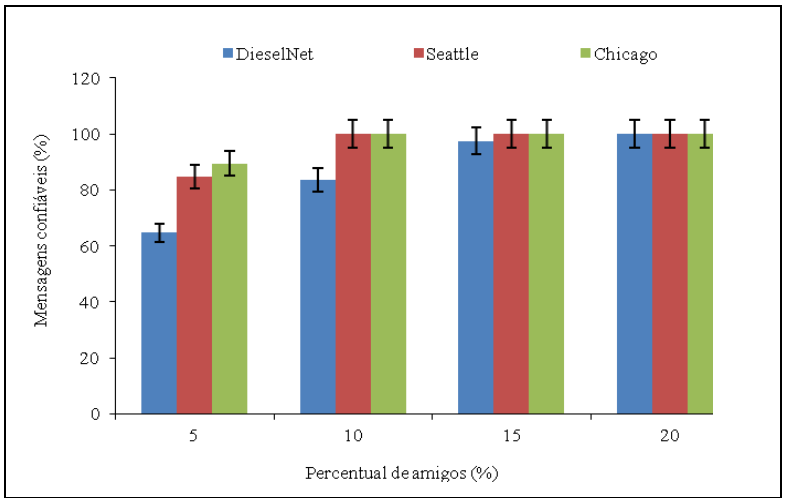

Figura 6.12. Percentual de mensagens confiáveis nos *traces*.

Na Figura 6.12 são mostrados os percentuais de mensagens confiáveis entregues pela rede com utilização dos *traces* DieselNet, Seattle e Chicago. No caso do DieselNet, o percentual de mensagens confiáveis aumentou gradativamente à medida que o percentual de amigos foi crescendo entre 5% e 20% de amigos, chegando ao patamar dos resultados obtidos nos *traces* Chicago e Seattle de aproximadamente 100% das mensagens confiáveis. O fato desses dois *traces* terem maior percentual de usuários confiáveis se reflete no maior percentual de mensagens com origem reconhecida, consideradas confiáveis. Por outro lado, o DieselNet avalia um período de tempo consideravelmente maior que os outros *traces*.

A Figura 6.13 apresenta o percentual de mensagens consideradas confiáveis por reputação pelo modelo de confiança nos *traces* utilizados. O aumento do percentual de amigos na rede implica em menor impacto de mensagens de reputação, pois o maior número de usuários diretamente confiáveis por meio da rede social facilita a troca de mensagens confiáveis sem a necessidade de mensagens de reputação. Com menor percentual de 5% de amigos, a importância do mecanismo de reputação torna-se maior por causa do limitado número de usuários da rede social enviando mensagens confiáveis. No caso do DieselNet, a importância da reputação foi maior no percentual de mensagens confiáveis, mesmo com descarte de reputações válidas por 30 dias (Seção 7.3) durante o período avaliado de 60 dias. Isso evita a sobrecarga com armazenamento de reputações.

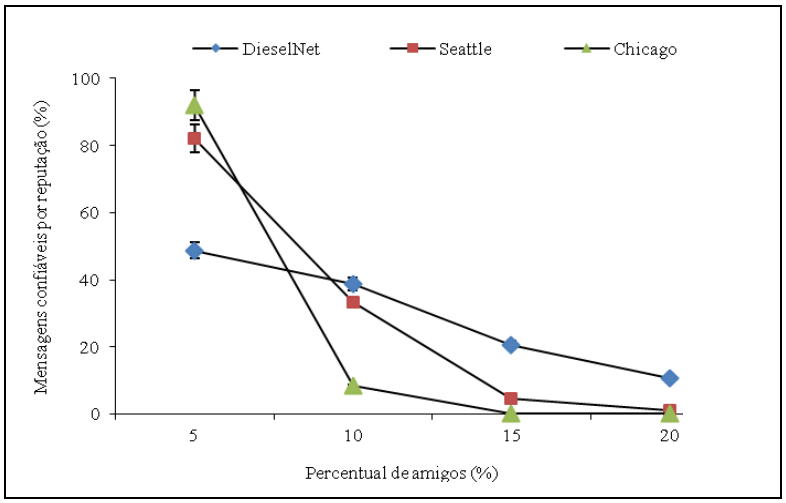

Figura 6.13. Percentual de mensagens confiáveis por reputação.

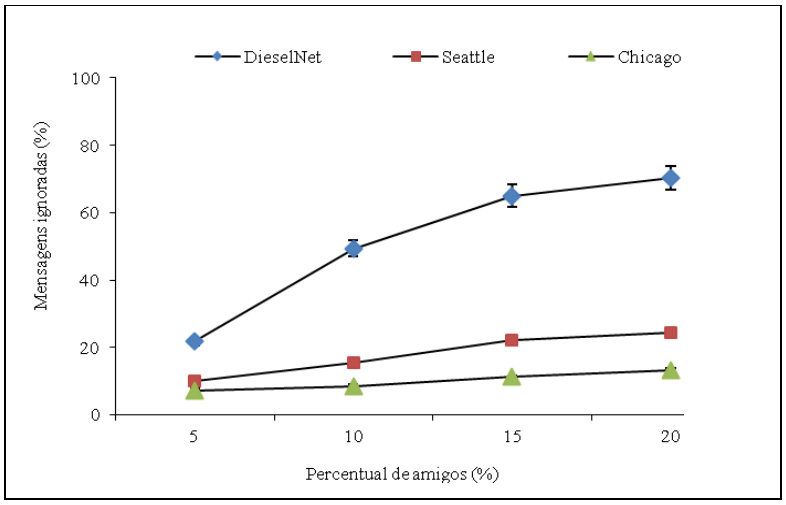

Figura 6.14. Percentual de mensagens ignoradas por reputação negativa.

Por meio da simulação de uma situação extrema com número de reputações negativas superior às reputações positivas, a Figura 6.14 apresenta o percentual de mensagens ignoradas devido ao mecanismo de reputação nos *traces* utilizados. A reputação negativa permite ao modelo de confiança uma forma de desconsiderar mensagens de usuários da rede social que tiveram avaliações negativas em suas contribuições, com valores próximos de 10% a 20%. No caso do DieselNet, como a importância da reputação foi maior no percentual de mensagens confiáveis anterior, o valor extremo de reputações negativas teve impacto mais significativo que nos outros *traces*.

O percentual de mensagens ignoradas deve-se à validação da reputação de usuários da rede social dentro dos limites aceitos para o modelo de confiança, o que permite restringir mensagens de nós com reputação negativa mesmo que sejam de amigos ou amigos de amigos. Se um amigo tiver reputação negativa em 5 (cinco) unidades ou um amigo de amigo tiver reputação menor que 2 (duas) unidades negativas, esse usuário não possuirá grau de confiança e suas mensagens serão ignoradas por esse usuário. Definidos os valores iniciais como máximo para confiança, os limites foram avaliados por valores de *threshold*: 5 a 10 para amigos e 5 a 7,5 para amigos de amigos.

O atraso das mensagens entregues foi comparado entre os *traces* DieselNet, Chicago e Seattle como mostrado na Figura 6.15. Não houve alteração significativa no atraso das mensagens com utilização do modelo de confiança em comparação com um cenário em que todos os usuários são confiáveis. Os resultados da média em todos os casos foram superiores à mediana, indicando que parte das mensagens é entregue com atraso menor que a mediana e a média é elevada por mensagens de atraso elevado. No caso de Chicago, os

valores maiores de atraso referem-se a longos períodos de desconexão. Valores próximos à média de atraso foram obtidos também na propagação de mensagem de reputação negativa.

A Figura 6.16 mostra o *overhead* de mensagens do SNVC em relação às mensagens recebidas pela rede, utilizando-se os *traces* DieselNet, Chicago e Seattle. A sobrecarga de mensagens do modelo de confiança é baixa devido ao contato direto entre amigos. A rede social só propaga novos relacionamentos aos amigos de amigos e reputação, o que totaliza aproximadamente 11% do total de mensagens entregues em cada cenário. O *overhead* avaliado representa baixo impacto, portanto é vantajoso aplicar o modelo de confiança.

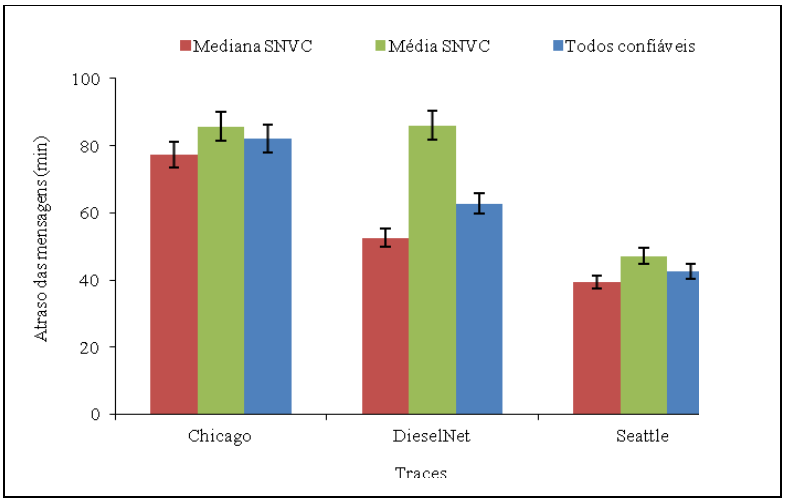

Figura 6.15. Média do atraso com modelo de confiança ou todos confiáveis.

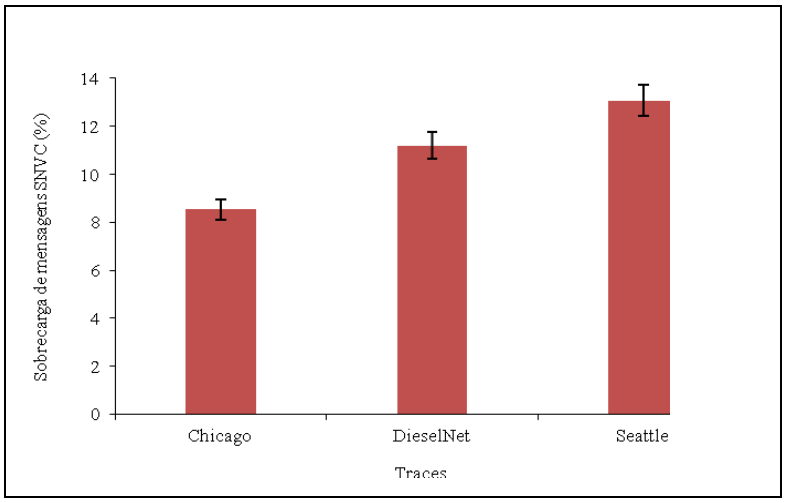

Figura 6.16. *Overhead* de mensagens com utilização do SNVC nos *traces* utilizados.

Tabela 6.4. Métricas e resultados aproximados na avaliação com *traces* reais.

Métricas	5% de amigos	10% de amigos	15% de amigos	20% de amigos
Média de usuários confiáveis	40%	70%	90%	97%
Mensagens confiáveis	80%	95%	100%	100%
Impacto da reputação	80%	30%	15%	5%
Mensagens ignoradas	5 a 20%	10 a 50%	15 a 60%	20 a 70%
Média de atraso da entrega	40 a 80 minutos			
***Overhead* de mensagens**	11% das mensagens recebidas			

A Tabela 6.4 mostra as métricas utilizadas e resultados aproximados obtidos com os *traces* reais na avaliação do modelo de confiança. Os percentuais dos resultados foram calculados como média dos *traces* DieselNet, Chicago e Seattle. A comparação desses três *traces* nos gráficos dessa seção permite confirmar as vantagens da utilização do modelo de confiança proposto e sua aplicabilidade em redes veiculares DTN. O funcionamento da rede social proposta teve avaliação positiva em cenários de 5 a 20% de amigos em relação aos nós da rede, tanto em cenário com muitos usuários como Chicago quanto redes esparsas como Seattle. No DieselNet ainda foi possível avaliar o comportamento da rede ao longo de um maior número de dias, também com avaliação positiva.

A utilização do modelo de confiança é viável em redes veiculares com percentual de amigos próximo ou superior a 5% dos nós da rede. Assim, espera-se restringir parte das mensagens recebidas por desconhecer sua origem. Muitos usuários perto de um evento em uma região podem disseminar alertas sobre o tráfego, assim a rede social pode propagar o mesmo evento por diferentes usuários. Basta que um desses usuários seja confiável para o usuário receber um alerta e tomar conhecimento sobre um evento.

Um conjunto de dados de alertas do Waze foi analisado nesse contexto [Silva, 2013]: algumas áreas têm centenas de alertas compartilhados, enquanto a maioria das áreas tem apenas um número pequeno. O conjunto de dados de alertas do Waze coletados diretamente do Twitter [Silva, 2013], uma vez que as informações de trânsito do Waze não são publicamente acessíveis por uma API. O conjunto de dados abrange seis meses entre dezembro/2012 e junho/2013 e consiste de 212.814 *tweets* contendo alertas sobre o tráfego compartilhado por usuários do Waze.

Em comparação com um cenário sem segurança onde todos os nós seriam supostamente confiáveis, a certificação SNVC não apresentou alteração significativa nos valores de atraso das mensagens recebidas. Com *overhead* de aproximadamente 11% das mensagens recebidas da rede como custo de implantação, afirma-se que o modelo de confiança proposto é vantajoso em relação ao cenário com mensagens sem autenticação devido à ausência do gerenciamento de chaves DTN.

6.5. Conclusão

A partir do relacionamento e conhecimento prévio dos usuários da rede veicular, a utilização do modelo de confiança proposto e seus critérios na seleção de mensagens confiáveis foram validados. As avaliações realizadas mostram o comportamento de uma rede veicular com a utilização de certificados em redes sociais para estabelecer confiança entre os usuários. Os resultados encorajam o aumento de amigos como uma forma de melhorar a troca de mensagens confiáveis, bem como a atribuição de bônus de reputação para promover o reconhecimento de usuários confiáveis.

As métricas avaliadas obtiveram percentual médio de usuários confiáveis por cada nó da rede veicular considerado viável a partir de 5% de amigos na rede, o que se reflete no percentual de mensagens confiáveis em relação a recebidas por nós da rede. O impacto de amigos de amigos e reputação na seleção de mensagens confiáveis foi considerado significativo, pois aumentou em 50% o percentual de mensagens confiáveis com 20% de amigos e aproximadamente duplicou esse percentual com 10% de amigos na rede. Tais percentuais corroboram os critérios de confiança propostos para autenticação dos usuários.

O impacto de intrusos e reputação negativa no modelo de confiança demonstrou uma forma de desconsiderar mensagens de usuários da rede social que tiveram avaliações negativas em suas informações anteriores, ignorando aproximadamente 20% a 30% das mensagens recebidas. A média de atraso na entrega das mensagens em um cenário com todos os nós considerados confiáveis foi próxima à mediana do atraso utilizando o modelo de confiança, pois algumas mensagens da rede social apresentam atraso elevado e tornam a média mais alta. O *overhead* de mensagens utilizadas na certificação SNVC foi considerado baixo, aproximadamente 11% do total de mensagens entregues.

As vantagens da utilização da rede social foram demonstradas por meio de simulações e *traces* de dados reais de mobilidade, sendo que as avaliações comprovam a

aplicabilidade do modelo de confiança proposto em redes vDTN. A maior segurança nas redes veiculares é alcançada devido à restrição de mensagens confiáveis, oriundas de usuários confiáveis e mecanismo de reputação, em relação a um cenário sem autenticação de mensagens. A certificação SNVC proposta representa uma solução de segurança baseada em rede social para problemas em aberto em redes tolerantes a interrupções.

Capítulo 7

Estudo comparativo

Este capítulo apresenta a comparação teórica e por simulações do modelo de confiança proposto neste trabalho com um mecanismo de reputação proposto anteriormente, que utiliza certificados em redes vDTN. Soluções de segurança para redes DTN são avaliadas em relação ao seu funcionamento e desempenho da rede. Além disso, é desejável a comparação com outro mecanismo de segurança já existente para essas redes, que apresente proposta relacionada, para melhor análise do impacto das novas soluções.

O modelo de confiança proposto permite que certificados de usuários da rede social reconhecidos como amigos por reputação sejam distinguidos como confiáveis. Para comparação com esta proposta, foi analisado o mecanismo de reputação RMDTV (*Reputation Mechanism for Delay Tolerant Vehicular Networks*) em que todos os veículos possuem certificados assinados por uma autoridade certificadora [Paula, 2010], diferentemente da certificação SNVC proposta neste trabalho. Há outros mecanismos de reputação relacionados a este trabalho na Seção 4 [Huang, 2014][Liang, 2013][Li, 2012], mas o RMDTV tem o modelo de rede mais próximo com uso de DTN.

A estrutura deste capítulo é composta em sua primeira parte da metodologia e comparação teórica entre as propostas na Seção 7.1, onde são apresentados os principais aspectos do RMDTV. A Seção 7.2 mostra o cenário e características do modelo de rede utilizado. Na Seção 7.3 apresentam-se os resultados e análise da comparação, seguidos da conclusão deste capítulo na Seção 7.4.

7.1. Metodologia e comparação

O funcionamento do modelo de confiança e da certificação SNVC propostos neste trabalho foi comparado ao mecanismo de reputação RMDTV anterior por meio de um conjunto de

simulações. O objetivo foi verificar o comportamento da rede, à medida que os usuários passam a participar e serem reconhecidos pelos outros usuários, considerando o cenário de redes veiculares tolerantes a interrupções.

Inicialmente houve um estudo e comparação teórica das diferenças entre a certificação SNVC e o mecanismo RMDTV. O mecanismo RMDTV também utilizou como base o PGP (*Pretty Good Privacy*) de forma que um nó da rede, após se comportar de maneira útil a outros usuários, agrega assinaturas de reputação atestando sua confiança. A partir da detecção de um evento no trânsito, cada veículo gera uma mensagem informando sua existência para distribuir em modo de difusão.

A partir das mensagens relevantes armazenadas em um veículo, o RMDTV toma uma decisão, ou seja, determina se avisa ou não ao motorista sobre uma possível situação de risco. Um veículo armazena informações sobre eventos até que seja recebida uma quantidade mínima de mensagens, então o processo de decisão é executado. O veículo ainda pode receber informações geradas por uma fonte confiável, como um ônibus ou órgão responsável pelo trânsito, e tomar a decisão apenas com base nessas informações.

As decisões tomadas por um veículo são decisões indicadas quando resultam da execução do processo de decisão do RMDTV, e são decisões forçadas quando o veículo não recebe o número mínimo de mensagens para execução da tomada de decisão [Paula, 2010]. No SNVC já ocorre decisão ao receber uma mensagem confiável, pois a rede social limita as informações recebidas apenas de usuários confiáveis. Dessa forma, não é necessário esperar atingir uma quantidade de informações ou tomar decisões forçadas.

No mecanismo RMDTV proposto anteriormente, os usuários da rede veicular atribuem reputações a outros usuários responsáveis pelo envio de informações corretas. Esses usuários adicionam as assinaturas de reputação a todas as mensagens geradas, no intuito de atestar sua confiança. De forma diferente, na certificação SNVC do modelo de confiança proposto, o usuário divulga as assinaturas de cada certificado aos seus amigos. Os amigos armazenam as assinaturas dos usuários confiáveis, portanto as mensagens enviadas utilizando o SNVC possuem menor tamanho por não enviar várias assinaturas.

Apenas reputações positivas são disseminadas no mecanismo RMDTV, logo não seria possível retirar uma assinatura ou bonificação anterior. Neste trabalho, é possível remover amigos ou difundir aos amigos que algum usuário forneceu informação incorreta, o que é contabilizado como reputação negativa. O cálculo da reputação no modelo de confiança proposto utiliza apenas as assinaturas de amigos do usuário que recebeu a mensagem, sendo necessário resultar reputação positiva para o usuário ser confiável.

O mecanismo RMDTV faz uso de uma infraestrutura de chave pública (PKI) para garantir a confidencialidade, autenticidade e integridade dos dados enviados. Considera que cada veículo recebe da Autoridade Certificadora (CA), no início de operação da rede, seu par de chaves (pública e privada) correspondente. Mesmo considerando como terceiro confiável o órgão governamental responsável pelo emplacamento dos veículos, todos os usuários possuem o mesmo grau de confiança em relação aos outros usuários. No modelo de confiança foram propostos graus de confiança que diferenciam amigos e amigos de amigos do usuário na análise de mensagens recebidas, inclusive assinaturas de reputação, ainda formam a rede social responsável pela certificação proposta.

A certificação proposta pelo modelo de confiança foi implementada para utilizar a rede social no mesmo ambiente que fosse executado o mecanismo RMDTV, de forma que ambos executassem em paralelo. Para tanto, procurou-se o ambiente mais adequado para simulação das características das redes veiculares DTN.

Para implementar e comparar os mecanismos foi utilizado o simulador "The ONE" (*Opportunistic Networking Evaluator*) [Keranen, 2009], que simula um modelo de comunicação tolerante a interrupções, no qual os nós da rede seguem o paradigma guardar-carregar-repassar mensagens (*store-carry-forward*), mantendo em um buffer caso o nó não tenha conexão direta com o destino. Cada teste foi executado repetidamente, sendo alterada a semente geradora do padrão de mobilidade. Foram utilizadas as seguintes métricas:

- Decisões certas em relação ao total de mensagens recebidas;
- Decisões indicadas do RMDTV em relação a decisões do modelo de confiança;
- Decisões erradas em relação à probabilidade de contato entre usuários;
- Decisões erradas afetadas por intrusos ou falsos positivos;
- Redução de tempo nas decisões certas do SNVC em relação ao RMDTV;
- Mensagens confiáveis no SNVC em relação às mensagens analisadas por RMDTV.

Tabela 7.1. Matriz de confusão para decisões do RMDTV.

Condição avaliada	**Decisão certa (Real)**	**Decisão errada (Real)**
Decisão certa	Verdadeiro Positivo	Falso Positivo
Decisão errada	Falso Negativo	Verdadeiro Negativo

A matriz de confusão apresentada na Tabela 7.1 descreve os termos avaliados que são característicos do RMDTV em relação a decisões certas e erradas. Ao final de cada dia de simulação é avaliado se a decisão tomada por cada usuário foi realmente a decisão certa ou ocorreu falso positivo. O modelo de confiança proposto neste trabalho propaga somente mensagens de usuários confiáveis, o que evita a ocorrência de falso negativo visto que uma informação correta é suficiente para impedir uma decisão errada.

7.2. Cenário da comparação

O cenário proposto pelo mecanismo RMDTV foi disponibilizado como um *trace* que permite a comparação com outras propostas, sendo utilizado um modelo de rede próximo do proposto neste trabalho em redes vDTN. Um conjunto de simulações foi executado para comparar o funcionamento dos mecanismos: RMDTV anterior e SNVC aqui proposto. O mapa digital da Figura 7.1 mostra a região de Belo Horizonte utilizada nas simulações. Com uma área de aproximadamente 55 km^2, esse mapa engloba toda a Avenida Antônio Carlos, um dos principais corredores da cidade, além da região central da cidade, onde circulam diariamente milhares de veículos, resultando em vários congestionamentos.

O tempo de simulação foi o equivalente a vinte dias úteis, iniciando-se às 7h da manhã do primeiro dia. Baseado em *traces* reais [Naumov, 2006], o modelo de mobilidade indica o comportamento dos usuários da rede durante os dias de trabalho. Foram simuladas quatro semanas de trabalho na rotina desses usuários. Mensagens com tamanho de 10 a 500kB cada são geradas por cada usuário da rede 3 vezes por dia de acordo com a probabilidade de eventos de alteração do trânsito [Paula, 2010]. No caso do modelo de confiança elas são propagadas para seus amigos e amigos de amigos, ainda é atribuída reputação para as mensagens em ambos os casos. Os valores do padrão IEEE 802.11p [IEEE 2010] foram utilizados para alcance de rádio 200m e largura de banda dos usuários 1Mbps. Tais simulações não consideraram restrições de processamento e armazenamento, os dados recebidos por cada nó foram armazenados em um *buffer* de tamanho ilimitado.

No cenário da Avenida Antônio Carlos foi colocada uma estação base para propagação das mensagens do RMDTV, mas a mesma não é utilizada pelo SNVC que considera apenas comunicação V2V. Inicialmente foi definido um horário para cada nó da rede, escolhido aleatoriamente entre 7h30min e 9h30min, indicando o início diário do percurso casa-trabalho, permitindo a cada nó um atraso ou adiantamento de até quinze

minutos, calculado aleatoriamente a cada dia. Uma vez em seu local de trabalho, os nós permanecem na região durante oito horas seguidas. Após esse período, cada nó tem probabilidade de 80% de seguir direto para casa ou 20% para realizar alguma atividade noturna com duração de uma a três horas – em média uma vez por semana. Em casa, os nós permanecem até o horário de seguir novamente para o trabalho.

As regiões residenciais, comerciais e de atividades noturnas definidas no WDM (*Working Day Movement)* estão marcadas no mapa da Figura 7.1 da seguinte forma: as áreas numeradas de 1 a 4 identificam regiões residenciais, enquanto as áreas 5 e 6 identificam regiões comerciais, as áreas 7 e 8 identificam regiões de atividades noturnas. Como atualmente as pessoas tendem a viver em lugares mais afastados do centro das grandes cidades (região 6), os 300 carros utilizados nas simulações foram divididos em dois grupos de nós na proporção de 60% e 40%, respectivamente. Cada nó corresponde a um par veículo-motorista. O primeiro grupo reside nas regiões 1 ou 2, trabalha na região 6 e frequenta atividades noturnas na região 8. Já o segundo reside nas regiões 3 ou 4, trabalha na região 5 e frequenta atividades noturnas na região 7.

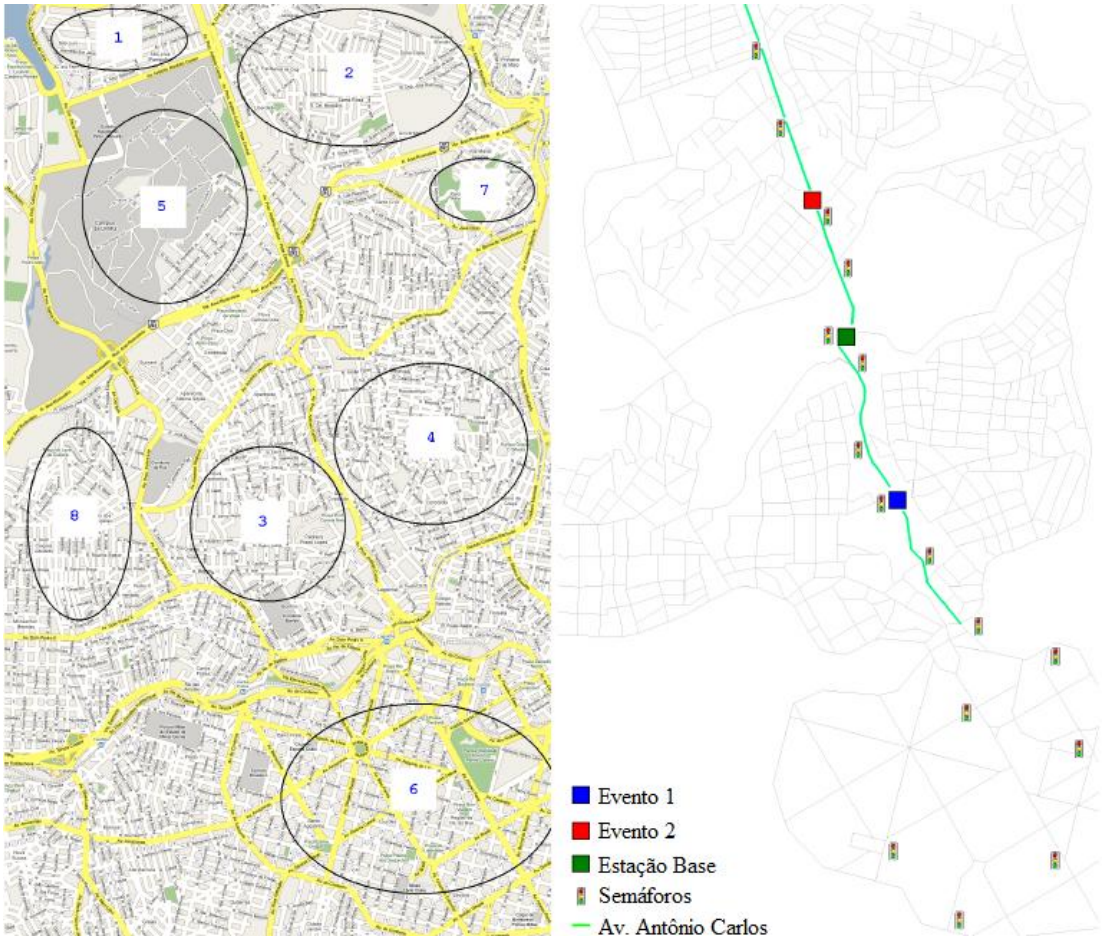

Figura 7.1. Cenário da comparação e representação no simulador [Paula, 2010].

Nos trajetos realizados dentro da rotina definida, os carros e ônibus se movem com velocidades entre 30km/h e 60km/h, valores que respeitam a velocidade máxima permitida nas avenidas de Belo Horizonte de 60km/h. Semáforos foram dispostos em alguns cruzamentos como mostrado na Figura 7.1, o que possibilita maiores oportunidades de contato entre os nós da rede.

Dois eventos foram simulados em dois locais diferentes identificados na Figura 7.1 como Evento 1 e Evento 2. O primeiro indica a existência de um congestionamento no sentido bairro-centro, o segundo indica um congestionamento no sentido centro-bairro. As probabilidades de ocorrência se baseiam no fato de que pela manhã existem mais veículos se deslocando no sentido bairro-centro, enquanto à tarde essa situação se inverte. As mensagens geradas informam se o trânsito está livre ou congestionado naquele ponto e expiram trinta minutos após sua criação. Cada teste foi executado repetidamente, no mínimo oito vezes, sendo alterada a semente geradora do padrão de mobilidade.

Tabela 7.2. Características do cenário e modelo de rede da comparação.

Área simulada	Aproximadamente 55 km^2
Tempo de simulação	20 dias úteis
Número de nós	300 carros e 6 ônibus
Velocidade dos nós	30 a 60 km/h
Modelo de mobilidade	*Working Day Movement* [Ekman, 2008]
Raio de alcance dos nós	200m (IEEE 802.11p)
Taxa de transmissão	1 Mbps
Nó da rede	Representa par veículo-motorista
Horário de início diário	07:30 às 09:30
Nós do grupo 1	Moradia: região 1 ou 2 Trabalho: região 6, Noite: região 8
Nós do grupo 2	Moradia: região 3 ou 4 Trabalho: região 5, Noite: região 7
Evento 1	Congestionamento bairro-centro
Evento 2	Congestionamento centro-bairro
Intrusos	Ataque de alarmes trocados
Percentual de amigos	10% dos nós da rede

A Tabela 7.2 resume as características do cenário e modelo de rede utilizado pelo RMDTV e na comparação. Os intrusos presentes na rede executam ataques de injeção de informação falsa (*bogus information*) [Wangham, 2014], ou seja, geram mensagens que informam impressões opostas àquelas por eles experimentadas. Assim há alarmes trocados, os intrusos informam a existência de um congestionamento em caso de tráfego livre e vice-versa. Se os intrusos atribuírem reputação a outros intrusos, tal comportamento influenciaria o mecanismo RMDTV, o que não acontece no modelo de confiança proposto.

7.3. Resultados e análise

Inicialmente, foi verificado o percentual de decisões tomadas com utilização dos mecanismos RMDTV e SNVC ao longo dos dias simulados. Enquanto o mecanismo anterior RMDTV inclui todas as informações recebidas para tomar decisões, o SNVC proposto no modelo de confiança utiliza mensagens apenas de usuários considerados confiáveis, ou seja, amigos ou amigos dos amigos. O percentual de amigos que cada nó possui na rede veicular foi estimado em 10% dos usuários da rede.

Posteriormente, foi calculado o tempo que seria reduzido com a certificação SNVC, que já toma decisão imediatamente ao receber mensagem de um usuário confiável, parte de sua rede social. Os resultados são apresentados nos gráficos a seguir com 95% para o intervalo de confiança.

Os primeiros dados coletados corresponderam ao percentual de decisões certas obtido com utilização da certificação SNVC proposta. A comparação desse percentual com a utilização do RMDTV demonstra o funcionamento do SNVC sob a execução de um ataque, no caso alarmes trocados. A tomada de decisões representa as diferenças entre SNVC e RMDTV, de forma que devem ser avaliados os percentuais de acertos e erros.

Na Figura 7.2 é observado o percentual a cada dia das decisões certas tomadas pelos nós da rede ao utilizarem, respectivamente, os mecanismos RMDTV e SNVC. A pequena diferença entre os percentuais de cada mecanismo é atribuída às decisões forçadas, que são utilizadas pelo mecanismo RMDTV quando não há critérios suficientes para decidir, mas o tempo esgotado obriga a tomar uma decisão. As decisões tomadas utilizando o SNVC refletem opiniões de amigos ou amigos de amigos, enquanto uma decisão forçada é baseada em apenas uma mensagem de origem duvidosa, que consequentemente tem maior chance de erro.

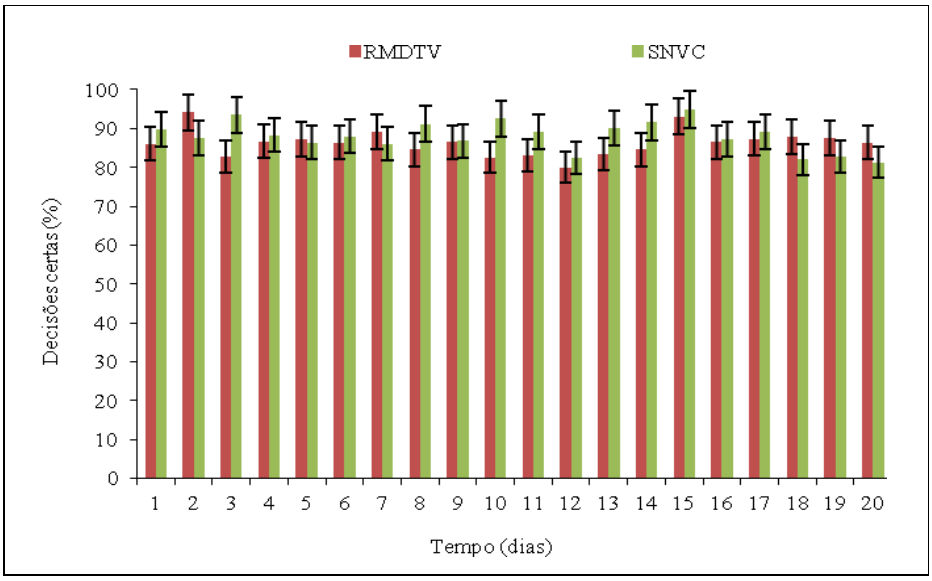

Figura 7.2. Decisões certas em relação ao total de mensagens recebidas.

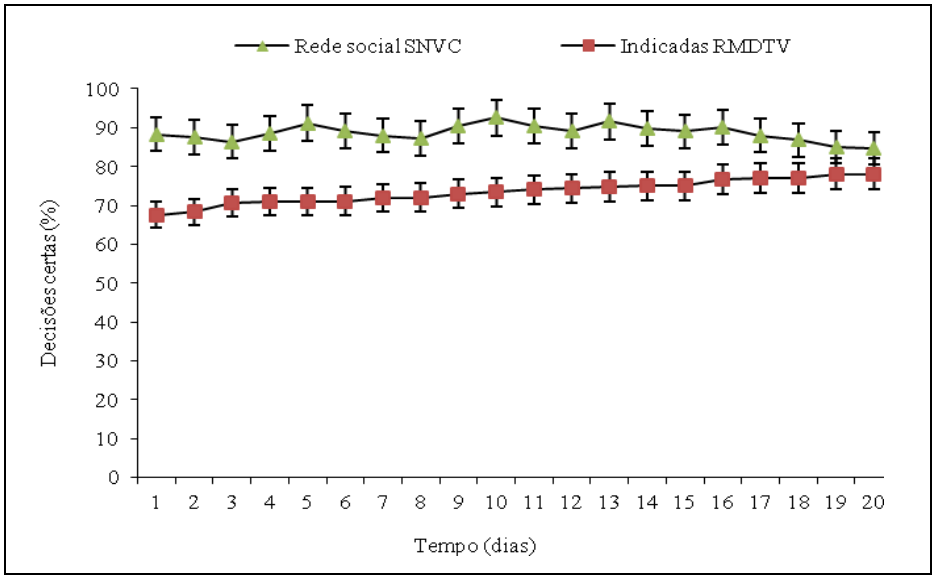

Figura 7.3. Decisões indicadas por RMDTV em relação a decisões da rede social.

Na Figura 7.3 observa-se o percentual de decisões certas comparando apenas as decisões indicadas pelo RMDTV com as mensagens relacionadas aos usuários confiáveis na rede social, que representam nesse caso os amigos e amigos dos amigos. Excluindo-se as decisões forçadas tomadas pelo RMDTV, tem-se a comparação mais precisa de suas decisões indicadas com o modelo de confiança proposto.

As decisões tomadas por indicação da rede social e certificação SNVC superam o percentual de decisões indicadas pelo RMDTV, sendo que o modelo de confiança ainda permite o reconhecimento por assinaturas de reputação. A diferença de até 20% das

decisões certas representa maior confiança nas decisões tomadas, o que agrega mais qualidade em relação ao algoritmo do mecanismo RMDTV. Esse último conhece os usuários da rede com o passar dos dias, o que faz melhorar suas decisões.

A Figura 7.4 mostra que o tempo gasto para tomar a decisão é menor quando a mensagem é da rede social com uso do SNVC, assim a origem confiável indica uma decisão imediata. No mecanismo RMDTV, há um número mínimo de informações recebidas para levar em conta a reputação. Nos gráficos são mostradas as decisões tomadas antes pelo SNVC a cada dia bem como o tempo médio reduzido, aproximadamente um minuto por decisão. As mensagens alcançam o usuário mais rápido devido à existência de vários caminhos no grafo da rede social proposta, pois há mais usuários confiáveis se o usuário tem mais amigos. O número de caminhos possíveis cresce também devido ao maior número de amigos dos amigos.

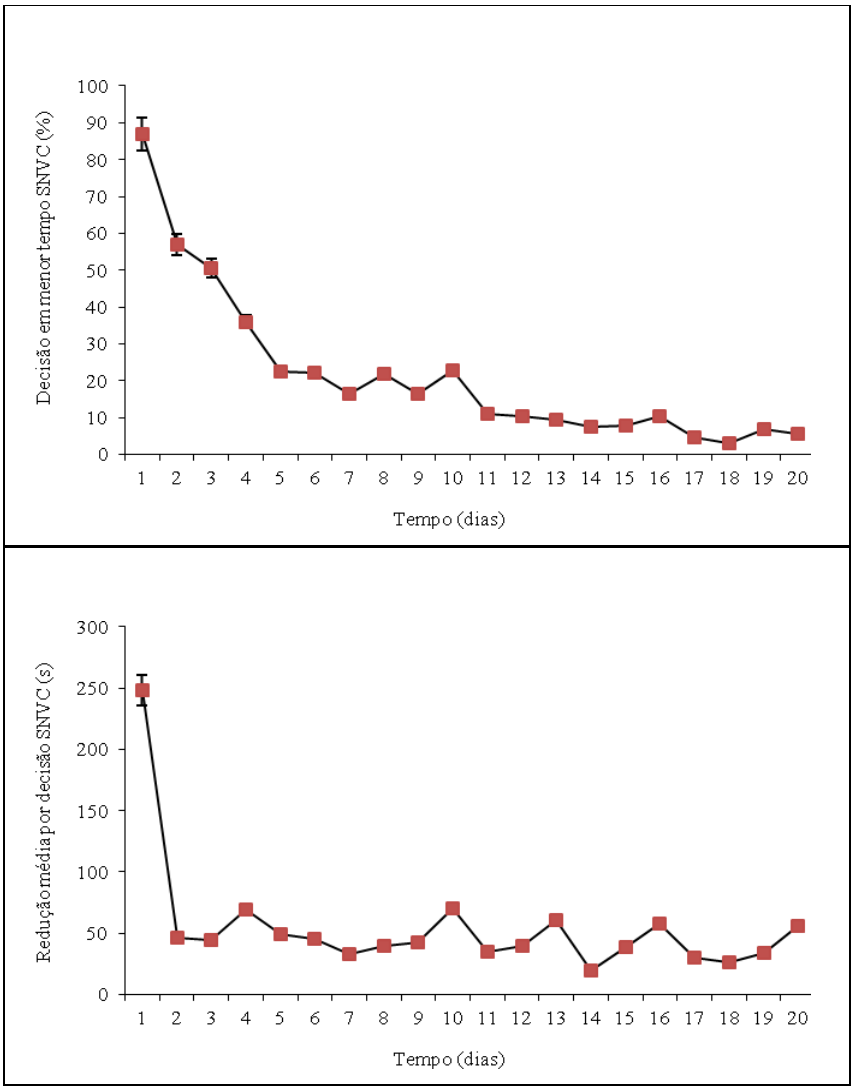

Figura 7.4. Redução de tempo para tomada de decisões.

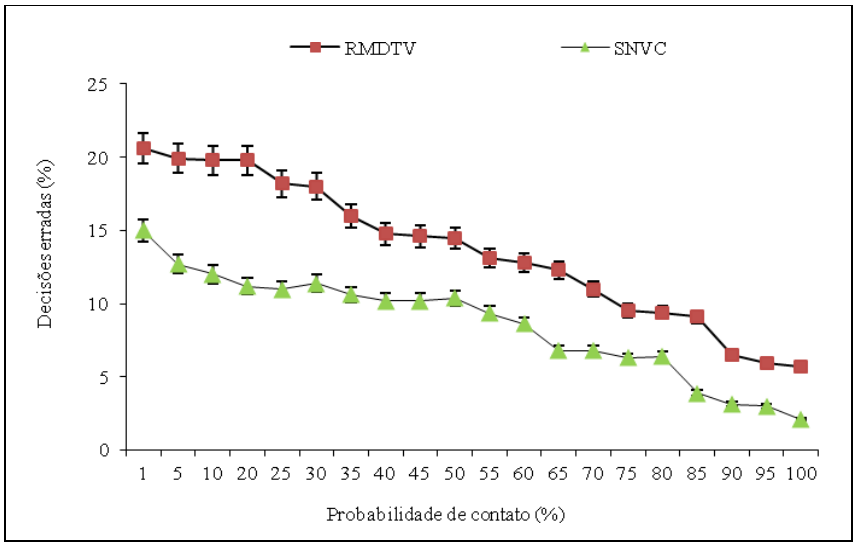

Figura 7.5. Decisões erradas em relação à probabilidade de contato entre usuários.

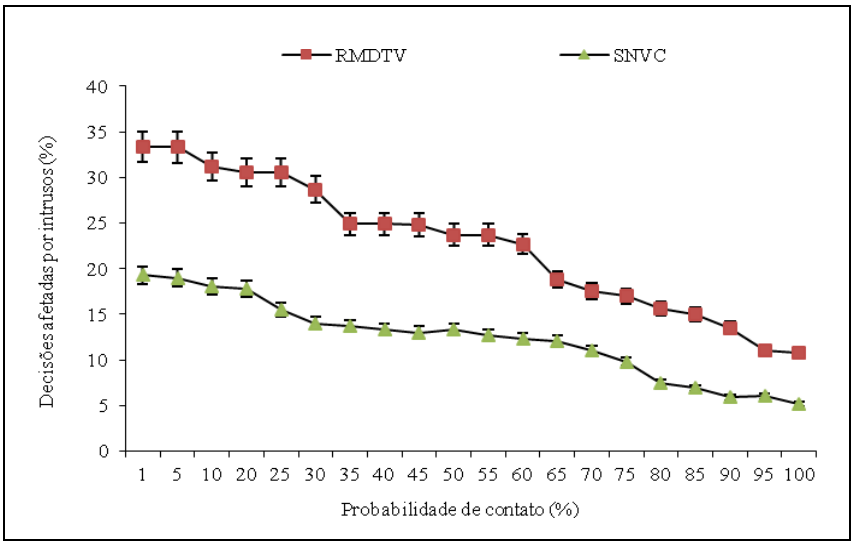

Figura 7.6. Decisões erradas afetadas por intrusos ou falsos positivos.

Na Figura 7.5 são observados os percentuais de decisões erradas tomadas pelos mecanismos, o que apresenta melhoria com o SNVC em relação ao RMDTV. Conforme citado, o risco de erro é menor quando se leva em conta apenas mensagens de usuários confiáveis do modelo de confiança em relação a decisões forçadas do RMDTV. A diminuição da chance de erro e do tempo necessário para tomada de decisão são vantagens de utilizar a seleção de mensagens confiáveis do modelo de confiança proposto.

Na Figura 7.6 é mostrado o impacto da presença de mais intrusos para decisões em cada mecanismo, com o aumento do percentual de intrusos de 10% anteriormente para 20% na avaliação com mesma probabilidade de contato diária. A presença de intrusos afeta

menos o SNVC em relação ao mecanismo RMDTV como foi observado, pois no modelo de confiança são consideradas confiáveis apenas mensagens de sua rede social.

A Figura 7.7 mostra a quantidade de mensagens consideradas confiáveis, incluindo as mensagens de reputação do modelo de confiança proposto. Apesar da restrição de mensagens recebidas a usuários confiáveis, o percentual observado diariamente foi superior às decisões indicadas pelo mecanismo RMDTV, o que representa um ganho na confiança das mensagens. A inclusão da reputação aumenta o percentual de mensagens confiáveis porque algum amigo de amigo pode atribuir um bônus para o certificado do usuário, que passa a ser confiável para quem recebe a mensagem que atribuiu reputação.

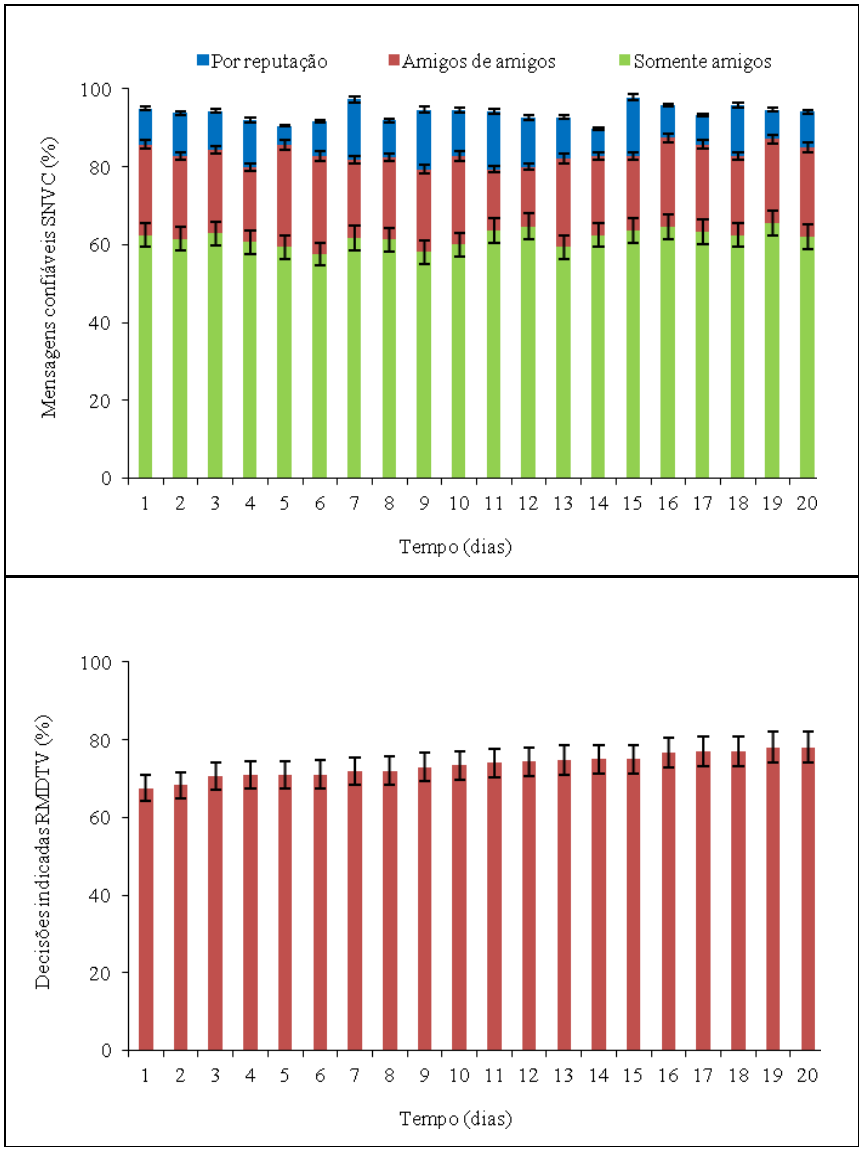

Figura 7.7. Mensagens confiáveis em relação às mensagens analisadas pelo RMDTV.

Ao final do período simulado de 20 dias úteis, cada um dos 300 usuários possuía em média 252 usuários confiáveis, incluindo amigos e amigos de amigos. Ainda foi alcançado um percentual de mensagens confiáveis de aproximadamente 95% das mensagens recebidas. As mensagens utilizadas para montagem da rede social foram equivalentes às 6.000 mensagens geradas a mais para reputação no mecanismo RMDTV e que não seriam necessárias para o modelo de confiança proposto neste trabalho.

A Tabela 7.3 sumariza a comparação realizada entre os mecanismos, mostrando os percentuais de melhoria do funcionamento do SNVC em relação ao RMDTV. Com 10% dos nós da rede representando amigos no modelo de confiança proposto, percebe-se vantagens em sua utilização quando comparado ao mecanismo RMDTV. Há redução no percentual de decisões erradas e no tempo para tomada de decisões, sem a necessidade de envolver uma autoridade certificadora.

Na rede social proposta, somente as mensagens confiáveis são utilizadas nas decisões, uma alternativa melhor que as decisões forçadas do RMDTV. Assim como no RMDTV as reputações são válidas por 30 dias [Paula, 2010], o período avaliado apresentou *overhead* semelhante e indicou que o SNVC utilize o mesmo critério para a reputação que seja válida por 30 dias, após esse prazo são então descartadas. No cenário do *trace* DieselNet (Seção 6.4), tal critério não representou alteração no percentual de mensagens confiáveis por reputação no período avaliado de 60 dias.

Tabela 7.3. Métricas e resultados qualitativos da comparação.

Métricas	**SNVC em relação ao RMDTV**
Decisões certas	Percentual semelhante
Decisões indicadas	Superior em 20 a 30%
Decisões erradas	Inferior em 5 a 15%
Falsos positivos	Inferior em cerca de 20%
Redução de tempo	Aproximadamente 50 s por decisão
Mensagens confiáveis	Aproximadamente 95% das recebidas
Overhead	Semelhante em número de mensagens

7.4. Conclusão

A utilização da certificação SNVC a partir do modelo de confiança proposto foi comparada ao mecanismo de reputação RMDTV. As avaliações realizadas mostram as vantagens da utilização do modelo de confiança proposto para tomada de decisões na rede veicular em relação ao uso de reputação.

Não houve variação significativa no percentual de decisões certas entre os dois mecanismos comparados, pois o SNVC entrega mensagens apenas de amigos ou amigos de amigos. Quanto maior o número de amigos que um usuário da rede possuir, maior a probabilidade de que uma mensagem recebida por ele seja reconhecida como confiável.

Quando se compara o percentual de decisões indicadas pelo mecanismo RMDTV, excluindo-se as decisões forçadas que não alcançaram um número mínimo de reputação, obtêm-se dados mais precisos para comparação com o modelo de confiança. A utilização da rede social é vantajosa em relação às decisões indicadas do RMDTV, pois o percentual de decisões certas devido a mensagens confiáveis no SNVC é superior ao percentual de decisões indicadas pelo RMDTV principalmente nos primeiros dias de utilização.

Os percentuais de decisões erradas tomadas pelos mecanismos ratificam a vantagem do modelo de confiança proposto, que representa menor possibilidade de erro na tomada de decisões em relação ao mecanismo RMDTV. Tal diferença é consequência do SNVC considerar apenas mensagens de usuários confiáveis, enquanto o algoritmo do RMDTV toma decisões forçadas quando não tem mensagens suficientes de reputação.

Além de representar aumento na qualidade das decisões tomadas, o modelo de confiança apresentou redução no tempo gasto para tomar decisões em relação ao tempo gasto pelo mecanismo RMDTV. A utilização da rede social como critério na seleção de mensagens foi considerada vantajosa, pois representou diminuição considerável no tempo médio para tomada de decisões e poucos segundos já são fundamentais para que um usuário evite um acidente.

Foi possível comparar nas simulações a utilização modelo de confiança com SNVC em relação ao mecanismo de reputação RMDTV, mostrando que o modelo proposto neste trabalho representa melhoria no percentual de decisões erradas e no tempo para tomada de decisões. Como não há necessidade de envolver uma autoridade certificadora, o modelo proposto demonstrou ser uma alternativa vantajosa ao gerenciamento de chaves em redes veiculares DTN, utilizando a certificação por meio de redes sociais.

Capítulo 8

Conclusões

Este trabalho apresenta o modelo de confiança proposto para segurança de redes veiculares tolerantes a interrupções, por meio da formação de redes sociais. Objetiva-se comunicação segura para troca de informações entre os veículos.

A proposta parte do relacionamento e conhecimento prévio dos usuários para estabelecer confiança em uma rede social. A utilização de certificados pelos próprios usuários possibilita o compartilhamento de chaves por meio de contato direto, entre duas pessoas que se conhecem e garantem sua identidade, que então assinam o certificado do outro mutuamente. Os certificados são validados por outros usuários que tenham a chave pública da assinatura disponível.

Além disso, o mecanismo de reputação possibilita também que usuários beneficiados possam gerar uma assinatura com bonificação positiva para identificar o outro certificado como um usuário confiável. As assinaturas propostas pelo modelo de confiança aumentam a probabilidade de o emissor das mensagens ser reconhecido como confiável, que é a situação exigida para que as mensagens sejam recebidas pelos usuários.

A comparação do modelo de confiança proposto com um mecanismo de reputação RMDTV anterior apresentou vantagens na utilização de certificados por meio de redes sociais em relação ao uso de apenas reputação para tomada de decisões. As decisões geradas por mensagens da rede social no SNVC resultam em menor taxa de erro e gastam menos tempo para serem tomadas que mensagens de reputação do RMDTV.

As avaliações utilizaram também *traces* reais de mobilidade de redes veiculares, que apresentam longos períodos sem conexões. Apesar da conectividade imprevisível em redes veiculares, verificou-se que não houve variação representativa na sobrecarga de mensagens da rede devido à utilização do modelo de confiança por redes sociais e que as mensagens de atualização de listas de amigos enviadas alcançam todos os usuários da rede social.

As análises realizadas demonstraram o impacto do modelo de confiança proposto na seleção das mensagens confiáveis. O número de mensagens entregues diminui, pois se restringe aos usuários confiáveis. Os resultados mostram vantagens de o usuário ter mais amigos, pois o número de caminhos no grafo do modelo de confiança proposto cresce também com mais amigos de amigos. Como inicialmente não existiam chaves para autenticação das mensagens, a certificação SNVC proposta representa uma alternativa ao gerenciamento de chaves baseando-se em uma rede social.

8.1. Contribuições

As contribuições deste trabalho são destacadas no aumento da segurança em redes tolerantes a interrupções (DTN) e especificamente no cenário de redes veiculares, ao propor um mecanismo de segurança que estabelece a confiança entre os usuários por meio de redes sociais. O modelo de confiança proposto permite a autenticação em redes vDTN por estabelecer confiança para comunicação segura. As questões de pesquisa levantadas na Seção 1.2 tiveram as seguintes contribuições:

- Como definir a confiança dos usuários em redes sem conectividade? O modelo proposto define critérios de confiança para usuários mesmo que não tenham conectividade, com adaptação do PGP para DTN.
- Como estabelecer graus de confiança e reputação para trocas de mensagens? Foram definidos graus de confiança de acordo com o modelo de relacionamento proposto que inclui reputação enviada por amigos e amigos de amigos.
- Como realizar a autenticação em redes vDTN? O modelo de confiança proposto inclui a certificação SNVC para autenticação em vDTN, provendo comunicação segura.
- Como gerenciar e compartilhar chaves em redes DTN? A rede social proposta no modelo de confiança permite a troca de material criptográfico. Assim, SNVC é uma alternativa ao gerenciamento de chaves com tolerância a interrupções, que pode ser aplicado em outras redes DTN no futuro.

O modelo de confiança propõe diferentes tipos de assinaturas que permitem o reconhecimento do certificado enviado junto com as mensagens dos usuários. Essas

assinaturas representam graus de confiança de acordo com o relacionamento entre os usuários da rede veicular, incluindo amigos de amigos e amigos por reputação.

Ao estabelecer graus de confiança para trocas de mensagens, são definidos critérios de confiança dos usuários em redes sem conectividade. Por não haver muitas referências nesse campo de pesquisa, as definições do comportamento de usuários na rede social são importantes contribuições. Por meio dessas definições, foi possível conceber a certificação SNVC para gerenciar e compartilhar chaves criptográficas em redes DTN, baseado na interação dos usuários que escolhem seus amigos e consequentemente tem acesso aos amigos dos amigos, o que possibilita a obtenção de um nível maior de segurança para redes veiculares.

As aplicações que adotarem o modelo de confiança proposto não devem depender de processamento do usuário, que receberá mensagens apenas de usuários confiáveis e será informado também do grau de confiança desse usuário. A utilização de mecanismos de segurança integrados a redes sociais, de forma implícita para o usuário, é uma proposta inovadora na abordagem de problemas relacionados à segurança em redes DTN. A concepção e a implementação desta proposta podem ser referência para outros trabalhos.

O modelo de confiança proposto foi avaliado por meio de simulações, comprovando o baixo impacto na entrega de mensagens e mostrando que a seleção de mensagens confiáveis favorece a disseminação de informações nas redes veiculares. A comparação com o mecanismo RMDTV demonstrou vantagens do modelo de confiança, servindo de base para novos mecanismos de reputação em redes DTN sem a presença de autoridade certificadora.

A utilização de *traces* reais de mobilidade de redes veiculares na avaliação deste trabalho pode tornar-se referência para trabalhos de pesquisa também em redes DTN que realizem simulações para a avaliação de propostas futuras. Os *traces* reais agregam valor às avaliações pelo menor controle dos parâmetros das simulações e movimento dos nós da rede veicular, possibilitando uma análise mais realística da proposta.

Este trabalho foi publicado (*SNVC: Social Networks for Vehicular Certification*) na revista *Computer Networks* para "*Special Issue on Cyber-Physical Systems for Mobile Opportunistic Networking*" 2016. As principais contribuições e parte dos resultados deste trabalho de tese foram publicados no 10º IEEE WiMob 2014, "*Social Networks for Certification in Vehicular Disruption Tolerant Networks*" [Oliveira, 2014]. Os resultados iniciais foram publicados no SBRC 2013, "Certificados Sociais para Segurança em Redes Veiculares Tolerantes a Interrupções" [Oliveira, 2013].

8.2. Trabalhos futuros

Para continuidade deste trabalho, espera-se a adaptação do modelo de confiança proposto de acordo com a configuração inicial dos veículos e possível integração com outras redes sociais como o *Facebook*. A certificação por meio de redes sociais pode ser ampliada para redes veiculares híbridas e DTN em geral, mediante avaliações. O que se aplica também a novos conceitos e pesquisas que porventura alterem características das redes vDTN.

Propõe-se ainda a implementação de um aplicativo que ofereça aos usuários o modelo de confiança por meio de redes sociais, que funcionará em ambiente *Android*. A disponibilização gratuita desse aplicativo obterá dados em grande escala que relacionem redes sociais e redes veiculares em ambiente real. A avaliação pretende relacionar os encontros e contatos oportunísticos à probabilidade desses usuários serem amigos na rede social, obtendo assim um grafo de relacionamento mais real.

Como exemplo de aplicação que utilize o modelo de confiança proposto, deve-se oferecer opções aos usuários para enviar áudios com informações para que sua rede social possa ouvir a mensagem de voz acompanhada do seu grau de confiança. A aplicação não deve depender de processamento do usuário para evitar sobrecarga de mensagens e atraso na tomada de decisões. Quando o veículo estiver parado ou num congestionamento, o motorista pode informar num mapa detalhes do evento e situação atual no local onde se encontra. Além disso, o motorista pode atribuir reputação para qualificar informações recebidas e sensores podem enviar mensagens automáticas sobre seu deslocamento.

Referências Bibliográficas

Almiron, M. G.; Ramos, H. S.; Oliveira, E. M. R.; Menezes, J. G. M.; Guidoni, D. L.; Vaz de Melo, P. O. S.; Cunha, F. D.; Aquino, A. L. L.; Mini, R. A. F.; Frery, A. C. & Loureiro, A. A. F. (2010). *Redes complexas na modelagem de redes de computadores.* Minicursos do Simpósio Brasileiro de Redes de Computadores, SBRC 2010, pp. 1–46.

Alves, R. S.; Campbell, I. V.; Couto, R. S.; Campista, M. E. M.; Moraes, I. M.; Rubinstein, M. G.; Costa, L. H. M. K.; Duarte, O. C. M. B. & Abdalla, M. (2009). *Redes Veiculares: Princípios, Aplicações e Desafios.* Minicursos do Simpósio Brasileiro de Redes de Computadores, SBRC 2009, pp. 199-254.

Asokan, N.; Kostiainen, K.; Ginzboorg, P.; Ott, J.; Luo, C. (2007). *Applicability of identity-based cryptography for disruption-tolerant networking*. In Proceedings of the International MobiSys workshop on Mobile opportunistic networking (MobiOpp). ACM, Nova Iorque, EUA, pp. 52-56.

Benamar, N.; Singh, K. D.; Benamar, M.; El Ouadghiri, D.; Bonnin, J.-M. (2014). *Routing protocols in Vehicular Delay Tolerant Networks: A comprehensive survey*. Computer Communications. Elsevier, Vol. 48, Julho 2014, pp. 141-158.

Benevenuto, F.; Rodrigues, T.; Cha, M. & Almeida, V. (2009). *Characterizing user behavior in online social networks.* In Proceedings of the ACM SIGCOMM Internet Measurement Conference, pp. 49-62.

Bhutta, M. N. M.; Cruickshank, H. S.; Sun, Z. (2014). *An Efficient, Scalable Key Transport Scheme (ESKTS) for Delay/Disruption Tolerant Networks*. Wireless Networks. Vol. 20, No. 6, Agosto 2014, pp. 1597-1609.

Biswas, S.; Tatchikou, R. & Dion, F. (2006). *Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety.* IEEE Communications Magazine, Volume 44, No. 1, pp. 74-82.

Buchegger, S. & 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.; Bissias, G.; Corner, M. D. & Levine, B. N. (2007). *Surviving Attacks on Disruption-Tolerant Networks without Authentication.* ACM International Symposium on Mobile Ad Hoc Networking and Computing.

Burgess, J.; Gallagher, B.; Jensen, D.; Levine, B. N. (2006). *MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networking*. In Proceedings of IEEE Infocom 2006. vol. 6. Barcelona, Espanha, 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 ACM International Workshop on Vehicular Ad Hoc Networks, pp. 19-28, Nova Iorque, EUA.

Caliskan, M.; Graupner, D. & Mauve, M. (2006). *Decentralized discovery of free parking places.* In VANET' 06: Proceedings of the ACM International Workshop on Vehicular Ad Hoc Networks, pp. 30-39, Nova Iorque, EUA.

Capkun, S.; Buttyan, L. & Hubaux, J.-P. (2003). *Self-organized public-key management for mobile ad hoc networks.* IEEE Transactions on Mobile Computing, vol. 2, no. 1, pp. 52-64.

Cavalcanti, S. R.; Campista, M. E. M.; Abdesslem, F. B.; Costa, L. H. M. K. & Amorim, M. D. (2008). *VEER: Um algoritmo de seleção de pares em redes ad hoc veiculares.* Simpósio Brasileiro de Redes de Computadores.

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

Cerf, V.; Burleigh, S.; Hooke, A.; Torgerson, L.; Durst, R.; Scott, K.; Travis, E. & Weiss, H. (2001). *Interplanetary Internet (IPN): Architectural Definition.* Relatório Técnico, IPN Research Group.

Chaintreau, A.; Hui, P.; Crowcroft, J.; Diot, C.; Gass, R. & Scott, J. (2006). *Impact of Human Mobility on the Design of Opportunistic Forwarding Algorithms.* IEEE International Conference on Computer Communications (INFOCOM).

Chaintreau, A.; Mtibaa, A.; Massoulie, L.; Diot, C. (2007). *The Diameter of Opportunistic Mobile Networks.* In Proceedings of the 2007 ACM CoNEXT Conference, pp. 1-12.

Chang, E.; Dillon, T. & Hussain, F. (2006). *Trust and reputation for service-oriented environments: Technologies for building business intelligence and consumer confidence*. 1a. edição. West Sussex, England: John Wiley and Sons.

Chen, L. J.; Yu, C. H.; Sun, T.; Chen, Y. C. & Chu H. H. (2006). *A hybrid routing approach for opportunistic network*. ACM Special Interest Group on Data Communication.

Chen, R.; Bao, F.; Chang, M.; Cho, J. H. (2014). *Dynamic trust management for delay tolerant networks and its application to secure routing.* IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 5, pp. 1200-1210.

Chen, W. & Cai, S. (2005). *Ad hoc peer-to-peer network architecture for vehicle safety communications*. IEEE Communications Magazine, Vol. 43, No. 4, pp. 100-107.

CTA - Chicago Transit Authority. (2010). *Bus Tracker API (Online)*. Disponível em: http://www.transitchicago.com/developers/bustracker.aspx. Acessado em 16/07/2015.

Conti, M. & Giordano, S. (2014). *Mobile ad hoc networking: milestones, challenges, and new research directions*. IEEE Communications Magazine, vol. 52, no. 1, pp. 85-96.

Corner, M.; Levine, B. & Brian, L. (2011). *A Mobility Testbed - UMass DOME*. Disponível em http://prisms.cs.umass.edu/dome/. Acessado em 12/05/2015.

Crawdad (2015). *A community resource for archiving wireless data at dartmouth*. Disponível em http://crawdad.cs.dartmouth.edu/. Acessado em 23/03/2015.

Cunha, F. D.; Vianna, A.C.; Mini, R. A. F.; Loureiro, A. A. F. (2013). *"How effective is to look at a vehicular network under a social perception?"* - In IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).

Cunha, F. D.; Vianna, A.C.; Mini, R. A. F.; Loureiro, A. A. F. (2014). *"Are Vehicular Networks Small World?"* - In 33rd Annual IEEE International Conference on Computer Communications (INFOCOM'14) - Workshop for Students.

Cutillo, L.; Molva, R.; Strufe, T. (2009). *Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust*. IEEE Communications Magazine, vol. 47, no. 12, pp. 94–101.

Daeinabi, A. e Rahbar, A. G. (2013). *Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks*. Multimedia tools and applications. Springer, vol. 66, no. 2, pp. 325–338.

Daly, E. M. & Haahr, M. (2007). *Social network analysis for routing in disconnected delay-tolerant manets.* In MobiHoc'07: ACM international symposium on Mobile ad hoc networking and computing, pp. 32-40.

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.

Di Pietro, R.; Guarino, S.; Verde, N. V.; Domingo-Ferrer, J. (2014). *Security in wireless ad-hoc networks - A survey*. Computer Communications. Elsevier, vol. 51, Setembro 2014, pp. 1-20.

Dini, G.; Duca, A. L. (2012). *Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network.* Ad-Hoc Networks. Elsevier, vol. 10, no. 7, pp. 1167-1178.

Djamaludin, Chris, Foo, Ernest, & Corke, Peter. (2013), *Establishing initial trust in autonomous delay tolerant networks without centralised PKI*. Computers & Security. Vol. 39, Part B, pp. 299–314.

Doering, M.; Pögel, T.; Pöttner, W. & Wolf, L. C. (2010). *A New Mobility Trace for Realistic Large-Scale Simulation of Bus-based DTNs*. In ACM MobiCom 2010 - Workshop on Challenged Networks (CHANTS), Chicago, EUA.

Durst, R. C. (2002). *An infrastructure security model for delay tolerant networks.* Disponível em http://www.dtnrg.org/wiki/Docs. Acessado em 12/03/2015.

Ekman, F.; Keränen, A.; Karvo, J. & Ott, J. (2008). *Working Day Movement Model.* In Proceedings of ACM SIGMOBILE Workshop on Mobility Models.

Engel, T.; Fischer, D.; Scherer, T. & Dagmara Spiewak, D. (2006). *A Survey on Security Challenges in Next Generation Mobile Networks.* International Conference on Mobile Computing and Ubiquitous Networking.

Engoulou, R. G.; Bellaïche, M.; Pierre, S.; Quintero, A. (2014). *VANET security surveys.* Computer Communications. Elsevier, Vol. 44, Maio 2014, pp. 1-13.

Fall, K. (2003). A Delay-Tolerant Network Architecture for Challenged Internets. *In Proceedings of ACM Special Interest Group on Data Communication*, pp. 27-34. SIGCOMM, Agosto 2003. Winner of SIGCOMM 2013 Test of Time Paper Award.

Fall, K. (2004). *Messaging in difficult environments.* Relatório Técnico IRB-TR-04-019, Intel Research Berkeley.

Fall, K. (2005). *Disruption tolerant networking for heterogeneous ad-hoc networks*. IEEE Military Communications Conference (MILCOM).

Farrell S. & Cahill, V. (2006). *Delay- and Disruption-Tolerant Networking.* Artech house, Londres.

FCC (2006) *FCC Report and Order 06-110: Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band*. Julho 2006.

Fernandes, N. C.; Moreira, M. D. D. et al. (2006). *Ataques e Mecanismos de Segurança em Redes Ad Hoc*. Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg), cap. 2, pp. 49-102.

Fernandes, N. C. & Duarte, O. C. M. B. (2008). *An Efficient Group Key Management for Secure Routing in Ad Hoc Networks.* IEEE Globecom 2008 Computer and Communications Network Security Symposium (GC'08 CCNS), EUA, pp. 1-5.

Fernandes, C. P.; Wangham, M.; Mello, E.; Simas, I. (2015). *RS4VANETs A Decentralized Reputation System for Assessing the Trustworthiness of Nodes in Vehicular Networks*. In Proceedings of International Wireless Communications & Mobile Computing Conference - IWCMC 2015, Croácia, pp. 268-273.

Gakenheimer, R. (1999). *Urban mobility in the developing world*. Elsevier Transportation Research Part A: Policy and Practice, vol. 33, no. 7-8, pp. 671-689.

Gansen, T.; Wischhof, L. & Ebner, A. (2008). *Car-2-X challenges- dreams and nightmares*. In Secure Vehicular Communications Workshop: Results and Challenges.

Gerla, M.; Kleinrock, L. (2011). *Vehicular networks and the future of the mobile internet*. Computer Networks, Elsevier, Volume 55, no. 2, pp. 457-469, Fevereiro 2011.

Golbeck, J. (2006). *Computing with Trust: Definition, Properties, and Algorithms*. Securecomm and Workshops - Security and Privacy for Emerging Areas in Communications Networks, Baltimore, pp. 1-7.

Grandison, T. & Sloman, M. (2000). *A survey of trust in internet applications*. In IEEE Communications Surveys e Tutorials, Vol. 3, No. 4, pp. 2-16.

Gray, E.; Seigneur, J.-M.; Chen, Y.; Jensen. C. (2003). *Trust Propagation in Small Worlds*. Chapter of Trust Management. Volume 2692 da série Lecture Notes in Computer Science, Springer, pp. 239-254.

Guidoni, D. L.; Boukerche, A.; Villas, L. A.; Souza, F. S.; Mini, R. A. & Loureiro, A. A. (2012). *A framework based on small world features to design HSNs topologies with QoS*. In IEEE International Symposium on Computers and Communications.

Guo, S.; Falaki, M. H.; Oliver, E. A.; Rahman, S.; Seth, A.; Zaharia, M. A.; Keshav, S. (2007). *Very Low-Cost Internet Access Using KioskNet*. ACM SIGCOMM Computer Communication Review, Volume 37, No. 5, Outubro 2007, pp. 95-100.

Guo, M.; Ammar, M. H. & Zegura, E. W. (2005). *V3: a vehicle-to-vehicle live video streaming architecture*. In IEEE International Conference on Pervasive Computing and Communications (PerCom).

Hu, Y. C.; Perrig, A. & Johnson, D. B. (2003). *Rushing Attacks and Defense in Wireless Ad Hoc Network*. IEEE International Conference on Web Information Systems Engineering.

Huang, Z.; Ruj, S.; Cavenaghi, M. A.; Stojmenovic, M.; Nayak, A. (2014). *A social network approach to trust management in VANETs*. Peer-to-Peer Networking and Applications. Volume 7, no. 3, pp. 229-242, Setembro 2014.

Huang, Z.; Ruj, S.; Cavenaghi, M.; Nayak, A. (2011). *Limitations of trust management schemes in VANET and countermeasures*. IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pp. 1228-1232, Setembro 2011.

Hui, Pan et al. (2005). *Pocket Switched Networking: Challenges, feasibility and implementation issues*. Workshop on Autonomic Communication. Springer Berlin Heidelberg, pp. 1-12.

Hui, P. Crowcroft, J. & Yoneki, E. (2008). *Bubble rap: social-based forwarding in delay tolerant networks*. In Proceedings of MobiHoc 2008, pp. 241–250.

IEEE (2013). *IEEE standard for wireless access in vehicular environments security services for applications and management messages*. IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006), pp. 1–289.

IEEE 802.11p (2010). *Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications - Amendment 6: Wireless Access in Vehicular Environments*. Julho 2010, http://www.ietf.org/mail-archive/web/its/current/pdfqf992dHy9x.pdf

IPCAS Lab. (2016). *Mobile Ad-Hoc and DTN Networks at IPCAS Lab*. Disponível em: http://www.ece.gatech.edu/research/labs/WCCL/DTN2.html, acessado em 30/05/2016.

Jagadale, P. S., & Jawalkar, P. (2015). *Misbehavior Packet Detection Approach using Effective Trust in Delay-Tolerant Networks.* International Journal of Science and Research (IJSR). Vol. 4, No. 6, Junho 2015, pp. 2644-2649.

Jamalipour, A.; Ma, Y. (2011). *Intermittently Connected Mobile Ad Hoc Networks.* Springer-Verlag Nova Iorque.

Jetcheva, J.; Hu, Y.; PalChaudhuri, S.; Saha, A.; Johnson, D. (2003). *Design and evaluation of a metropolitan area multitier wireless ad hoc network architecture*. In Fifth IEEE Workshop on Mobile Computing Systems and Applications, pp. 32-43.

Jia Z.; Lin, X.; Tan, S. H.; Li, L. & Yang, Y. (2012). *Public key distribution scheme for delay tolerant networks based on two-channel cryptography.* Journal of Network and Computer Applications, Elsevier. Vol. 35, No. 3, pp. 905-913.

Jiang, C.-J.; Chen, C.; Chang, J.-W.; Jan, R.-H. & Chiang, T. C. (2009*). Construct small worlds in wireless networks using data mules.* In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pp. 28-35.

Jiang, D. & Delgrossi, L. (2008). *IEEE 802.11p: Towards an international standard for wireless access in vehicular environments*. In IEEE Vehicular Technology Conference (VTC-Spring).

Jiangyi, H.; Burmester, M. (2009). *Cooperation in Mobile Ad Hoc Networks*. Chapter of Guide to Wireless Ad Hoc Networks. Parte da série Computer Communications and Networks, Springer, pp 43-57.

Johnson, D.; Menezes, A. e Vanstone, S. A. (2001). The elliptic curve digital signature algorithm (ecdsa). International Journal of Information Security. Agosto 2001, Vol. 1, No. 1, pp. 36-63.

Jones, E. P. C.; Li, L.; Ward, P. A. S. (2005). *Practical routing in delay-tolerant networks.* ACM SIGCOMM Workshop on Delay-tolerant Networking.

Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K. & Weil, T. (2011). *Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions.* IEEE Communications Surveys & Tutorials. Vol. 13, No. 4, pp. 584-616.

Kargl, F.; Papadimitratos, P.; Buttyan, L.; Muter, M. et. al. (2008). *Secure vehicular communication systems: implementation, performance, and research challenges.* IEEE Communications Magazine, Vol. 46, No. 11, pp. 110-118.

Kate, A.; Zaverucha, G. M. & Hengartner, U. (2007). *Anonymity and Security in Delay Tolerant Networks.* International Conference on Security and Privacy in Communication Networks.

Keranen, A.; Ott, J. & Kärkkäinen, T. (2009). *The ONE Simulator for DTN Protocol Evaluation*. ACM International Conference on Simulation Tools and Techniques.

Lee, K.; Lee, S.-H.; Cheung, R.; Lee, U. & Gerla, M. (2007). *First experience with CarTorrent in a real vehicular ad hoc network testbed.* In Mobile Networking for Vehicular Environments (MOVE).

Lequerica, I.; Longaron, M. G.; Ruiz, R. M. (2010). *Drive and Share: Efficient Provisioning of Social Networks in Vehicular Scenarios*. IEEE Communications Magazine, vol. 48, no. 11, Novembro 2010, pp. 90-97.

Li, Q.; Malip, A.; Martin, K. M.; Ng, S.-L.; Zhang, J. (2012). *A reputation-based announcement scheme for VANETs.* IEEE Transactions on Vehicular Technology, vol. 61, no. 9, pp. 4095-4108.

Li, C.-T.; Hwang, M.-S.; Chu, Y.-P. (2008). *A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks.* Computer Communications. Elsevier, vol. 31, pp. 2803-2814.

Liang, X.; Lin, X.; Shen, X. (2013). *Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks*. IEEE Trans. Parallel and Distributed Systems.

Liang, X.; Zhang, K.; Shen, X.; Lin, X. (2014). *Security and privacy in mobile social networks: challenges and solutions*. IEEE Wireless Communications, vol.21, no.1, pp. 33-41, Fevereiro 2014.

Liu, H. & Qiu, Y. (2007). *A Reputation Model based on Transactions in Peer-to-Peer Networks*. In IEEE International Conference on Semantics, Knowledge and Grid, Shan Xi, pp. 398-401.

Liu, X.; Li, Z.; Li, W.; Lu, S.; Wang, X. & Chen, D. (2012). *Exploring social properties in vehicular ad hoc networks.* In Proceedings of ACM Fourth Asia-Pacific Symposium on Internetware, Nova Iorque, EUA. ACM.

Lu, N.; Luan, T. H.; Wang, M.; Shen, X.; Bai, F. (2014). *Bounds of asymptotic performance limits of social-proximity vehicular networks.* IEEE/ACM Transactions on Networking, vol. 22, no. 3, pp. 812-825, Junho 2014.

Lu, R.; Lin, X.; Shen, X. (2010). *SPRING: A Social-based Privacy-preserving Packet Forwarding Protocol for Vehicular Delay Tolerant Networks.* In proceedings of IEEE INFOCOM 2010, pp.1-9, Março 2010.

Luan, T.; Lu, R.; Shen, X.; Bai, F. (2015). *Social on the road: enabling secure and efficient social networking on highways*. IEEE Wireless Communications, vol.22, no.1, pp. 44-51, Fevereiro 2015.

Luo, P.; Huang, H.; Shu, W.; Li, M.; Wu, M. (2008). *Performance Evaluation of Vehicular DTN Routing under Realistic Mobility Models*. In IEEE Wireless Communications and Networking Conference (WCNC).

Lv, X.; Mu, Y.; Li, H. (2014). *Non-Interactive Key Establishment for Bundle Security Protocol of Space DTNs*. IEEE Transactions on Information Forensics and Security, vol. 9, no. 1, pp. 5-13, Janeiro 2014.

Macedo, D. F.; Oliveira, S.; Teixeira, F. A.; Aquino, A. L. L. & Oliveira, R. R. (2012). *$(CIA)^2$-ITS: Interconnecting Mobile and Ubiquitous Devices for Intelligent Transportation Systems.* In IEEE Pervasive Computing and Communication (PerCom).

Maaroufi, S. & Pierre, S. (2014). *Vehicular social systems: an overview and a performance case study*. In Proceedings of the ACM international symposium on Development and analysis of intelligent vehicular networks and applications (DIVANet '14). ACM, Nova Iorque, EUA, pp. 17-24.

Malhotra, Y. (2014). *Quantitative Modeling of Trust and Trust Management Protocols in Next Generation Social Networks Based Wireless Mobile Ad Hoc Networks*. Acessado em 30/04/2015. Disponível no portal SSRN: http://ssrn.com/abstract=2539180

Marmol, F. G. & Perez, G. M. (2012). *Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks*. Journal of Network and Computer Applications, vol. 35, no. 3, pp. 934-941.

Minhas, U.; Zhang, J.; Tran, T.; Cohen, R. (2010). *Intelligent agents in mobile vehicular ad-hoc networks: leveraging trust modeling based on direct experience with incentives for honesty*. IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, pp 243-247.

Mitropoulos, G. K. et al. (2010). *Wireless Local Danger Warning: Cooperative Foresighted Driving Using Intervehicle Communication*. In IEEE Transactions on Intelligent Transportation Systems, vol. 11, no. 3, pp. 539-553.

Mota, V. F. S.; Silva, T. H. & Nogueira, J. M. S. (2009). *Introduzindo Tolerância a Interrupção em Redes Ad Hoc Móveis para Cenários de Emergência.* Simpósio Brasileiro de Redes de Computadores.

Nadeem, T.; Dashtinezhad, S.; Liao, C. & Iftode, L. (2004). *Traffic-View: traffic data dissemination using car-to-car communication*. ACM SIGMOBILE Mobile Computing and Communications Review, Vol. 8, No. 3, pp. 6-19.

NASA Tournament Lab. (2014). *NASA's Disruption Tolerant Networking Challenge Series.* http://www.topcoder.com/dtn/security/, acessado em 19/12/2014.

Naumov, V.; Baumann, R. & Gross, T. (2006). *An Evaluation of Inter-Vehicle Ad Hoc Networks Based on Realistic Vehicular Traces*. In Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'06).

Nogueira, M.; Silva, E.; Albini, L.; Santos, A. L. (2011). *Survivable key management on WANETs*. IEEE Wireless Communications, v. 18, p. 82-88.

Oliveira, C. T.; Moreira, M. D. D.; Rubinstein, M. G.; Costa, L. H. M. K. & Duarte, O. C. M. B. (2007). *Redes Tolerantes a Atrasos e Desconexões*. Minicursos do Simpósio Brasileiro de Redes de Computadores, pp. 203-256.

Oliveira, S.; Oliveira, T. R. & Nogueira, J. M. S. (2008). *Um Modelo de Gerenciamento de Segurança em Redes de Sensores Sem Fio*. Simpósio Brasileiro de Redes de Computadores.

Oliveira, T. R.; Oliveira, S. & Nogueira, J. M. S. (2010). *Modelo de Gerenciamento de Segurança Adaptativo para Redes de Emergência.* Simpósio Brasileiro de Redes de Computadores.

Oliveira, T. R.; Oliveira, S.; Macedo, D. F. & Nogueira, J. M. S. (2013). *Certificados Sociais para Segurança em Redes Veiculares Tolerantes a Interrupções.* Simpósio Brasileiro de Redes de Computadores.

Oliveira, T. R.; Oliveira, S.; Macedo, D. F. & Nogueira, J. M. S. (2014). *Social Networks for Certification in Vehicular Disruption Tolerant Networks.* IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 391-398.

Ott, J.; Kutscher, D. & Dwertmann, C. (2006). *Integrating DTN and MANET routing.* In Proceedings of SIGCOMM workshop on Challenged networks, pp. 221-228.

Panayappan, R.; Trivedi, J.; Studer, A. & Perrig, A. (2007). *VANET-based approach for parking space availability.* In ACM International Workshop on Vehicular Ad Hoc Networks.

Papadimitratos, P.; Buttyan, L.; Holczer, T.; Schoch, E.; Freudiger, J.; Raya, M.; Ma, Z.; Kargl, F.; Kung, A. & Hubaux, J. P. (2008). *Secure vehicular communication systems: design and architecture.* IEEE Wireless Communications Magazine, Vol. 46, No. 11, pp. 100-109.

Papadimitratos, P.; Calandriello, G.; Hubaux, J.-P. & Lioy A. (2009) *Impact of Vehicular Communication Security on Transportation Safety.* IEEE INFOCOM Mobile Networking for Vehicular Environments.

Paula, W. P.; Oliveira, S. & Nogueira, J. M. S. (2010). Um Mecanismo de Reputação para Redes Veiculares Tolerantes a Atrasos e Desconexões. Simpósio Brasileiro de Redes de Computadores.

Pereira, P. R.; Casaca, A.; Rodrigues, J. J. P. C.; Soares, V. N. G. J.; Triay, J.; Pastor, C. C. (2012). *From Delay-Tolerant Networks to Vehicular Delay-Tolerant Networks.* IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 1166-1182.

Portmann, M. & Pirzada, A. A. (2008). *Wireless Mesh Networks for Public Safety and Crisis Management Applications*. IEEE Internet Computing, Vol. 12, No. 1, pp. 18-25.

Qianhong, W.; Domingo-Ferrer, J.; Gonzalez-Nicolas, U. (2010). *Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications*. IEEE Transactions on Vehicular Technology. Vol. 59, pp. 559-573.

Rawat, A.; Sharma, S.; Sushil, R. (2012). *Vanet: security attacks and its possible solutions.* Journal of Information and Operations Management, Vol. 3, pp. 301-304.

Raya, M.; Aziz, A. & Hubaux, J. P. (2006). *Efficient Secure Aggregation in VANETs.* ACM VANET'06: Proceedings of ACM International Workshop on Vehicular Ad Hoc Networks, pp. 67-75, Nova Iorque, EUA.

Raya, M. & Hubaux, J. P. (2007). *Securing vehicular ad hoc networks*. In Journal of Computer Security, Vol. 15, No. 1, pp. 39-68.

Raya, M.; Shokri, R.; Hubaux J. P. (2010) *On the tradeoff between trust and privacy in wireless ad hoc networks.* In WISEC - ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp 75–80.

Reina, D. G.; Askalani, M. et al. (2015). *A Survey on Multihop Ad Hoc Networks for Disaster Response Scenarios*. International Journal of Distributed Sensor Networks, vol. 2015, pp. 1-16.

Rivas, D. A.; Ordinas, J. M. B.; Zapata, M. G. ; Pozo, J. D. M. (2011). *Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation.* Journal of Network and Computer Applications, no. 34, pp. 1942–1955.

RNP – Rede Nacional de Ensino e Pesquisa. (2014). *Introdução à criptografia e PGP.* http://www.rnp.br/cais/keyserver/, acessado em 19/12/2014.

Saha, S.; Sheldekar, A. et al. (2011). *Post disaster management using delay tolerant network*. Communications in Computer and Information Science. Springer, vol. 162, pp. 170-184.

Schütze, T. (2011). *Automotive security: Cryptography for car2x communication*. In Embedded World Conference.

Seth A. & Keshav S. (2005). *Practical Security for Disconnected Nodes.* Workshop on Secure Network Protocols, pp. 31-36, IEEE Computer Society Washington, DC, USA.

Silva, C. M.; Aquino, A. L. L. & Meira, W. Jr. (2014). *Design of Roadside Infrastructure for Information Dissemination in Vehicular Networks* - In Network Operations and Management Symposium (NOMS).

Silva, T. H.; Loureiro, A. A. F.; Salles, J. et al. (2013). *Traffic Condition Is More Than Colored Lines on a Map: Characterization of Waze Alerts*. Springer International Conference on Social Informatics (SocInfo'13), Novembro 2013, Japão. pp. 309-318.

Smaldone, S.; Han, L.; Shankar, P.; Iftode, L. (2008). *RoadSpeak: enabling voice chat on roadways using vehicular social networks.* In Proceedings of the ACM Workshop on Social Network Systems (SocialNets). Nova Iorque, EUA, pp. 43-48.

Spyropoulos, T.; Psounis, K.; Raghavendra, C.S. (2005). *Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks.* In Proceedings of ACM SIGCOMM Workshop on Delay-Tolerant Networking. ACM Press, Nova Iorque, EUA, pp. 252–259.

Symington, S. F.; Farrell S.; Weiss H. & Lovell P. (2011). *Bundle Security Protocol Specification.* Disponível em http://tools.ietf.org/pdf/rfc6257. Acessado em 12/02/2015.

Tanenbaum, A. S. & Wetherall, D. (2011). *Redes de Computadores.* São Paulo, Pearson Prentice Hall, 5ª edição, 2011.

Teixeira, F. A.; Silva, V. F.; Leoni, J. L.; Macedo, D. F.; Nogueira, J. M. S. (2014). *Vehicular networks using the IEEE 802.11p standard: An experimental analysis.* Vehicular Communications, Vol. 1, No. 2, Abril 2014, pp. 91-96.

Trifunovic, S.; Legendre, F.; Anastasiades, C. (2010). *Social trust in opportunistic networks.* In INFOCOM IEEE Conference on Computer Communications Workshops, Março 2010, pp. 1-6.

Uppoor, S.; Trullols-Cruces, O.; Fiore, M.; Barcelo-Ordinas, J. M. (2014). *Generation and Analysis of a Large-Scale Urban Vehicular Mobility Dataset.* IEEE Transactions on Mobile Computing, Vol. 13, No. 5, pp. 1061-1075, Maio 2014.

Velloso, P. B. et al. (2008). *Analyzing a human-based trust model for mobile ad hoc networks.* IEEE Symposium on Computers and Communications, ISCC, pp. 240-245.

Velloso, P. B.; Laufer, R. P.; Cunha, D. O.; Duarte, O. C. M. B. & Pujolle, G. (2010). *Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model*. In IEEE Transactions on Network and Service Management. ISSN 1932-4537, Vol. 7, no 3, pp. 172-185.

Verma, C. K.; Tamma, B. R.; et al. (2011). *A realistic small-world model for wireless mesh networks.* IEEE Communications Letters, Vol. 15, No. 4, pp. 455-457.

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

Wan, J.; Zhang, D.; Zhao, S.; Yang, L.; Lloret, J. (2014). *Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions*. Communications Magazine, IEEE , vol.52, no.8, pp. 106-113, Agosto 2014.

Wangham, M. S.; Nogueira, M.; Fernandes, C. P.; Paviani, O.; Silva, B. F. (2014). *Segurança em Redes Veiculares: Inovações e Direções Futuras.* Minicursos do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg 2014, pp. 145-194.

Warthman, F. (2008). *Delay-Tolerant Networks (DTNs) - A Tutorial.* Relatório Técnico, InterPlanetary Internet Special Interest Group.

Wischhof, L.; Ebner, A.; Rohling, H.; Lott, M. & Halfmann, R. (2003). *SOTIS: A self-organizing traffic information system*. In IEEE Vehicular Technology Conference.

Wu, J.; Wang, Y. (2015). *Opportunistic Mobile Social Networks.* CRC Press, EUA. ISBN 9781466594951.

Xu, S.; Li, X.; Parker, T.P.; Wang, X. (2011). *Exploiting Trust-Based Social Networks for Distributed Protection of Sensitive Data*. IEEE Transactions on Information Forensics and Security, vol.6, no.1, pp. 39-52, Março 2011.

Yu, G. & Cheng, S. (2011). *Comparison research on the performance of DTN route protocol and Ad hoc route protocol*. International Conference on Multimedia Technology (ICMT), pp. 6273-6277.

Yu, H.; Kaminsky, M.; Gibbons, P. B.; Flaxman, A. D. (2008). *SybilGuard: Defending Against Sybil Attacks via Social Networks*. IEEE/ACM Transactions on Networking, vol. 16, no. 3, Junho 2008, pp. 576-589.

Zhang, J. (2011). *A survey on trust management for VANETs*. In IEEE International Conference on Advanced Information Networking and Applications, pp. 105-112.

Zhang, K.; Liang, X.; Shen; X.; Lu, R. (2014). *Exploiting multimedia services in mobile social networks from security and privacy perspectives.* IEEE Communications Magazine, vol.52, no.3, Março 2014, pp.58-65.

Zhou, J.; Song, M.; Song, J.; Zhou, X.; Sun, L. (2014). *Autonomic Group Key Management in Deep Space DTN. Wireless Personal Communications*. Volume 77, No. 1, Julho 2014, pp 269-287.

Zhu, H.; Lu, R.; Shen, X. & Lin, X. (2009). *Security in service-oriented vehicular networks.* IEEE Wireless Communications, Vol. 16, No. 4, pp. 16-22.

Zhu, X.; Lu, Y.; Zhang, B. & Hou, Z. (2013). *A Distributed Pseudonym Management Scheme in VANETs.* International Journal of Distributed Sensor Networks, Vol. 16, No. 4, pp. 16-22.

Zimmermann, P. R. (1995). *The official PGP user's guide*. MIT Press, Cambridge, MA.

Zou, X. & Deng, J. (2010). *Detection of Fabricated CTS Packet Attacks in Wireless LANs*. In Proceedings of International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Houston, EUA; Novembro 2010, pp. 105-115.