Capítulo 4

Segurança em Redes Veiculares: Inovações e Direções Futuras

Michelle S. Wangham[◇], **Michele Nogueira**[†], **Cláudio P. Fernandes**[◇], **Osmarildo Paviani**[◇], **Benevid F. da Silva**[†]

[◇] Universidade do Vale do Itajaí (UNIVALI)

[†] Universidade Federal do Paraná (UFPR)

Abstract

Over the past years, many research efforts have focused on enhancing vehicular networks (VANETs - Vehicular Adhoc Networks), as they are considered the foremost technology to provide safety and convenience to drivers as well as to support new applications to passengers' entertainment. Despite the benefits offered by VANETs, these networks introduce security challenges, such as the difficulty in keeping data privacy and the effortlessness in generating malicious behaviors, which although they have been gradually addressed in the literature, they result in yet open issues for research and innovation. In this chapter, we revisit (i) *the main concepts of vehicular networks,* (ii) *the major vulnerabilities and attacks against these networks, and* (iii) *the most prominent existing countermeasures. The open issues related to the existing countermeasures and the impacts of using those countermeasures are critically discussed, pointing out future directions for research and innovation.*

Resumo

Ao longo dos últimos anos, muitos esforços de pesquisa têm se concentrado no avanço das redes veiculares (VANETs - Vehicular Adhoc Networks), consideradas hoje uma das principais tecnologias para fornecer segurança e conveniência aos motoristas, bem como possibilitar novas aplicações voltadas ao entretenimento dos passageiros. Apesar dos vários benefícios oferecidos pelas redes veiculares, estas introduzem desafios de segurança, tais como a dificuldade em garantir a privacidade dos dados e a facilidade em gerar comportamentos maliciosos na rede, os quais, ainda geram questões abertas em termos de pesquisa e inovação. Neste capítulo, são revisitados (i) *os principais conceitos de VANETS,* (ii) *as principais vulnerabilidades e ataques de segurança, e* (iii) *as contramedidas mais proeminentes. As questões em aberto relacionadas às contramedidas de segurança e os impactos decorrentes do uso destas são discutidos de forma crítica, apontando direções futuras para pesquisa e inovação.*

 ©2014 SBC — Soc. Bras. de Computação

4.1. Introdução

Os noticiários mostram diariamente acidentes e congestionamentos que poderiam ser evitados com a utilização de Sistemas de Transportes Inteligentes (ITS- *Intelligent Transportation Systems*). Estes sistemas se apoiam nos avanços tecnológicos da comunicação sem fio e da computação móvel e na criação de aplicações que facilitem o cotidiano de motoristas e pedestres, assim como a gestão de trânsito e tráfego urbano realizada por empresas e pelo governo, visando o desenvolvimento de cidades inteligentes [Avelar et al. 2014]. Por exemplo, o uso de técnicas e equipamentos específicos que possibilitem a comunicação entre veículos [Faezipour et al. 2012]. Tendo em vista o potencial de revolucionar a experiência ao dirigir e a segurança, a comunicação entre veículos (V2V - *Vehicle-to-Vehicle*) está se tornando cada vez mais popular e tem atraído a atenção da indústria automobilística e da academia, além de permitir a existência de redes veiculares [Karagiannis et al. 2011].

A idéia básica das VANETs (*Vehicular Adhoc Networks*) é fazer uso, com alguns ajustes, das tecnologias amplamente adotadas e baratas das redes sem fio e das redes de sensores, e instalá-las em veículos. Os veículos são então capazes de coletar, gerar e analisar uma grande quantidade de dados, porém, para de fato proverem assistência a passageiros e motoristas, esses dados precisam ser compartilhados. Nas VANETs, o compartilhamento desses dados pode ser realizado de forma colaborativa diretamente entre os veículos em "um salto" de comunicação ou ainda através de "múltiplos saltos" de comunicação (V2V), em que veículos intermediários auxiliam na comunicação repassando as mensagens a outros veículos dentro da área de cobertura do sinal de comunicação sem fio [Hussain et al. 2012]. A comunicação através de múltiplos saltos possui limitações de alcance de propagação dos dados e está sujeita a intempéries. Desta forma, a fim de aumentar a cobertura da comunicação, pontos fixos na estrada (unidades de acostamento ou *Road Side Unit* - RSUs) podem também ser implantados, suportando comunicações V2I (*Vehicle-to-Infraestructure*), aquelas entre o veículo e uma RSU.

As aplicações e os serviços emergentes em redes veiculares exigem grandes mudanças nos modelos de computação e de comunicação, devido às suas características próprias como alta dinamicidade dos veículos, densidade variável, desconexões frequentes e outras. Tais aspectos motivam o desenvolvimento de modelos específicos para as redes veiculares [Lee et al. 2014]. Trabalhos recentes descrevem diversas possibilidades para combinação das redes veiculares com o modelo de computação em nuvem (V2C - *Vehicle-to-cloud*), com as redes sociais e com os modelos de redes da Internet do Futuro, tais como Redes Orientadas a Conteúdos e Redes Tolerantes a Atrasos e Desconexões [Gerla e Kleinrock 2011, Karagiannis et al. 2011, Hussain et al. 2012, Wang et al. 2012, Lee et al. 2014, Grassi et al. 2014, Mezghani et al. 2014a]. Além disso, as aplicações de tecnologias de comunicação mais avançadas, tais como rádio cognitivo e *Long-Term Evolution* (LTE), são cada vez mais utilizadas para aperfeiçoar o desempenho das comunicações sem fio em VANETs e compartilhar os dados de forma mais eficiente e robusta [Silva et al. 2014a].

A segurança em redes veiculares é um fator imprescindível que precisa ser observado, pois a falta desta pode afetar a vida de pessoas. Como quaisquer redes de computadores sem fio e redes *ad hoc* estas estão suscetíveis a ataques por usuários ou nós maliciosos, tais como ataques de negação de serviço, modificação de mensagens e

 ©2014 SBC — Soc. Bras. de Computação

análise de tráfego [Raya et al. 2006a, Nogueira et al. 2009, Hartenstein e Laberteaux 2010]. Porém, as características das VANETs, tais como a alta mobilidade dos nós, desconexões frequentes, densidade variável e escala da rede, trazem novos desafios à segurança. Como as VANETs suportam aplicações de emergência em tempo real e lidam com informações críticas de segurança no trânsito, estas devem satisfazer os seguintes requisitos de segurança: confidencialidade, integridade, disponibilidade, autenticidade, privacidade e não repudiação para prover segurança na comunicação dos dados [Samara et al. 2010]. Os desafios de segurança aumentam quando as redes veiculares são combinadas com outras tecnologias que compõem os plataformas em nuvem e orientadas a conteúdos. As aplicações nesses novos e promissores ambientes encorajam o compartilhamento de recursos e informações. Entretanto, essas plataformas também passam a ser alvo de ataques, como por exemplo, de negação de serviço ou de injeção de aplicativos maliciosos [Lee et al. 2014], sendo a prevenção desses mais complexa.

Muitas pesquisas estão sendo realizadas para garantir a segurança em VANETs. De acordo com [Isaac et al. 2010], o principal desafio em proporcionar segurança nessas redes consiste no fato de que em nenhum momento, durante a comunicação V2V a verdadeira identidade dos motoristas deve ser exposta, uma vez que adversários podem usar esta informação para atacar, aplicando identidades falsas para não serem descobertos. No entanto, os veículos e os condutores, muitas vezes, precisam divulgar suas identidades às RSUs em uma comunicação V2I, para poderem se comunicar com essas. Assim, garantir a autenticidade e o não repúdio sem afetar a privacidade é um grande desafio em ambientes veiculares. Outro desafio é a sensibilidade aos atrasos, uma vez que atrasos significantes proíbem o uso de protocolos e mecanismos de segurança que têm grande sobrecarga ou que dependem de múltiplos estágios de comunicação entre os nós, como por exemplo, os sistemas de reputação [Isaac et al. 2010].

Na tentativa de atender aos requisitos das redes veiculares, em julho de 2010, o IEEE 802.11p foi definido por um grupo de trabalho do IEEE para facilitar a implantação dessas redes em ambientes de alta velocidade (comunicação V2V e V2I). O padrão de acesso sem fio em ambientes veiculares - WAVE (*Wireless Access in the Vehicular Environment*), além de ser um modo de operação do IEEE 802.11p, é composto por um conjunto de normas, dentre estas, destaca-se a IEEE 1609.2 (serviços de segurança WAVE). Esta norma define os mecanismos de segurança a serem usados, o formato dos pacotes, os protocolos para tratamento das mensagens e um certificado digital compacto especial para comunicações veiculares. No entanto, o padrão IEEE 1609.2 não define como deve ser a identificação do veículo e como proteger a privacidade, deixando essas questões em aberto [Lin et al. 2008, Sukuvaara et al. 2013].

Diante das recentes pesquisas a cerca das inovações das redes veiculares, os objetivos deste capítulo consistem em revisitar os conceitos e as vulnerabilidades de segurança existentes em VANETs, e analisar de forma crítica os desafios de segurança e as principais contramedidas propostas em trabalhos acadêmicos. As questões-chave analisadas neste capítulo focam na autenticação de usuários e veículos versus a privacidade dos dados, nos ataques gerados por nós maliciosos e nos novos ataques decorrentes do uso de tecnologias como computação em nuvem e da integração dessas redes com modelos visionados para a Internet do Futuro.

 ©2014 SBC — Soc. Bras. de Computação

Este capítulo está dividido em cinco seções. Nesta primeira seção, foi apresentada uma contextualização, destacando os objetivos e a motivação para a escolha do tema. A Seção 4.2 apresenta uma visão geral sobre redes veiculares, abordando as principais características e restrições, os principais padrões de comunicação e alguns domínios de aplicações de redes veiculares. Na Seção 4.3, são elencados os principais requisitos de segurança em redes veiculares, o perfil dos atacantes e os principais ataques descritos na literatura. A Seção 4.4 apresenta o estado da arte em termos das principais contramedidas aos ataques analisados, dentre estas destacam-se: os serviços de segurança WAVE; os mecanismos de autenticação; os controles criptográficos e os sistemas de reputação. Por fim, a Seção 4.5 traz uma síntese dos principais aspectos da segurança em redes veiculares analisados e as tendências de pesquisa nesta área.

4.2. Visão Geral sobre Redes Veiculares

As redes veiculares são um tipo de rede sem fio em ascensão devido aos avanços na indústria automobilística e nas tecnologias de comunicação sem fio. Os avanços na indústria automobilística estão possibilitando agregar novas tecnologias aos veículos, provendo aos usuários acesso a novos serviços, como informações sobre o ambiente e as condições do trânsito, alertas de perigos nas vias, conexão com a Internet, entre muitos outros [Macedo et al. 2013]. Além disso, a evolução das tecnologias de comunicação sem fio, a reserva de uma banda dedicada para comunicação de curto alcance (DSRC do Inglês *Dedicate Short-range Communications*) e a definição de um conjunto de padrões específicos para as redes veiculares (IEEE 1609) tem contribuído para o amadurecimento destas redes [Al-Sultan et al. 2014].

Os veículos são os principais componentes de uma rede veicular, os chamados nós. Estes possuem uma interface de comunicação sem fio para enviar, receber ou trocar informações. A Figura 4.1 ilustra o processo de comunicação em uma rede veicular. Os nós A, B e C representam um cenário em que os veículos estão circulando por uma via e trocando informações entre si e com uma infraestrutura fixa no acostamento. A comunicação entre os nós A, B e C caracteriza uma comunicação de veículo para veículo (V2V). Neste modelo, para que uma informação de alerta seja encaminhada do nó A para o C, é preciso que o nó B, que se encontra no alcance de ambos, faça o encaminhamento da mensagem da origem (A) para o destino (C). A comunicação representada pelo nó A e a infraestrutura $I1$ (V2I) corresponde à troca de informações entre os nós de uma rede veicular e equipamentos fixos ou unidades de acostamento (RSUs − *Road Side Unit*) ao longo da via. Neste modo, um nó RSU pode estabelecer a comunicação com outras redes de serviços ou até mesmo com a Internet.

As VANETs são geralmente comparadas com as redes *ad hoc* tradicionais, porém existem alguns aspectos que são favoráveis às redes veiculares, como a baixa restrição do consumo de energia, o poder computacional elevado e a mobilidade previsível dos nós. O consumo de energia de um nó veicular não é considerado crítico pois este possui uma fonte de energia superior a de um nó *ad hoc* tradicional. O poder computacional também é superior, podendo ter maior capacidade de processamento, armazenamento e largura de banda, e ainda, agregar outros recursos, como antenas com tecnologias avançadas, sistemas de posicionamento global (GPS), sensores, entre muitos outros. Por fim, a mobilidade dos nós em um ambiente urbano pode ser previsível, pois os veículos tendem a seguir o trajeto

 ©2014 SBC — Soc. Bras. de Computação

estabelecido pelas vias e sinalizações de trânsito [Sichitiu e Kihl 2008a].

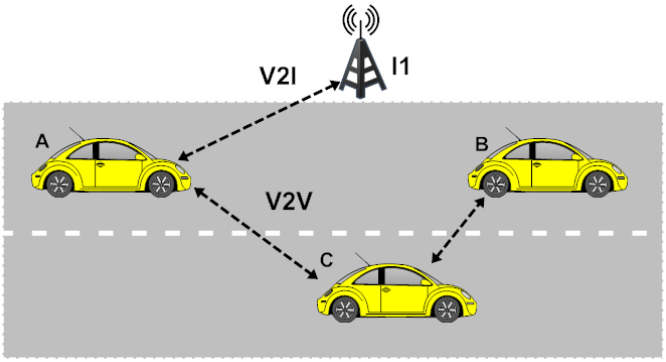

Figura 4.1. Esquema de comunicação em uma rede veicular

4.2.1. Características das Redes Veiculares

Os aspectos citados anteriormente são favoráveis às redes veiculares, contudo, existem outras características específicas do ambiente e precisam ser consideradas no desenvolvimento de seus protocolos e serviços [Al-Sultan et al. 2014, Hartenstein e Laberteaux 2008, Mejri et al. 2014]. Entre estas, citam-se:

- **Densidade variável da rede**: densidade pode variar de muito alta, a exemplo de um engarrafamento, ou muito baixa, como em horários noturnos ou nos subúrbios;
- **Escala da rede**: pode abranger áreas de grande densidade, como o centro de cidades ou rodovias de grande circulação;
- **Alta mobilidade**: é considerada uma das mais importantes, pois os nós estão sempre em movimento e se deslocando em velocidades elevadas e com direções variadas;
- **Topologia dinâmica da rede**: devido à alta mobilidade, a topologia muda rapidamente. O tempo de comunicação entre os nós geralmente é muito curto, principalmente, se estiverem se movendo em direções contrárias, fazendo com que o alcance da comunicação (diâmetro efetivo da rede) mude constantemente;
- **Desconexões frequentes**: a topologia dinâmica, a alta mobilidade e outros fatores como condições climáticas e densidade do tráfego podem causar desconexões frequentes dos nós.

Estas especificidades dificultam ou impossibilitam a aplicação de padrões e protocolos já consolidados para as redes *ad hoc* em redes veiculares, determinando novos desafios para o processo de comunicação neste ambiente. Em [Al-Sultan et al. 2014] são apresentados alguns dos principais desafios em VANETs:

- **Encobrimento de sinal**: objetos localizados entre dois veículos que estejam se comunicando é um dos desafios que afeta a eficiência das VANET. Estes objetos podem ser outros veículos ou construções distribuídos em torno das rodovias ou das cidades;

 ©2014 SBC — Soc. Bras. de Computação

- **Limitações de banda**: deve-se realizar um gerenciamento eficiente de banda para que não ocorra um congestionamento do canal. Isto ocorre porque neste modelo de rede não se tem um coordenador central que controla a comunicação entre os nós, e que teria a responsabilidade de gerenciar a banda e as operações de contenção;

- **Conectividade**: devido à alta mobilidade e às mudanças rápidas da topologia, que levam a uma fragmentação frequente nas redes, o tempo de vida de uma ligação precisa ser alongado o quanto for possível. Esta tarefa pode ser feita através do aumento da potência de transmissão, contudo, isto pode levar à degradação do rendimento;

- **Diâmetro pequeno**: o diâmetro efetivo de uma VANET é pequeno, o que leva a uma conectividade fraca entre os nodos. Deste modo, é impraticável para um nó manter de forma completa uma topologia global da rede. Esta restrição do diâmetro da rede resulta em problemas, quando se aplica, algoritmos de roteamento existentes em redes *ad hoc*;

- **Privacidade e segurança**: manter um equilíbrio entre segurança e privacidade é um dos principais desafios das VANETs. Um receptor quer ter certeza que pode confiar na fonte da informação. Entretanto, ter acesso a identidade do emissor pode contradizer os requisitos de privacidade deste emissor;

- **Protocolos de roteamento**: devido às características da rede, desenvolver um protocolo de roteamento eficiente que possa entregar um pacote com o período mínimo de tempo e com pouca perda de pacotes é considerado um desafio crítico nas VANETs.

4.2.2. Padrões de Comunicação usados em Redes Veiculares

A reserva de uma faixa de comunicação de curto alcance dedicada (DSRC) pode ser considerada uma das primeiras iniciativas de padronização das tecnologias, específicas para as comunicações veiculares de curto alcance, V2V e V2I. A iniciativa de alocação desta faixa partiu dos Estados Unidos, que, em 1999, através da FCC (*Federal Communications Commission*), alocaram a banda de 5.9 GHz (5.850 – 5.925 GHz) para este fim. Posteriormente, surgiram outras iniciativas de alocar esta faixa de comunicação com o mesmo objetivo, como a Europa e o Japão, que alocaram a banda de 5.8 GHz [Li e Wang 2007, Al-Sultan et al. 2014, Faezipour et al. 2012]. Em 2002, a FCC sofreu grande influência da ITSA (*Intelligent Transportation Society of America*) em relação ao licenciamento, regras de serviços, e as possíveis tecnologias para a banda DSRC. As recomendações sugeriam a adoção pela FCC de um padrão único de arquitetura para as camadas físicas (PHY) e de controle de acesso ao meio (MAC) e que esta fosse desenvolvida pela ASTM (*American Society for Testing and Materials*), utilizando como base o padrão IEEE 802.11.

Em 2004, um grupo de trabalho da IEEE (grupo de trabalho p ou TGp do grupo de trabalho IEEE 802.11) assumiu o papel iniciado pela ASTM e começou o desenvolvimento de uma emenda ao padrão 802.11 para incluir as demandas das redes veiculares. Esta emenda ficou conhecida como 802.11p. Outro grupo de trabalho da IEEE (grupo de trabalho 1609) ficou responsável por desenvolver as especificações para cobrir as camadas adicionais através de um conjunto de protocolos. Atualmente, o conjunto de padrões IEEE

 ©2014 SBC — Soc. Bras. de Computação

1609 consiste em um conjunto de documentos que, coletivamente com o IEEE 802.11p, são chamados de WAVE, que tem como objetivo facilitar o acesso sem fio às redes veiculares. Em termos de nomenclatura, comumente refere-se ao projeto conceitual como arquitetura WAVE e aos sistemas que o utiliza como sistemas WAVE [Toor et al. 2008, Al-Sultan et al. 2014, Faezipour et al. 2012].

A família de padrões IEEE 1609 é dividida em uma série de documentos que descrevem o funcionamento e os protocolos da arquitetura WAVE. A Figura 4.2 demonstra a organização da arquitetura em relação ao modelo ISO/OSI, e também uma referência entre as camadas e os documentos que formam a família de padrões IEEE 1609, conjuntamente com o protocolo IEEE 802.11p.

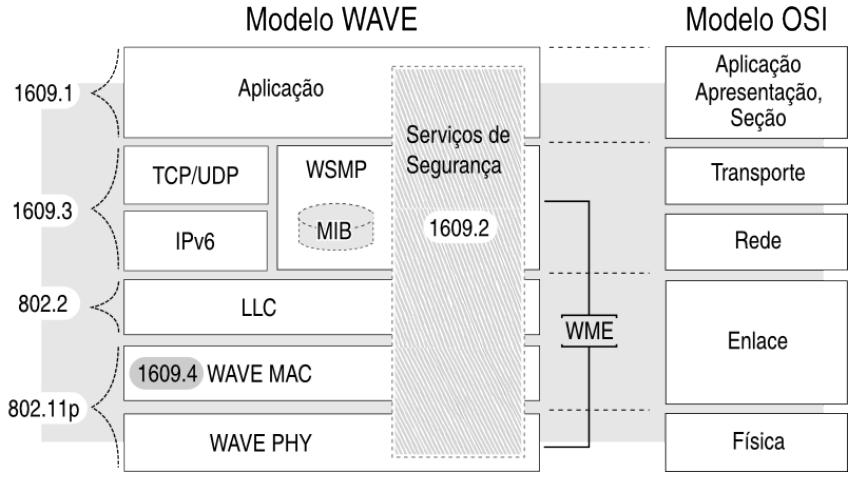

Figura 4.2. Arquitetura WAVE [Uzcategui e Acosta-Marum 2009]

Em síntese, os principais documentos da família IEEE 1609 são:

- **IEEE P1609.0**: descreve a arquitetura WAVE. Este define o funcionamento dos padrões e os serviços necessários para que os dispositivos possam se comunicar, utilizando os múltiplos canais DSRC em um ambiente de alta mobilidade.

- **IEEE P1609.1**: está relacionado com o gerenciamento de recursos (define os fluxos de dados e os recursos). Este descreve também os componentes básicos da arquitetura WAVE e define as mensagens de comando, os formatos para armazenamento dos dados e especifica os tipos de dispositivos que podem ser suportados por uma unidade de bordo (*On-Board Unit* − OBU)[1].

- **IEEE 1609.2**: refere-se aos serviços de segurança para as aplicações e o gerenciamento de mensagens. Este documento define os métodos de processamento e os formatos das mensagens de segurança utilizados pelos sistemas WAVE e DSRC. Este descreve como prover segurança para as mensagens de aplicações e de gerenciamento, bem como as funções necessárias para suportar mensagens seguras e a privacidade dos veículos (ver Seção 4.4.1).

[1]Unidade embarcada nos veículos que permite a comunicação entre os nós da rede.

 ©2014 SBC — Soc. Bras. de Computação

- **IEEE 1609.3**: descreve os serviços para as camadas de rede e de transporte, como o roteamento e endereçamento com suporte a troca de mensagens seguras. O WAVE suporta duas pilhas de protocolo: o IP na versão 6 (IPv6) e o WSMP (*WAVE Short-Message Protocol*). A razão para ter duas pilhas de protocolo é a necessidade de suportar comunicações de alta prioridade e sensíveis ao tempo, como também aplicações não tão exigentes, como as transações que utilizam as transmissões TCP/UDP. Este padrão também define um conjunto de funções de gerenciamento, denominado WME (*WAVE management entity*), que deve ser utilizado para prover serviços de rede, e uma base de informações de gerenciamento (MIB, do Inglês *Management Information Base*).

- **IEEE 1609.4**: descreve as operações em múltiplos canais que utilizam o protocolo 802.11p (controle de acesso ao meio e camada física) para a arquitetura WAVE.

- **IEEE 1609.11**: define os serviços e o formato das mensagens necessárias para utilização de sistemas de pagamentos eletrônicos seguros. O IEEE 1609.12 especifica os valores dos identificadores que foram alocados para os sistemas WAVE.

As camadas PHY e MAC, especificadas pelo IEEE 802.11p, são baseadas no IEEE 802.11a para definição da camada física e no IEEE 802.11e para a camada de controle de acesso ao meio, respectivamente. A camada IEEE 802.11p PHY é baseada na OFDM (do inglês *Orthogonal frequency-division multiplexing*), que utiliza uma técnica de modulação que faz a multiplexação por divisão de frequência para encaminhar os sinais através de diferentes canais/frequências. As taxas de fluxo estão entre 3-27 Mbps, utilizando canais com largura de 10MHZ, e podendo alcançar cerca de 1000m [Mejri et al. 2014]. A camada IEEE 802.11p MAC utiliza o EDCA (do inglês *Enhanced Distributed Channel Access*), que é um melhoramento do DCF (do inglês *Distributed Coordination Function*), um protocolo que utiliza uma função de coordenação distribuída, em que a decisão de qual estação pode transmitir é realizada individualmente pelos pontos da rede, a fim de evitar colisões. O EDCA introduz, entre outras características, o conceito de gerenciamento com qualidade de serviço, utilizando categorias de acesso (divididas em tráfego de fundo, de melhor esforço, de vídeo e de voz), para garantir que as mensagens de segurança sejam transmitidas dentro de um tempo razoável [Uzcategui e Acosta-Marum 2009].

Um sistema WAVE é composto basicamente por entidades que são denominadas unidades de bordo (OBUs) e unidades de acostamento (RSUs). Uma OBU é um componente embarcado nos veículos que funciona enquanto estes transitam. Estas unidades realizam diversas funções, dentre estas, o roteamento entre os nós da rede, o controle de congestionamento e a transferência de mensagens confiáveis. As entidades RSUs são componentes instalados em postes de luz, semáforos, em margens das vias, entre outros.

Atualmente, existem outros padrões de tecnologias sem fio que podem ser utilizadas para prover serviços e informações para uma rede veicular. Estas tecnologias incluem as redes de celular (LTE, GSM, entre outras) e as redes locais sem fio (WLAN 802.11 a/b/g/n). De acordo com [Hill e Garrett 2011], as redes de telefonia celular não são apropriadas para troca de dados em tempo real utilizadas nas comunicações V2V e V2I, devido à latência da rede e às possíveis quedas de conexão, contudo, estas podem prover serviços valiosos para estes ambientes, principalmente, para aplicações que necessitam de

 ©2014 SBC — Soc. Bras. de Computação

conectividade. Os aparelhos celulares (*smartphones*) são capazes de oferecer informações e entretenimento durante a viagem muito além do que os meios de transmissão por banda AM/FM comuns nos veículos. O uso destas tecnologias não está limitado a receber apenas dados da viagem, de modo que as conexões com a rede de telefonia celular estão sendo gradativamente utilizadas para outros fins, como coletar dados para investigação ou para aplicações telemáticas, especialmente, em frotas de veículos (táxi, caminhões, etc).

Em relação às redes sem fio locais, que utilizam a tecnologia Wi-Fi (*Wireless Fidelity*), foram inicialmente desenvolvidas para prover comunicação sem fio no lugar das redes locais cabeadas. Os equipamentos são amplamente utilizados em residências, no comércio e ambientes industriais. Os protocolos desta tecnologia são descritos pelo padrão IEEE 802.11 original, e define as especificações das camadas PHY e MAC para prover a conectividade sem fio para dispositivos fixos e móveis em uma rede local. O protocolo de controle de acesso ao meio (MAC) é o principal elemento de uma WLAN, responsável por gerenciar as situações de congestionamentos que podem ocorrer na rede. As redes que seguem o padrão podem implementar um dos dois métodos de acesso, o DCF (*Distributed Coordination Function*), para acesso assíncrono, distribuído e orientado a contenções, e o PCF (*Point Coordination Function*), para acesso centralizado e livre de contenções [Bononi et al. 2004]. O objetivo do PCF é dar suporte para serviços de tempo real, dando mais prioridade de acesso ao meio sem fio para as estações (nós) em relação ao DCF. O DCF é considerado a base para as redes sem fio *ad hoc* e utiliza o protocolo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) para prevenção de colisões e acesso ao meio [Bononi et al. 2004, Mangold et al. 2002]. As redes WLANs e o padrão IEEE 802.11 original não foram projetados para suportar as aplicações veiculares que utilizam a comunicação V2V ou V2I, contudo, segundo [Hill e Garrett 2011] têm sido utilizadas eficientemente em aplicações que envolvem a comunicação entre veículos e estações fixas, como em estacionamentos e pátios de manutenção.

Outras tecnologias de comunicação sem fio podem ser utilizadas em aplicações de redes veiculares, contudo, estas são limitadas pelas características do ambiente. Como exemplo, tem-se o *Bluetooth* (padrão IEEE 802.15.1), utilizado para comunicações sem fio de curto alcance para conectar dispositivos de uma rede PAN (*Personal Area Network*). Esta tecnologia é considerada de baixo custo, de fácil uso e é amplamente utilizada nos veículos através dos dispositivos multimídias. Contudo, no contexto da comunicação veicular, o *Bluetooth* tem diversas desvantagens. O número limitado de nós, a baixa taxa de transferência e o curto alcance da comunicação são exemplos dos limites que esta tecnologia possui diante das redes veiculares [Sichitiu e Kihl 2008b].

4.2.3. Redes Veiculares, Nuvem e a Internet do Futuro

Os recentes avanços tecnológicos, principalmente nas áreas da computação móvel, redes sem fio e sensoriamento remoto, estão impulsionando o desenvolvimento dos sistemas de transporte inteligente (ITS). Os veículos estão se tornando sistemas computacionais sofisticados, embarcados com diversos sensores e computadores dedicados a funções específicas. Com o advento da comunicação sem fio, estes podem trocar as informações coletadas de seus sensores e do ambiente com os demais veículos que estejam por perto [Papadimitratos et al. 2009].

 ©2014 SBC — Soc. Bras. de Computação

Os veículos podem ser considerados uma plataforma de observação ideal do ambiente, contudo, se as informações coletadas permanecerem localmente podem não ter muita relevância em uma rede veicular. Tendo como base este princípio, os autores em [Gerla 2012] propuseram um modelo de computação em nuvem veicular (VCC do Inglês *Vehicular Cloud Computing*), baseado na computação em nuvem móvel (MCC do Inglês *Mobile Cloud Computing*). Uma MCC utiliza o poder computacional dos dispositivos móveis a fim de permitir que os dados sejam processados e armazenados localmente, minimizando os custos de fazer o *upload* ou *download* dos dados da Internet. Deste modo, alguns dos benefícios em relação a uma nuvem na Internet é a redução dos atrasos na comunicação, redução da área de alcance e a ampliação das possíveis aplicações [Gerla 2012].

Uma VCC aproveita a capacidade de processamento e armazenamento de uma coleção de veículos para formar uma nuvem na qual serviços são produzidos, mantidos e consumidos [Lee et al. 2014]. Por exemplo, em uma situação em que um motorista busca por um restaurante em uma cidade, é mais útil se ele conseguir as recomendações diretamente com os veículos próximos, que possuem maior conhecimento da vizinhança, do que recorrer à Internet. Em [Lee et al. 2014], os autores introduzem o conceito de rede em nuvem veicular (VCN do inglês *Vehicular Cloud Networking*). Este conceito é baseado na integração das redes orientadas a informações (ICN do inglês *Information-centric networking*) ou analogamente, redes orientadas a conteúdo (CCN do inglês *Content Centric Network*) com a VCC. O ICN é um conceito que resulta das atividades de pesquisa relacionadas com a Internet do Futuro e baseia-se em uma arquitetura de comunicação para distribuição eficiente de conteúdo na Internet. Neste conceito, o paradigma principal para distribuição não é a comunicação fim a fim, mas sim a distribuição de conteúdo. Este paradigma utiliza atributos dos dados ou do nó como identificação do conteúdo, geolocalização ou contexto, ao invés de um endereço específico, como por exemplo o endereço IP (*Internet Protocol*) [Ahlgren et al. 2012].

O conceito de VCN [Lee et al. 2014] tem como base a arquitetura NDN (*Named Data Networking*), a qual segue a arquitetura de ICN e foi estendida para as VANETs. Esta arquitetura trabalha com dois tipos de pacotes: pacote de interesse e pacote de dados (conteúdo), que se referem ao cliente e ao distribuidor de conteúdos, respectivamente. Basicamente, esta arquitetura funciona do seguinte modo: um cliente faz uma requisição de um conteúdo transmitindo o seu pacote de interesse para os potenciais distribuidores de conteúdo. Quando um determinado distribuidor recebe este pacote de interesse, este confirma que seus dados coincidem com a busca e responde encaminhando o pacote de dados para o cliente através do caminho reverso do pacote de interesse. A arquitetura NDN permite que os roteadores façam o armazenamento dos dados para que agilizem as próximas consultas recorrentes, tornando a distribuição de conteúdo mais eficiente.

O objetivo de uma VCN é criar uma nuvem veicular temporária, com a participação de veículos e RSUs. Os membros desta nuvem colaboram para produzir serviços que não poderiam ser realizados de modo individual. A Figura 4.3 ilustra o funcionamento de uma VCN [Lee et al. 2014]. Quando um determinado veículo, no caso V_1, executa uma aplicação, este se torna o líder da nuvem e, então, recruta membros que podem prover recursos para compor a nuvem veicular. O alcance desta nuvem depende da aplicação, mas pode ser uma distância pré-definida, como parte de uma via ou um cruzamento, etc. O líder transmite uma mensagem em *broadcast* para os veículos de acordo com o

 ©2014 SBC — Soc. Bras. de Computação

alcance determinado, conforme o tipo de recursos necessários. Os veículos que quiserem compartilhar os recursos, no exemplo representados por V_2 e C_1, respondem a mensagem enviada pelo líder com a informação sobre a capacidade de seus recursos. Após receber as mensagens de retorno, o líder seleciona os membros com os quais organiza a nuvem.

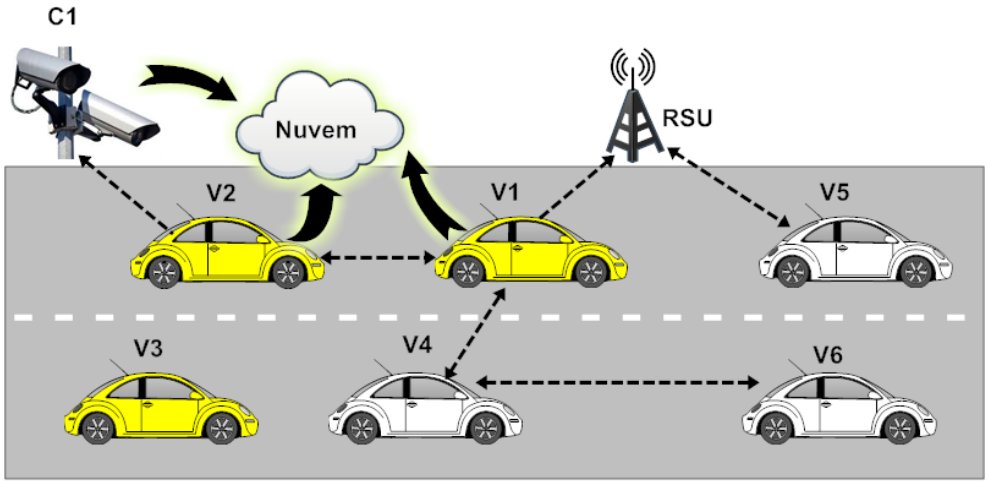

Figura 4.3. Funcionamento de uma VCN [Lee et al. 2014]

Com a nuvem formada, o líder divide a aplicação em diversas tarefas e distribui para os membros, com base na acessibilidade e disponibilidade dos recursos. Após completar a execução das tarefas, os membros retornam os resultados para o líder. Após coletar os resultados de todas as tarefas, o líder processa e salva a saída obtida. Caso não seja possível processar ou armazenar o conteúdo em um único nó, este pode selecionar outros nós para fazê-lo, representado pelo V_4. Por fim, este conteúdo fica acessível para todos os veículos da rede, na Figura, representados por V_5 e V_6. Caso um veículo deixe a nuvem, o líder pode selecionar a substituição do mesmo, encaminhando uma mensagem para os veículos dentro do alcance delimitado, a fim de completar o conjunto de recursos necessários. E, caso o líder deixe a nuvem ou ela não seja mais necessária, o líder encaminha uma mensagem para os membros, removendo-os da lista de membros e liberando-os para que possam fazer parte de outras nuvens.

De acordo com [Faezipour et al. 2012], algumas companhias automotivas têm dado alguns passos em direção à conectividade entre veículos e a nuvem. Em particular, a Toyota tem anunciado uma parceria com a Microsoft para oferecer esta conectividade. Os planos são para, a partir de 2015, conectar os carros na plataforma de nuvens Microsoft Azure para prover uma solução de telemática em nuvem. Ainda segundo os autores, este tipo de comunicação é útil para prover uma assistência ativa ao motorista e para o rastreamento de veículos em redes de gerenciamento de frotas.

Em relação a tecnologias emergentes, especificamente em relação a IoT (do inglês *Internet of Things*), [He et al. 2014] consideram que esta pode trazer soluções que irão transformar os sistemas de transporte e os serviços da indústria automotiva. Considerando que os veículos trazem sensores cada vez mais poderosos, conectividade, capacidade de processar dados, as tecnologias da IoT podem ser utilizadas para juntar estas capacidades e compartilhar os recursos subutilizados. Com a IoT, é possível rastrear a localização de cada veículo, monitorar seu movimento e prever sua localização futura. Ainda segundo

 ©2014 SBC — Soc. Bras. de Computação

os autores, na IoT, pode haver a integração da computação em nuvem, das redes de sensores sem fio, das redes de sensores RFID, das redes de satélites e de outras tecnologias. Esta união vai possibilitar a criação de uma nova geração de nuvens de dados veiculares baseadas na IoT, para prover serviços que, entre outras coisas, aumentem a segurança nas estradas, reduzam os engarrafamentos, gerenciem o tráfego e recomendem a manutenção ou reparo do veículo [He et al. 2014].

4.2.4. Domínios de Aplicações em Redes Veiculares

A maioria das aplicações emergentes suportadas por redes veiculares estão relacionadas às questões de segurança necessárias a todos os veículos. Contudo, o acesso às redes infraestruturadas permite que inúmeras aplicações e serviços sejam providos para estes ambientes [Karagiannis et al. 2011, Silva et al. 2014b]. Com base nos trabalhos de [Papadimitratos et al. 2009, Hossain et al. 2010, Karagiannis et al. 2011], as aplicações podem ser classificadas em três tipos: aplicações de segurança (*safety*) no transporte, aplicações de gerenciamento e eficiência de tráfego e aplicações de *Infotainment*.

As aplicações do primeiro tipo buscam melhorar a segurança dos usuários nas vias, notificando os veículos sobre qualquer situação de perigo na vizinhança com intuito de reduzir a probabilidade de acidentes [Hossain et al. 2010]. Os exemplos mais comuns deste tipo são os alertas de colisão, assistência para mudança de faixa, aviso de ultrapassagem, e avisos de veículos de emergência. As aplicações de gerenciamento e eficiência de tráfego focam em 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. As aplicações de gerenciamento de velocidade e de navegação cooperativa são dois grupos típicos deste tipo de aplicações, a saber:

- **Aplicações de gerenciamento de velocidade**: têm como objetivo auxiliar o motorista a controlar a velocidade para que tenha uma direção estável e evitar que o mesmo tenha que parar sem necessidade. Notificadores ou reguladores de limite de velocidade ou a indicação no painel de uma luz verde que indique quanto esteja em uma velocidade ideal são dois exemplos deste grupo;
- **Navegação cooperativa**: utilizada para aumentar a eficiência do tráfego pelo gerenciamento da navegação dos veículos através da cooperação entre estes e entre as unidades de acostamento das vias. Alguns exemplos deste tipo de aplicações são: informações de tráfego e recomendação de um itinerário, cooperação para o controle de uma navegação adaptativa e em grupos.

O terceiro tipo são as aplicações que oferecem, entre outras coisas, informação e entretenimento para o conforto dos motoristas e passageiros, e são comumente citadas como aplicações de *Infotainment*. Este tipo de aplicação pode oferecer uma grande variedade de serviços, como disseminação de conteúdos multimídia em tempo real ou não, jogos interativos, busca de informações locais, como restaurantes ou postos de combustível, informações climáticas ou até mesmo acesso a Internet, para *download* de informações, músicas, etc [Hossain et al. 2010]. Alguns trabalhos recentes apresentam abordagens específicas para distribuição de conteúdo aos usuários das redes veiculares [Mezghani et al. 2014b].

 ©2014 SBC — Soc. Bras. de Computação

A Tabela 4.1 apresenta uma lista de aplicações e alguns de seus requisitos. Cada aplicação está relacionada ao tipo de comunicação, ao tipo da mensagem, ao tempo da mensagem, à latência (tempo de atraso máximo requerido pela aplicação) e a outros requisitos (prioridade, alcance, etc) [Papadimitratos et al. 2009].

Tabela 4.1. Características de Aplicações Veiculares [Papadimitratos et al. 2009]

#	Aplicações	Comunicação	Tipo	Tempo	Latência	Outros
1	Alerta de veículo lento	*ad hoc*, V2V	*broadcast* permanente	500ms	100ms	Alcance: 300m, alta prioridade
2	Alerta de colisão em cruzamento	*ad hoc*, infraestrutura, V2V, V2I	*broadcast* permanente	100ms	100ms	Posicionamento preciso em um mapa digital, alta prioridade
3	Pré-colisão	*ad hoc*, V2V	*broadcast* periódico, *unicast*	100ms	50ms	Alcance 50m, prioridade alta/média
4	Gerenciamento de Cruzamento	infraestrutura, *ad hoc*, V2I, V2V	*broadcast* periódico, *unicast*	1000ms	500ms	Precisão do posicionamento: < 5m
5	*Download* de Mídia	infraestrutura, rede de telefonia celular, etc	*unicast*, *broadcast*, sob-demanda	n/d	500ms	Acesso à internet, Gerência dos direitos reservados
6	Assistência para direção ecológica	infraestrutura, *ad hoc*, V2I, V2V e rede de telefonia celular	*unicast*, *broadcast*, sob-demanda	1000ms	500ms	Acesso à Internet disponibilidade do serviço

As aplicações 1, 2 e 3 estão relacionadas com a categoria de segurança no transporte. Estas utilizam em sua maioria a comunicação *ad hoc*, possuem uma restrição de tempo rigorosa e tem uma prioridade elevada no enlace dos dados. Entre estas, a aplicação de pré-colisão é a mais rigorosa com o requisito de latência. Este tipo de aplicação pode ser mais relevante para comunicações de curto alcance, que corresponde a pequenas distâncias entre os veículos. A aplicação 4 está relacionada com a categoria gerenciamento e eficiência do tráfego e caracteriza-se pela comunicação *ad hoc* com a infraestrutura (RSUs, pedágios, etc). A prioridade determinada é baixa em relação as aplicações de segurança e os requisitos de latência são maiores. As demais aplicações, 5 e 6, estão relacionadas com a categoria *infotainment*. Este tipo de aplicação depende mais da comunicação com redes infraestruturadas (redes de telefonia celular, Internet, etc) do que a comunicação V2V. A preocupação com a latência é menos que as outras categorias de aplicação, contudo, existem outras questões a serem observadas, como o gerenciamento dos direitos do conteúdo a ser obtido e a disponibilidade de determinados serviços, bem como o acesso à Internet.

4.3. Ameaças e Ataques de Segurança em Redes Veiculares

Ao abordar as questões de segurança em redes veiculares é interessante especificar os requisitos de segurança que devem ser garantidos para o correto funcionamento dessas

 ©2014 SBC — Soc. Bras. de Computação

redes (Seção 4.3.1), os perfis dos atacantes na rede (Seção 4.3.2), bem como os tipos de ataques que podem ser executados por estes (Seção 4.3.3). As próximas subseções detalham esses três aspectos.

4.3.1. Requisitos de Segurança

As VANETs devem satisfazer os seguintes requisitos de segurança no suporte aos diferentes tipo de aplicações [Raya et al. 2006a, Samara et al. 2010, Tangade e Manvi 2013]:

- **Confidencialidade**: o sigilo deve ser fornecido ao dado sensível que está sendo enviado pela VANET, sobretudo em aplicações financeiras e comerciais.
- **Integridade**: as mensagens enviadas através da rede não podem ser corrompidas. Possíveis ataques que possam comprometer a integridade das mensagens são os ataques de nós maliciosos ou falhas de sinal que produzem erros na transmissão.
- **Autenticidade**: a identidade dos nós na rede deve ser assegurada. Caso contrário, será possível a um atacante simular um nó legítimo, a fim de enviar e receber mensagens em seu nome.
- **Disponibilidade**: a rede deve estar disponível e funcional em todos os momentos, a fim de possibilitar o envio e recebimento de mensagens. Duas possíveis ameaças à disponibilidade são: os ataques de negação de serviço (DoS, *Denial of Service*) e ataques *jamming* [Xu et al. 2006]. Outro problema de disponibilidade pode ser causado por nós egoístas que não oferecem os seus serviços para o benefício de outros nós, a fim de salvar os seus próprios recursos como a energia da bateria. A disponibilidade também pode ser comprometida por interferências nos sinais de transmissão, pelo problema do terminal escondido, pelo devanecimento do sinal e outros.
- **Não repúdio**: um nó remetente pode tentar negar o envio de uma mensagem, a fim de evitar a sua responsabilidade pelo seu conteúdo. Garantir o não-repúdio é particularmente útil para detectar a ação de nós maliciosos.
- **Privacidade**: o sigilo das informações dos motoristas (tais como, identidade, velocidade, caminho percorrido) contra observadores não autorizados deve ser garantido.

4.3.2. Perfil dos Atacantes

O objetivo do atacante é criar problemas para outros usuários da rede, por exemplo alterando o conteúdo das mensagens ou invadindo sua privacidade. Antes de descrever os diferentes ataques em VANETs, os perfis dos ataques são categorizados. Um nó é considerado adversário ou malicioso se este tenta injetar qualquer tipo de mau comportamento na rede que pode fazer com que outros nós e/ou rede funcionem de forma inadequada [Tangade e Manvi 2013]. Os atacantes em redes veiculares podem ter perfis variados. Para classificar a capacidade destes atacantes, os autores em [Raya e Hubaux 2007] definiram quatro dimensões:

 ©2014 SBC — Soc. Bras. de Computação

- **Interno versus externo**: o atacante interno é aquele que está autenticado, que tem conhecimento detalhado da rede e que pode se comunicar com os outros nós. Os ataques mais sofisticados podem ser elaborados quando este atacante tem todas as informações sobre a configuração da rede. O atacante externo é considerado pelos membros da rede como um intruso, sendo que os ataques que pode executar são limitados (por exemplo, o uso indevido de protocolos específicos da rede).

- **Malicioso versus racional**: o atacante malicioso não busca vantagens pessoais a partir dos seus ataques e tem como objetivo prejudicar os nós ou a funcionalidade da rede. Por isso, esse pode empregar qualquer meio sem se preocupar com custos e consequências. Esta categoria de invasores é considerada a mais perigosa, uma vez que pode causar graves danos à rede [Tangade e Manvi 2013]. Ao contrário, um atacante racional busca ganho pessoal e, portanto, é mais previsível no que diz respeito às ações e aos alvos. Em [Samara et al. 2010], os autores classificam ainda um invasor como egoísta quando este informa aos outros veículos presentes na rodovia que há congestionamento na estrada, apenas para tomar proveito da situação.

- **Ativo versus passivo**: um atacante ativo é aquele que pode gerar sinais e inserir ou modificar dados na rede com o objetivo de prejudicar outros nós ou parte da rede. Estes podem gerar pacotes contendo informações falsas ou não encaminhar os pacotes recebidos. Já um invasor passivo, apenas obtém informações para posterior uso. Estes atacantes escutam o canal sem fio para coletar informações de tráfego que podem ser transferidas para outros atacantes.

- **Local versus estendido**: um atacante local está limitado ao seu alcance, mesmo que este controle algumas poucas entidades (veículos ou unidades de acostamento). Ao contrário, o invasor estendido controla várias entidades (veículos ou unidades de acostamento) que estão espalhadas em toda a rede, aumentando assim o seu escopo.

4.3.3. Ataques

Para construir uma arquitetura de segurança robusta para VANETs, é importante estudar as características dos ataques que podem ocorrer. Assim como as redes clássicas, as redes veiculares são vulneráveis a muitos ataques. O fato destas redes ainda estarem em implementação faz com que a situação seja ainda mais complicada. Alguns ataques são vislumbrados e soluções são concebidas, considerando que um dia estes ataques serão de fato lançados sobre a rede, quando esta estiver em operação [Engoulou et al. 2014]. A seguir, são descritos os principais ataques analisados na literatura.

Ataques contra a Disponibilidade

- **Negação de serviço (DoS)**: o principal objetivo desta categoria de ataques é evitar que usuários legítimos acessem aos serviços ou recursos de rede. Em VANETs, este problema pode ser crítico, quando o usuário não pode se comunicar dentro da rede e transmitir dados para outros veículos, uma vez que isto pode resultar em uma situação de risco de vida. Um atacante pode proferir ataques de DoS de três maneiras, a saber: (i) sobrecarrega o nó para que este não possa realizar outra tarefa,

 ©2014 SBC — Soc. Bras. de Computação

tornando o nó continuamente ocupado; (ii) ataca o canal de comunicação gerando altas frequências de modo que nenhum veículo seja capaz de se comunicar com outros veículos na rede, e (iii) não encaminhamento (bloqueio) de pacotes [Pathre et al. 2013]. A seguir, estão descritos outros ataques desta categoria.

- **Negação de serviço distribuída (DDoS)**: são mais graves do que os ataques de DoS, pois estes partem de diferentes localizações e em diferentes horários, porém o objetivo geral é a violação da disponibilidade de um nó ou de uma unidade de acostamento - RSU. A Figura 4.5 ilustra um ataque de três veículos (B, C, D) que enviam uma grande quantidade de pacotes contra uma unidade de acostamento (RSU), ocasionando indisponibilidade da rede. Quando outros nós tentarem acessar a RSU, não será possível, pois esta estará sobrecarregada [Pathre et al. 2013].

- **Supressão de mensagem**[2]: um atacante intercepta seletivamente pacotes da rede e suprime (bloqueia) esses pacotes que inclusive poderão ser utilizados em outro momento. O objetivo de tal ataque é, por exemplo, impedir o aviso de um congestionamento, evitando que os veículos busquem caminhos alternativos, obrigando estes a entrarem no congestionamento [Tangade e Manvi 2013].

- **Buraco negro (*black hole*)**: buraco negro é uma área da rede na qual o tráfego de rede é redirecionado ou passa naturalmente, porém, ou não há veículos neste local ou veículos maliciosos que estão nesta área se recusam a participar. Isto faz com que os pacotes de dados se percam na rede. A Figura 4.4 ilustra este ataque, no qual veículos maliciosos se recusam a transmitir a mensagem enviada pelo veículo C sobre um acidente e que deveria ser encaminhada para os veículos E e F [Al-kahtani 2012].

- **Temporização**[3]: ocorre quando um veículo malicioso recebe uma mensagem de emergência e não a transmite imediatamente aos veículos vizinhos. Ao invés de transmitir a mensagem, o veículo atrasa o envio, resultando no atraso de recebimento das mensagens pelos veículos vizinhos [Al-kahtani 2012].

- **Jamming**: é um ataque físico de negação de serviço, no qual o atacante transmite um sinal para perturbar o canal de comunicação, o que reduz a relação sinal ruído SNR (*Signal to Noise Ratio*) para o receptor [Mejri et al. 2014]. No cenário das VANETs, um atacante pode de forma relativamente fácil particionar a rede, sem comprometer os mecanismos de criptografia [Pathre et al. 2013]. Resultados publicados na literatura têm demonstrado o impacto devastador na rede causado por esses ataques [Avelar et al. 2014, Lima et al. 2013].

- **Software malicioso - *malware***: dada a existência de componentes de software para operar a unidade de bordo (OBU) e a unidade de acostamento (RSU), a infiltração de software malicioso (*malware*) é possível na rede durante a atualização/instalação do software nas unidades da rede veicular. O efeito de um *malware* é semelhante aos vírus e worms em uma rede de computadores normal, exceto que, em uma

[2]É um ataque que também viola a integridade da mensagem.
[3]Este ataque também viola a integridade.

 ©2014 SBC — Soc. Bras. de Computação

rede veicular, interrupções de funcionamento normal podem ser seguidas por sérias consequências [Mejri et al. 2014].

- ***Spam***: como na Internet, as mensagens de spam não têm nenhuma utilidade para os usuários. Em uma rede veicular, que é um ambiente de rádio móvel, este tipo de ataque consome largura de banda e provoca colisões voluntárias. A falta de uma gestão centralizada do meio de transmissão torna mais difícil controlar estes ataques. Assim como os softwares maliciosos, os *spams* aumentam significativamente a latência da rede.

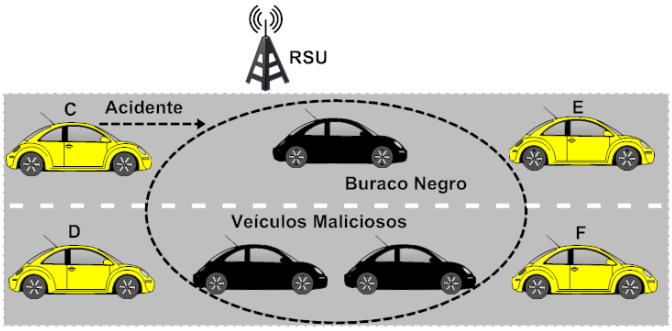

Figura 4.4. Ataque Buraco Negro (*black hole*)

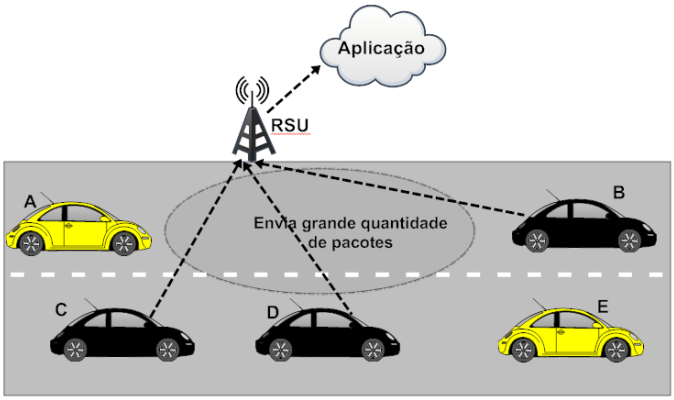

Figura 4.5. Ataque de Negação de Serviço Distribuído (*DDoS*)

Ataques contra a Autenticidade e a Identificação

- **Forjamento de endereço (*address spoofing*)**: acontece quando o ataque fabrica um pacote contendo um endereço falso de origem, fazendo com que o nó atacado acredite que a conexão está vindo de um nó com permissão para se conectar à rede [Al-kahtani 2012].

- **Mascaramento**: um veículo malicioso falsifica sua identidade e finge ser outro veículo para ganhar acesso não autorizado a um recurso da rede. Por exemplo, um veículo malicioso pode fingir ser uma ambulância para obter vantagem no trânsito. Após o mascaramento, um atacante pode introduzir ou substituir um nó de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo (p.ex uma unidade de acostamento), permitindo assim a captura de senhas de acesso e informações que por este passem a trafegar [Engoulou et al. 2014];

 ©2014 SBC — Soc. Bras. de Computação

- **Sybil**: um atacante gera múltiplas identidades para simular vários nós na rede. Cada nó transmite mensagens com múltiplas identidades. Assim, outros veículos percebem que existem muitos veículos na rede ao mesmo tempo. Por exemplo, um atacante pode fingir e agir como uma centena de veículos para convencer os outros veículos da estrada que há congestionamento, com o objetivo de convencer os veículos a trafegarem por outras estradas [Tangade e Manvi 2013].

- **Tunelamento ou *wormhole attack***: neste ataque, pelo menos dois nós maliciosas cooperam para transferir pacotes da rede veicular por um túnel privado criado por estes. O principal objetivo destes nós maliciosos é afetar os pacotes de pedido de roteamento. Neste ataque, estes nós podem diminuir o número de contagens de saltos para que o que os pacotes passem sempre pelo túnel privado [Safi et al. 2009]. Em VANETs, normalmente, para aplicações que requerem roteamento, os protocolos AODV e DSR são usados, sendo que estes são vulneráveis a este tipo de ataque.

- **Replicação do certificado ou da chave**: o ataque consiste na utilização de chaves ou certificados duplicados, que são utilizados como prova de identificação para criar ambiguidade, dificultando a identificação de um veículo pelas autoridades, especialmente em caso de disputa (repudiação) [Mejri et al. 2014].

Ataques contra a Integridade e Confiança dos Dados

- **Forjamento de dados de posicionamento do GPS (*GPS spoofing*)**: o satélite GPS mantém uma tabela com a localização geográfica e a identidade do veículo na rede. 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 et al. 2012]. Os atacantes podem ainda modificar pacotes de localização, repetir pacotes e bloquear pacotes urgentes de localização [Isaac et al. 2010].

- **Ilusão (ataque contra os sensores do veículo)**: 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. Os métodos de autenticação e integridade utilizados tradicionalmente em redes sem fio são inadequadas contra o ataque ilusão [Isaac et al. 2010, Al-kahtani 2012].

- **Injeção de informação falsa (*bogus information*)**: nesta categoria, um atacante pode ser um intruso ou um usuário legítimo que transmite informações falsas na rede veicular para obter vantagens ou afetar a decisão de outros veículos, por exemplo, em [Rawat et al. 2012, Al-kahtani 2012], os autores apresentam a transmissão de informações erradas sobre as condições de tráfego de modo a tornar mais fácil o seu movimento na estrada. O **ataque social** é um tipo de ataque desta categoria. Neste, o atacante procura confundir e distrair a vítima enviando mensagem antiética e/ou imoral para o motorista ficar perturbado. O usuário legítimo reage de forma irritada

 ©2014 SBC — Soc. Bras. de Computação

ao receber esse tipo de mensagem podendo se distrair e causar um acidente [Rawat et al. 2012]. A Figura 4.6 ilustra um exemplo deste ataque.

- **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 faz o intermédio entre a comunicação das duas vítimas, interceptando as mensagens enquanto estas acreditam que estão se comunicando diretamente. Este é um ataque que viola a autenticidade do remente e a integridade das mensagens [Mejri et al. 2014]. A Figura 4.7 mostra um ataque no qual o veículo malicioso M ouve a comunicação entre os veículos A e B, modifica o alerta recebido e propaga uma informação falsa (para os veículos B e C) como se fosse o veículo A. Em seguida, esta informação é difundida por toda a rede [Al-kahtani 2012].

- **Ataque de Mensagem Antiga - *Replay***: este é um ataque clássico que consiste em retransmitir uma mensagem já enviada, para obter benefícios referentes à mensagem no momento da sua apresentação. Por isso, o atacante injeta novamente os pacotes anteriormente recebidos na rede. Este ataque pode ser usado, por exemplo, para retransmitir quadros de *beacons*, de modo que o atacante possa manipular a localização e as tabelas de roteamento dos nós. Ao contrário de outros ataques, este pode ser realizado por falsos usuários [Mejri et al. 2014].

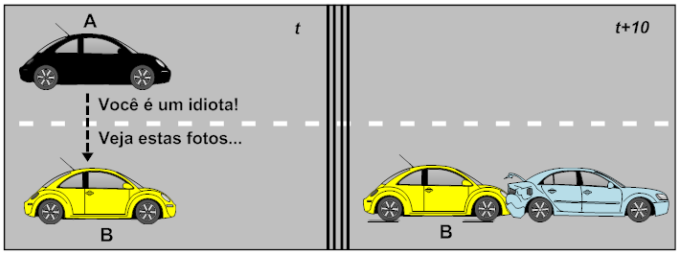

Figura 4.6. Ataque Social

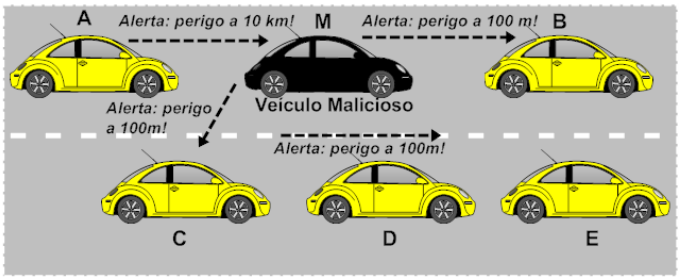

Figura 4.7. Ataque de Modificação de Mensagem (*Man in the Middle*)

Ataques contra a Confidencialidade

- **Análise de tráfego**: um atacante que venha a ter acesso à rede pode interceptar o tráfego de pacotes e coletar dados que estejam sendo transmitidos sem o uso de criptografia. Este é um ataque passivo que é executado em redes *ad hoc* [Isaac et al. 2010].

 ©2014 SBC — Soc. Bras. de Computação

- **Força bruta**: um ataque de força bruta pode ter como foco as mensagens trocadas (quebrar as chaves criptográficas) ou ainda o processo de identificação e autenticação. Em uma rede veicular, na qual os tempos de conexão são relativamente curtos, um ataque de força bruta não é fácil de realizar, uma vez que consome muito tempo e necessita de muitos recursos [Mejri et al. 2014, Pathre et al. 2013].

- **Revelação de identidade**: um atacante pode obter a identidade do proprietário de um determinado veículo violando a sua privacidade. Normalmente, o proprietário de um veículo também é seu motorista, por isso é simples a obtenção dos dados pessoais desta pessoa [Tangade e Manvi 2013].

Outros Ataques

- **Ataques contra o não-repúdio ou perda de eventos de rastreabilidade (*accountability*)**: de acordo com [Mejri et al. 2014], apesar de sua importância, não foi encontrado na literatura um documento afirmando a possibilidade deste ataque ocorrer nas redes veiculares. O ataque de não repúdio consiste em tomar medidas para permitir ao atacante negar a realização por ele de uma ou mais ações. Este tipo de ataque está essencialmente baseado na eliminação de traços de transações, criando uma confusão para a entidade de auditoria. Os ataques de *sybil* e duplicação de chaves e certificados podem servir como preliminar para o ataque de repúdio.

- **Ataques contra a privacidade**: estes ataques representam a violação da privacidade dos condutores e usuários em VANET. Vários estudos na literatura classificam os ataques de privacidade como uma categoria separada para VANETs. Como um exemplo prático, 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 [Mejri et al. 2014].

- **Conluio**: um atacante pode formar alianças com outros nós da rede para alcançar um objetivo comum. Este objetivo pode ser o vandalismo ou o terrorismo na rede, resultando na indisponibilidade da rede ou de uma aplicação ou denegrir a reputação de (confiança) um veículo [Zhang 2011].

4.3.4. Correlação dos Ataques, Perfil dos Atacantes e Propriedades Violadas

Esta seção correlaciona, através da tabela 4.2, os ataques apresentados na Seção 4.3 com o perfil do atacante e as propriedades de segurança violadas.

 ©2014 SBC — Soc. Bras. de Computação

Tabela 4.2. Comparação dos Ataques de Segurança

Nome do Ataque	Perfil do Atacante	Propriedades Violadas
Negação de serviço (DoS)	Interno ou Externo, Malicioso, Ativo, Estendido	Disponibilidade
Supressão de Mensagem	Interno, Racional, Ativo, Local	Disponibilidade Integridade
Buraco Negro (*black hole*)	Interno, Malicioso, Ativo, Local,	Disponibilidade
Temporização	Interno, Racional, Ativo, Estendido	Disponibilidade
Jamming	Interno ou Externo, Malicioso, Ativo, Local	Disponibilidade
Negação de Serviço Distribuído (DDoS)	Interno ou Externo, Malicioso, Ativo, Estendido	Disponibilidade
Software Malicioso - *Malware*	Interno ou Externo, Malicioso, Ativo, Estendido	Disponibilidade Integridade
Spam	Interno ou Externo, Malicioso, Ativo, Estendido	Disponibilidade
Forjamento de Endereço	Interno, Malicioso, Ativo, Estendido	Autenticidade
Mascaramento	Interno, Racional, Ativo, Estendido	Autenticidade
Sybil	Interno, Malicioso ou Racional, Ativo, Local ou Estendido	Autenticidade
Tunelamento ou *Wormhole*	Interno, Malicioso ou Racional, Ativo, Estendido	Autenticidade Disponibilidade
Replicação do Certificado ou da Chave	Interno, Malicioso ou Racional, Ativo, Local	Autenticidade
GPS *spoofing*	Interno ou Externo, Malicioso, Ativo, Local	Integridade Autenticidade
Ilusão	Interno, Racional, Ativo, Local	Integridade
Injeção de informação falsa	Interno, Malicioso, Ativo, Local ou Estendido	Integridade
Ataque social	Interno, Malicioso, Ativo, Local	Integridade
Modificação de mensagem	Interno, Malicioso, Ativo, Local	Integridade, Disponibilidade
Ataque de Mensagem Antiga (*Replay*)	Interno, Malicioso, Ativo, Estendido	Integridade, Disponibilidade
Análise de Tráfego	Interno ou externo, Racional ou Malicioso, Passivo, Local	Confidencialidade
Força bruta	Interno ou Externo, Racional, Ativo, Local	Confidencialidade, Autenticidade
Revelação de Identidade	Interno ou Externo, Malicioso ou Racional, Passivo, Local	Confidencialidade, Privacidade
Ataques contra o não-repúdio e *accountability*	Interno, Malicioso, Ativo, Local	Confidencialidade
Ataques contra a privacidade	Interno ou Externo, Malicioso ou Racional, Ativo, Estendido	Confidencialidade, Privacidade
Conluio	Interno, Malicioso ou Racional, Ativo, Estendido	Integridade Disponibilidade

4.4. Principais Contramedidas e suas Restrições

Esta seção apresenta as principais contramedidas existentes na literatura e suas limitações diante de conter os efeitos de ataques. A Seção 4.4.1 apresenta os serviços de segurança definidos pelo padrão IEEE 1609. A Seção 4.4.2 provê uma descrição dos mecanismos de criptografia e gerenciamento de chaves propostos para redes veiculares. A Seção 4.4.3 fornece uma visão geral sobre os mecanismos de autenticação e técnicas de anonimato. Finalmente, a Seção 4.4.4 detalha os sistemas de reputação e modelos de confiança.

4.4.1. Serviços de segurança WAVE (IEEE 1609.2)

Como descrito na Seção 4.2.2, a arquitetura WAVE é composta por seis documentos, dentre estes o documento 1609.2 especifica um conjunto de serviços para prover segurança às

 ©2014 SBC — Soc. Bras. de Computação

mensagens WAVE contra análise de tráfego (*eavesdroping*), forjamento (*spoofing*) e outros tipos de ataques em ambientes de redes veiculares [Lin et al. 2008]. 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. 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: serviços providos pela Entidade de Gerenciamento de Certificados (*CME - Certificate Management Entity*) e que 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*) e gerenciam as informações relacionadas aos certificados e às chaves privadas que são usados no envio seguro dos anúncios de serviços WAVE (WSAs).

Uma implementação do WAVE deve incluir pelo menos um dos seguintes serviços de processamento de segurança indicados na [IEEE 2013]: (i) gerar dados assinados; (ii) gerar dados criptografados; (iii) verificar os dados assinados; (iv) decriptografar e criptografar os dados; (v) gerar Serviços de Anúncio WAVE (WSA) assinados; (vi) verificar assinaturas WSA no receptor; (vii) gerar um pedido de certificado (*Certificate Signing Request - CSR*); $(viii)$ verificar resposta ao pedido de certificado; (xi) verificar a lista de certificados revogados.

Os serviços e as entidades dos Serviços de Segurança WAVE estão ilustrados na Figura 4.8. A figura mostra os pontos de acesso de serviços (SAPs -Service Access

 ©2014 SBC — Soc. Bras. de Computação

Points), que suportam as comunicações entre entidades dos Serviços de Segurança WAVE e outras entidades. A norma na IEEE 1609.2 especifica o processamento de segurança via primitivas definidas nestes SAPs.

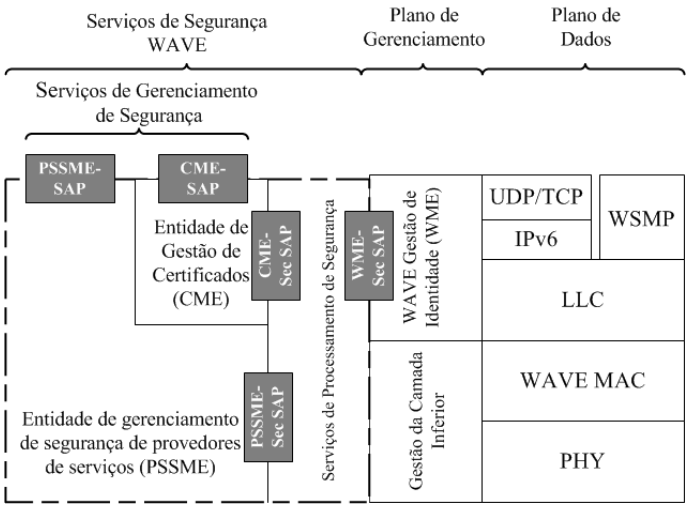

Figura 4.8. Serviços de Segurança na Pilha de Protocolos WAVE [IEEE 2013]

A Figura 4.9 ilustra o modelo geral para o processamento da segurança segundo a norma IEEE 1609.2. Os serviços de segurança são utilizados por uma Entidade de Comunicação Segura (SCE – *Secure Communications Entity*) e retornam a saída para a mesma SCE. A entidade remetente (que pode ser uma aplicação, uma outra entidade de camada superior, o WME ou qualquer outra entidade) utiliza os serviços de segurança para realizar o processamento de segurança do lado do remetente. Os resultados deste processamento são devolvidos para a entidade remetente, que, em seguida, transmite a Unidade de Dados do Protocolo de Aplicação (APDU) resultante para a entidade destinatária [IEEE 2013]. A entidade destinatária recebe a APDU e, em seguida, utiliza os serviços de segurança para realizar o processamento da segurança sobre o conteúdo da APDU. Estes retornam o resultado para a entidade remetente para processamento adicional que pode incluir várias chamadas dos serviços de segurança, caso necessário [IEEE 2013].

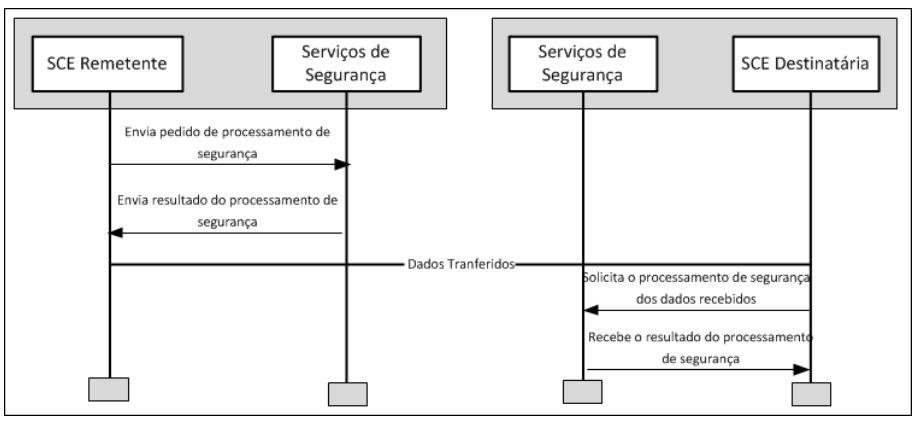

Figura 4.9. Fluxo do Processamento nos Serviços de Segurança IEEE 1609.2 [IEEE 2013]

 ©2014 SBC — Soc. Bras. de Computação

Com a norma IEEE 1609.2, tem-se uma base criptográfica sólida para a concepção de sistemas de transportes inteligentes (ITS) 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 [Schütze 2011], a implementação da norma IEEE 1609.2 em software não é uma solução muito realista, devido às limitações de desempenho. Além do problema de desempenho, os processadores automotivos atuais não têm proteção suficiente contra manipulações maliciosas. De acordo com o autor, os cartões inteligentes (*smartcards*) são uma alternativa por pelo menos duas razões: a maioria dos cartões inteligentes tem uma unidade de número longo aritmética que acelera as operações de chave pública consideravelmente e estes possuem proteção contra adulteração (*tamper resistance*). No passado, os cartões inteligentes não foram qualificados para as condições ambientais dos automóveis, mas as empresas de cartões recentemente começaram a produzir cartões especiais para uso em automóveis, por exemplo, os produtos Infineon SLI70 ou o SLM76 cartões especiais para M2M (*Machine to Machine*).

A norma IEEE 1609.2 especifica apenas os formatos e como ocorre os processamentos para prover segurança criptográfica às PDUs. Porém, a privacidade e o anonimato são questões consideradas fora do escopo, já que estas requerem atenção por parte dos desenvolvedores das diferentes partes de um dispositivo WAVE [IEEE 2013].

4.4.2. Mecanismos Criptográficos e Gerenciamento de Chaves

As aplicações de segurança (*safety*) suportadas por VANETs possibilitam a tomada de decisão por um motorista com base em mensagens recebidas de outros veículos. Contudo, se um veículo se comporta de modo malicioso, injetando ou alterando estas mensagens, este pode colocar o motorista em situação de perigo e, em alguns casos, com risco de morte [Wasef et al. 2010]. Desta forma, a autenticidade das mensagens é obrigatória para proteger as VANETs contra nós atacantes. Porém, caso as mensagens não contenham qualquer informação sensível, a confidencialidade não é necessária. Como resultado, a troca de mensagens de segurança em uma VANET precisa de autenticação, mas nem sempre de cifragem. Vários autores [Raya e Hubaux 2007, Mejri et al. 2014] escolheram as assinaturas digitais como solução para autenticação das mensagens. Neste caso, o método mais eficiente e mais simples é atribuir para cada veículo um par de chaves (privada/pública) permitindo ao veículo a possibilidade de assinar digitalmente as mensagens e, assim, autenticar-se perante os destinatários das mensagens. Diante da necessidade de responsabilização das aplicações em VANETs, a abordagem de gestão de confiança auto-organizada, como a do PGP (*Pretty Good Privacy*) não é satisfatória. As chaves públicas utilizadas em uma rede veicular devem ser emitidas e assinadas por uma autoridade confiável. A necessidade de certificados digitais emitidos por uma autoridade implica no uso de uma Infraestrutura de Chaves Públicas (ICP) veicular [Wasef et al. 2010].

O uso de uma ICP tem sido amplamente utilizado como solução para os problemas de segurança em VANETs [Raya et al. 2006b, Wasef et al. 2010]. Uma função importante de qualquer sistema ICP é a renovação e a revogação de certificados. Cada certificado emitido possui uma validade, indicando o período que ele pode ser utilizado por um determinado usuário. Antes que expire sua validade, uma autoridade certificadora (AC) pode executar o processo de renovação, emitindo um novo certificado para o usuário [Nowatkowski 2010]. A revogação de certificados é uma forma de terminar a associação

 ©2014 SBC — Soc. Bras. de Computação

de um veículo com a rede, de modo que suas mensagens sejam ignoradas.

Uma AC também possui a responsabilidade de emitir e distribuir os certificados de chave pública. Estas responsabilidades são utilizadas para auxiliar na revogação de certificados inválidos. Segundo [Al Falasi e Barka 2011], existem muitas abordagens na literatura que lidam com a informação do estado do certificado, sendo uma das mais discutidas, a distribuição de uma lista de certificados revogados (CRL do Inglês *Certificate Revocation List*). Uma CRL é gerada pela AC utilizando uma chave privada para garantir sua autenticidade e contém a relação dos certificados revogados, a data da revogação e a data de geração da lista. Conforme [Papadimitratos et al. 2008, Al Falasi e Barka 2011], as CRLs são emitidas para revogar os certificados conforme decisões técnicas ou administrativas tomadas pela AC, como por exemplo, baseadas na mudança de proprietário, roubo, ou aluguel do veículo, entre outras.

Conforme [Al Falasi e Barka 2011], o esquema de revogação segue duas abordagens, a centralizada e descentralizada. Na abordagem centralizada, uma entidade central é a única responsável pela tomada de decisão sobre as revogações. De outro lado, na abordagem descentralizada, a decisão é tomada por um grupo de veículos na vizinhança (um salto de distância) do veículo que terá o certificado revogado. De acordo com [Aslam e Zou 2009], as soluções com base em AC centralizadas devem ser organizadas de forma hierárquica para prover um gerenciamento eficiente. A hierarquia pode ser baseada em áreas (países ou continentes), que por sua vez podem ser divididas em regiões (estados ou países). Cada região teria sua AC regional e estaria ligada às demais regiões através da AC de área (raiz), com base em uma relação de confiança para realizar o processo de verificação dos certificados. Em [Al Falasi e Barka 2011], os autores ressaltam o custo computacional desse processo de verificação perante uma grande cadeia de regiões, além de ser difícil, uma vez que a distribuição destas listas deve cobrir todas as regiões, os veículos se movem de uma região para outra. Para exemplificar, se uma AC revoga um determinado certificado, é preciso distribuir esta informação em sua região e também encaminhar à AC raiz para que o mesmo encaminhe a informação para todas as demais ACs, que por sua vez, precisam espalhar a informação em suas regiões. Diversos esquemas de revogação de certificados têm sido propostos na literatura baseados nesta abordagem centralizada, como em [Laberteaux et al. 2008, Aslam e Zou 2009, Nowatkowski 2010, Haas et al. 2011].

Em uma solução descentralizada de revogação de certificados, os veículos são responsáveis por tomar a decisão de excluir da rede um determinado veículo por mau comportamento. Uma AC pode ser utilizada para fazer a revogação, contudo, a decisão e a execução do processo de despejo são dos veículos. Este processo é conhecido como exclusão de nós (*node eviction*), e possui diversas fases, como a detectar o veículo com mau comportamento, relatar o mau comportamento, revogar do certificado (função das ACs) e disseminação da informação [Kherani e Rao 2010]. Existem algumas abordagens utilizando esta solução descentralizada, como por exemplo [Wasef e Shen 2009].

Uma forma alternativa para assinatura digital de mensagens em redes veiculares são os mecanismos de assinatura sem certificados, por exemplo, os que fazem uso de criptografia baseada em identidade (do inglês *Identity-Based Cryptography - IBC*) [Karagiannis et al. 2011, Silva et al. 2008]. O uso de criptografia baseada em identidade elimina a necessidade de verificar a validade dos certificados na tradicional infraestrutura de chave

 ©2014 SBC — Soc. Bras. de Computação

pública (ICP). Nestes sistemas criptográficos, a chave pública de cada usuário é facilmente calculável a partir de uma sequência arbitrária correspondente à identidade do usuário (por exemplo, um endereço de e-mail, um número de telefone, etc). Os mecanismos de assinatura que fazem uso de IBC são muitos eficientes e recomendados para redes veiculares, pois uma entidade verificadora (por exemplo, uma unidade de bordo - OBU) não necessita armazenar, buscar e verificar os certificados de chaves públicas assinados por uma terceira autoridade confiável [Biswas et al. 2011].

De acordo com [Schleiffer et al. 2013], mecanismos de segurança com base em criptografia já estão sendo aplicados em veículos, em especial, para proteção contra furto, falsificação e atualização segura de softwares. Para proteção contra roubo e falsificação, mecanismos de criptografia que utilizam chaves simétricas ou assimétricas têm sido utilizados. Para atualização segura de softwares utiliza-se basicamente um par de chaves (pública/privada) baseadas em RSA. A chave pública é armazenada no veículo, e a privada em um servidor, que a utiliza para assinalar um *firmware* o qual posteriormente será verificado pelo veículo. A atualização segura de software é encontrada na maioria dos veículos, sendo utilizadas geralmente para sistemas de informação, entretenimento, segurança e em ECUs (*Eletric Control Unit*).

Nos trabalhos de [Schleiffer et al. 2013, Wolf e Gendrullis 2012] são apresentadas as principais iniciativas da indústria automobilística para prover mecanismos de segurança baseados em criptografia, a exemplo do consórcio HIS (*Hersteller Initiative Software*) da Alemanha, que especificou o SHE (*Secure Hardware Extension*). Através de um esquema básico de gerenciamento de chaves, SHE utiliza uma única chave simétrica por veículo, instalada em cada ECU na linha de montagem. Sua funcionalidade central é o armazenamento das chaves simétricas e as operações básicas (encriptação/decriptação) com estas chaves, a fim de prover a atualização segura de aplicações do veículo e outras operações. Outro exemplo é o projeto de pesquisa Europeu EVITA, o qual busca desenvolver três módulos de segurança, EVITA *light*, EVITA *medium* e EVITA *full*. O foco desta iniciativa é a segurança da comunicação V2V/V2I.

Segundo [Mejri et al. 2014], a criptografia moderna oferece diversas técnicas de segurança que atendem aos requisitos de confidencialidade, autenticidade, integridade, não-repúdio, entre outros (ver Seção 4.3.1), presentes nas VANETs, sendo utilizadas como contramedidas aos diferentes tipos ataques existentes nas VANETs:

- **Contra Negação de Serviço (DoS):** uso de mecanismos de autenticação baseados em assinatura e *bit commitment*;
- **Contra *Jamming*:** troca do canal de comunicação e utilização da técnica FHSS (*Frequency Hopping Spread Spectrum*), a qual envolve algoritmos criptográficos para gerar números pseudo-aleatórios para o algoritmo de salto;
- **Contra Ataques de Supressão de Mensagem:** uso de uma ICP veicular ou da técnica de *zero-knowledge*;
- **Contra Buraco Negro:** para estes tipos de ataques não existem soluções de criptografia reais, porém, o uso de hardwares confiáveis, assinatura digital em softwares e sensores podem minimizar os efeitos dos seguintes ataques;

 ©2014 SBC — Soc. Bras. de Computação

- **Contra Temporização:** utilizar técnica de *timestamp* (baseada em assinatura digital e em funções *hash*) para controle de tempo em aplicações sensíveis ao atraso de pacotes;
- **Contra GPS *Spoofing*:** uso de mecanismos de *bit commitment*, juntamente com sistemas de posicionamento para aceitar somente dados de localização autênticos;
- **Contra Força Bruta:** uso de algoritmos de geração de chaves e encriptação fortes, que sejam inquebráveis dentro de um espaço de tempo razoável;
- **Contra *Sybil*:** reforçar os mecanismos de autenticação com uso de técnicas de criptografia como *bit commitment* e *zero-knowledge*;
- **Contra Replicação do Certificado ou Chave:** uso de chaves e certificados descartáveis; checagem da validade dos certificados digitais em tempo real através da lista de certificados revogados; uso de certificação cruzada entre diferentes ACs envolvidas no esquema de segurança.
- **Ataque de Mensagem Antiga (*Replay*):** as mensagens devem incluir o timestamp. Ele é utilizado pelo receptor para verificar se a mensagem já não está em cache e também para evitar este tipo de ataque. Este tipo de contramedida, que busca garantir a troca de mensagens seguras, está presente no IEEE P1609.2 [Laurendeau e Barbeau 2006].
- **Análise de Tráfego e *Eavesdropping*:** para estes tipos de ataques é necessário criptografar somente as mensagens importantes, as quais colocam em risco a privacidade do usuário, como dados de posicionamento (GPS), identificação do veículo, etc.

Em relação aos esquemas de comprometimento de bit (*bit commitment*) e conhecimento zero (*zero-knowledge*) citados pelo autor, o comprometimento de bit é uma das primitivas fundamentais da criptografia moderna, sendo uma ferramenta essencial na construção de protocolos criptográficos. Um problema comum em criptografia é uma parte A obter provas de que uma outra parte B é quem realmente afirma ser. Atualmente existem muitas formas de se provar uma identidade utilizando a criptografia, como uso de protocolos criptográficos, assinaturas digitais, esquemas que empregam a prova de conhecimento zero, etc. Nos esquemas de prova de conhecimento zero, uma parte A não conhece os detalhes da mensagem da outra parte, mas utiliza determinados meios para verificar se a mensagem é de quem afirma ser (autenticidade) [Ribeiro et al. 2004, Mohr 2007]. Em [Ribeiro et al. 2004] são abordados os principais esquemas de chave pública que empregam a prova de conhecimento zero.

Em geral, um protocolo que usa o esquema de comprometimento de bit segue duas fases, (i) o comprometimento e (ii) a abertura, sendo estas executadas por duas partes, A e B. Inicialmente, A se compromete com um valor v, enviando determinadas informações para B que contenha vestígios do valor v. De modo esperado, B não deve ser capaz de descobrir o valor v a partir dos vestígios do valor encaminhado ou entre as possíveis interações com A. Somente na fase de abertura, A pode revelar a B o valor v, que por sua vez pode verificar se o mesmo corresponde ao valor esperado com base nos vestígios enviados preliminarmente [Juels e Wattenberg 1999, Alves 2011, Pinto 2013].

 ©2014 SBC — Soc. Bras. de Computação

4.4.3. Mecanismos de Autenticação e Técnicas de Anonimato

Dentre os desafios de segurança em redes veiculares, um dos mais atuais é prover autenticidade e não repúdio, além de preservar a privacidade dos dados durante uma comunicação [Mejri et al. 2014]. Estes requisitos são em alguns momentos conflitantes [Isaac et al. 2010]. Diante das inovadoras aplicações em redes veiculares, um atacante pode controlar um veículo, observando seus padrões de comunicação e movimento. O anonimato é uma preocupação crítica em VANETs e visa ocultar a identidade física de um nó (geralmente um veículo) [Isaac et al. 2010].

O anonimato em redes veiculares é utilizado para evitar ataques por rastreamento e impedir que entidades não autorizadas sejam capazes de localizar ou rastrear a trajetória de um veículo ou grupo de veículos. Em especial, uma entidade não autorizada não deve ser capaz de saber se mensagens diferentes foram criadas pelo mesmo nó. O anonimato dos veículos pode ser garantido pelo uso de pseudônimos que não indicam a identidade dos seus proprietários. Estes pseudônimos podem ser chaves recebidas por uma Autoridade Certificadora (AC), por unidades de acostamento (RSUs) ou que estejam instaladas nas unidades de bordo dos veículos [Chen et al. 2011]. Um problema ocorre quando um veículo totalmente anônimo transforma-se em um veículo malicioso. Neste caso, pode não haver maneira de identificá-lo para revogar o seu anonimato e puni-lo [Huang et al. 2014].

Os mecanismos de segurança devem fornecer privacidade (anonimato) para os veículos, porém também devem ser capazes de monitorar o comportamento destes veículos para que quando um veículo assuma um comportamento inadequado (malicioso), este possa ser identificado. Em outras palavras, os veículos em uma VANET precisam ter uma privacidade condicional. Ou seja, a privacidade dos veículos será garantida se eles se comportarem de forma adequada na rede. Caso contrário, a privacidade deve ser revogada e estes não permanecerão mais como anônimos [Huang et al. 2014, Chuang e Lee 2011, Xiong et al. 2013]. A seguir, são apresentados mecanismos e técnicas de anonimato em VANETs mais proeminentes na literatura.

PAAVE [Paruchuri e Durresi 2010]

O Protocolo para Autenticação Anônima em Redes Veiculares (do inglês, *Protocol for Anonymous Authentication in Vehicular Networks*) [Paruchuri e Durresi 2010] aborda a preservação da privacidade com rastreabilidade de autoridade usando cartões inteligentes (*smartcards*), que geram dinamicamente as chaves anônimas. O protocolo faz uso de um módulo de segurança veicular (VSM), em um cartão inteligente, para armazenar de forma segura as informações de identidade de um veículo, incluindo informações do condutor e todas as chaves criptográficas necessárias para comunicação com outros veículos e com as unidades de acostamento (RSUs). Os cartões VSM armazenam informações usadas para autenticar e identificar as OBUs pertencentes a rede veicular.

A Figura 4.10 ilustra a arquitetura proposta para comunicação e autenticação anônima. Toda comunicação a partir de uma OBU passa através do VSM para ser criptografada antes da transmissão. Qualquer mensagem recebida também é decriptografada pelo VSM. Isto ocorre pois é o cartão VSM que armazena as chaves criptográficas necessárias e que executa os protocolos criptográficos. A autoridade confiável da rede veicular (TA, do inglês *Trusted Authority*) é responsável por (i) iniciar os VSMs, (ii) manter o registro das

 ©2014 SBC — Soc. Bras. de Computação

identidades dos membros da rede e (iii) emitir os certificados das OBUs. O protocolo PAAVE compreende principalmente os seguintes elementos:

- **Mecanismo de Autenticação**: antes de enviar ou receber qualquer mensagem, cada OBU precisa se autenticar em uma RSU (protocolo de desafio-resposta baseado em criptografia de chave pública). A autenticação deve ocorrer mesmo quando a RSU estiver fora do raio de comunicação da OBU. Neste último caso, o processo será intermediado por outras OBUs.
- **Chaves de Sessão para Comunicação**: cada RSU gera uma nova chave de sessão no início de cada sessão. Esta chave de sessão é dada a todas as OBUs autenticadas pela RSU, assim, a chave de sessão pode ser vista como uma chave de grupo compartilhada por todas as OBU autenticadas pela mesma RSU. As OBUs autenticadas por diferentes RSUs receberão chaves de sessão diferentes. Para tratar deste problema, no início de cada sessão, cada RSU se comunica com RSUs vizinhas e obtém as suas chaves de sessão e os seus identificadores. Quando um nó (OBU) se registra em uma RSU, a RSU envia todas as chaves de sessão das RSUs vizinhas, juntamente com a sua própria chave de sessão e os identificadores de chave correspondentes. Cada vez que uma OBU recebe um aviso de uma nova RSU, esta obtém o novo conjunto de chaves de sessão da RSU.
- **Mecanismo de Comunicação e Verificação de Mensagens**: sempre que uma OBU tem que transmitir uma mensagem m, a mensagem é criptografada pelo módulo VSM com a chave de sessão compartilhada dentro do *cluster* de RSUs.

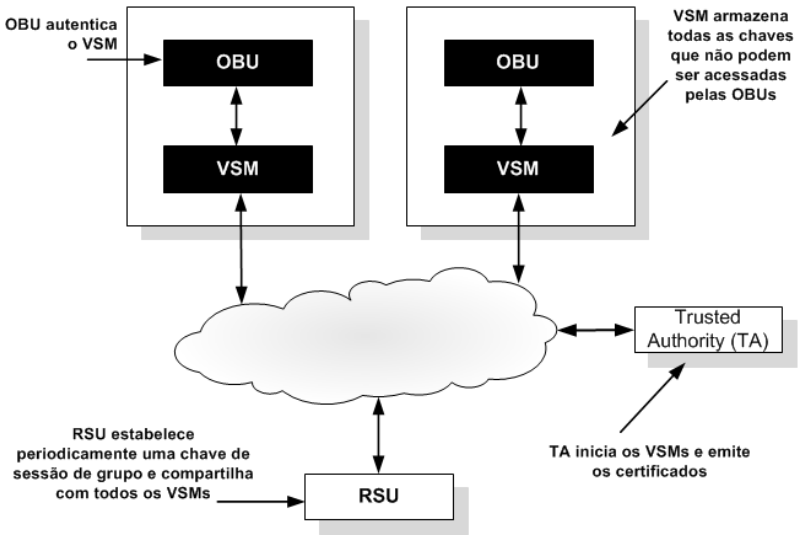

Figura 4.10. Arquitetura: Comunicação e Autenticação Anônimas [Paruchuri e Durresi 2010]

O PAAVE não faz uso de listas de certificados revogados (CRLs - *Certificate Revocation Lists*), pois esta técnica causa uma sobrecarga de armazenamento e de processamento significativa em cada OBU. No protocolo, como cada OBU precisa se autenticar em uma RSU para obter a chave de sessão, esta pode negar um pedido de OBUs maliciosas. Além disso, cada RSU compartilha informações sobre OBUs maliciosas com todas as

 ©2014 SBC — Soc. Bras. de Computação

outras RSUs. Isto evita que a OBU obtenha uma chave de sessão de qualquer ponto da rede. Além disso, se a OBU está se movendo de uma RSU para outra, esta tem que se re-autenticar na nova RSU, assim os privilégios de comunicação da OBU podem ser revogados mesmo antes do fim da sessão.

De acordo com [Paruchuri e Durresi 2010], o protocolo PAAVE apresenta melhor eficiência em relação a propostas anteriores [Lin et al. 2007, Raya e Hubaux 2007, Lu et al. 2008], em termos de armazenamento de chaves anônimas, sobrecarga de comunicação e tempo computacional para verificar mensagens.

AOSA [Weerasinghe et al. 2010]

As comunicações intermediadas por unidades de acostamento (RSUs) podem ser usadas para rastrear a localização dos veículos, sendo uma séria ameaça à privacidade dos usuários. O protocolo AOSA (*Anonymous Online Service Access*) [Weerasinghe et al. 2010] possibilita acesso anônimo aos serviços online com garantia de privacidade de localização, através de não rastreabilidade (*unlinkability)*. No protocolo AOSA, os autores consideram um modelo de rede veicular segura composta por unidades de bordo (OBUs), unidades de acostamento (RSUs) e servidores de aplicação (administrativos), os quais possibilitam comunicação V2V e V2I. As RSUs estão fisicamente conectadas à infraestrutura da VANET por meio de uma rede cabeada e são gerenciadas por uma autoridade confiável (p.ex. o Departamento de Trânsito). Além disso, uma autoridade de registro confiável (AR) fornece serviços de registro aos veículos. Todos os veículos devem se registrar na AR antes de ingressar na VANET. Uma Infraestrutura de Chaves Públicas (ICP) é implementada na rede veicular e a AR também pode funcionar com uma Autoridade Certificadora (AC) para gerenciar as chaves e os certificados dos veículos. A confiança entre as entidades é mantida, usando chaves e certificados emitidos pela AC confiável.

Para comunicação anônima segura, cada veículo usa chaves privadas/públicas anônimas, chamadas pseudo chaves, com um certificado de chave pública assinado pela AC. Estas pseudo chaves e os certificados são alterados com frequência para manter a privacidade de localização. Pode-se usar um grande número de pares de chaves e certificados pré-carregados ou adquirir frequentemente pseudo chaves e certificados de curta validade junto às RSUs. Em conformidade com a norma IEEE 1609.2, cada mensagem V2V e V2I deve conter a assinatura da mensagem e o certificado de chave pública. Portanto, os veículos usam a pseudo chave corrente para assinar e verificar as assinaturas, fazendo uso do certificado anexado e da chave pública da AC.

A execução do protocolo segue duas fases. Na **primeira fase**, todos os veículos e prestadores de serviços devem se registrar junto à AR. Os veículos que desejam usar serviços online devem também se inscrever para o serviço requirido por meio da AR. Quando AR/AC emite as pseudo chaves públicas/privadas, o certificado de chave pública deve incluir informações sobre todos os serviços registrados com uma assinatura cega (*blind signature*) de cada provedor de serviços. Os veículos só podem usar a parte específica do certificado para o pedido de serviço específico. Cada informação de serviço é criptografada com a chave pública do provedor de serviços, para que cada provedor possa acessar apenas às suas próprias informações.

No protocolo AOSA, os veículos formam grupos dinamicamente, e pequenas

 ©2014 SBC — Soc. Bras. de Computação

assinaturas de grupo são usadas para lidar com todas as chaves e assinaturas do grupo [Boneh et al. 2004]. A viabilidade do uso de chaves de grupos em cenários VANET está sendo usada e avaliada em diversas pesquisas [Raya e Hubaux 2007, Lin et al. 2007]. Todos os membros de um grupo compartilham uma chave pública de grupo e cada veículo membro tem uma chave secreta única que pode ser utilizada com a chave pública do grupo comum. Além disso, todos os membros compartilham um conjunto de identificadores temporários comuns. Duas assinaturas de um mesmo veículo não podem ser ligadas entre si. No entanto, o líder do grupo e a autoridade de registro podem colaborar para descobrir a verdadeira identidade do assinante da mensagem.

Na **segunda fase**, quando um veículo necessita acessar um serviço, este envia uma solicitação de acesso ao serviço por meio do líder do grupo. A mensagem de pedido deve ser assinada pelo veículo, usando seu pseudônimo atual e o certificado de chave pública emitido pela AC deve ser incluído. Esta mensagem de pedido é primeiro criptografado com a chave pública do prestador de serviços e então é criptografado com a chave secreta do grupo pelo veículo fonte. A mensagem é então enviada para o líder do grupo. O líder do grupo decifra a mensagem e adiciona a sua assinatura e o certificado de chave pública do grupo e encaminha a nova mensagem para um servidor *proxy* através da RSU. O servidor *proxy* verifica o certificado do líder do grupo e encaminha o pedido ao provedor de serviço solicitado. O servidor *proxy* também mantém um registro da localização da RSU que encaminhou a mensagem para fins de resposta. Depois de receber o pedido de serviço, o provedor de serviços decifra o pedido com a sua chave privada e, em seguida, atesta as credenciais anônimas do veículo, usando o certificado do serviço e a chave pública da AC. Finalmente, o provedor de serviços verifica a autorização do veículo para o serviço. O provedor de serviços envia uma chave de sessão para compartilhar com o veículo. Esta mensagem é primeiro criptografada com a chave pública anônima do veículo e, em seguida, encriptada com a chave pública do líder do grupo.

No protocolo AOSA, para comunicação anônima segura entre veículos e provedores de serviços, observa-se o uso de diversas operações de cifragem e de assinatura baseadas em criptografia assimétrica que acarretam sobrecarga computacional que, dependendo da aplicação, pode não ser desprezível. Nas simulações realizadas, os autores não compararam os impactos (sobrecarga) do protocolo AOSA em relação aos outros procolos que também garantem a comunicação anônima.

TEAM [Chuang e Lee 2011]

De acordo com os autores em [Chuang e Lee 2011], os esquemas de autenticação seguras suportados por criptografia assimétrica não são adequados para ambientes altamente dinâmicos como as VANETs, pois estes esquemas não lidam com o processo de autenticação de forma eficiente. Diante desta limitação, os autores propuseram um esquema de autenticação leve, descentralizado, chamado TEAM (*Trust-Extended Authentication Mechanism*) para comunicação V2V. O mecanismo é leve porque usa apenas operações XOR e uma função *hash*. O mecanismo TEAM adota ainda o conceito de relações de confiança transitiva para melhorar o desempenho do processo de autenticação. O mecanismo proposto satisfaz os seguintes requisitos de segurança: anonimato, privacidade de localização e autenticidade.

No modelo de rede assumido pelos autores, os veículos podem ser classificados com os seguintes papéis (ver Figura 4.11): i) Executor da Lei (VL), como um carro de

 ©2014 SBC — Soc. Bras. de Computação

polícia que funciona como um servidor de autenticação móvel (SA); ii) Veículo Não Confiável (VNC); e iii) Veículo Confiável (VC). Os autores assumem como premissas que cada unidade de bordo (OBU) dos veículos é equipada com um hardware de segurança, que inclui um *Tamper Proof Device - TPD* para prover o processamento criptográfico das informações e um *Event Data Recorder - EDR*, e que o VL é um veículo confiável. Um veículo é considerado confiável se este puder autenticar-se com sucesso, caso contrário, ele é considerado não confiável. Em um ambiente de comunicação segura, uma OBU deve-se autenticar com sucesso antes de acessar um serviço. Entretanto, nas redes de comunicação V2V, como o número de veículos executores da lei (VLs) é finito, uma OBU nem sempre tem um VL em sua vizinhança. Os autores se baseiam no conceito de relações de confiança transitiva para tratar esta questão, conforme ilustrado na Figura 4.12.

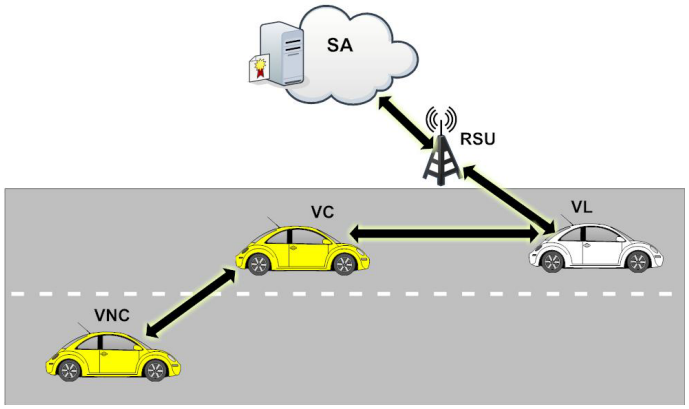

Figura 4.11. Modelo de Rede Veicular [Chuang e Lee 2011]

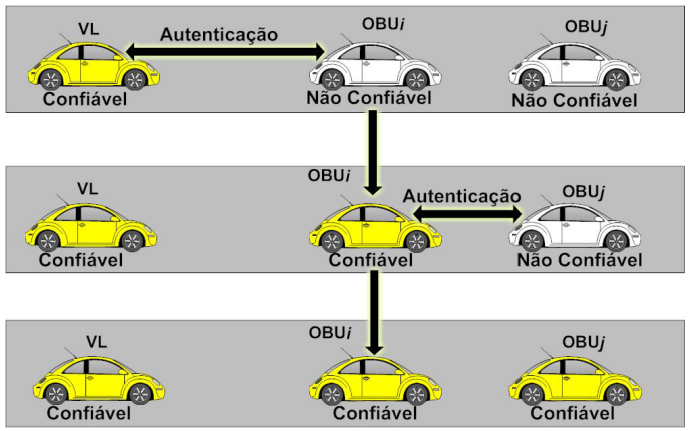

Figura 4.12. Relação de Confiança Transitiva no TEAM [Chuang e Lee 2011]

Na Figura 4.12, inicialmente, existem três veículos na rede: um VL confiável e dois outros veículos que não são confiáveis (OBU_i e OBU_j). A OBU_i torna-se confiável quando esta autentica-se no VL. Neste momento, OBU_i recebe a autorização para autenticar outras OBUs. Em seguida, como o VL não está acessível para a OBU_j, esta pode se autenticar diretamente na OBU_i (já que esta, após a autenticação, assume o papel de VL temporário). Como resultado, todos os veículos de uma VANET podem concluir o processo de autenticação rapidamente, fazendo uso de relações de confiança transitivas.

 ©2014 SBC — Soc. Bras. de Computação

O mecanismo TEAM é um esquema de autenticação descentralizado, logo um veículo executor da lei (VL) não necessita manter informações de autenticação de todos os veículos. As principais operações do mecanismo são: registro inicial, login, autenticação geral e procedimentos de autenticação de confiança estendida. Antes de um veículo poder participar de uma rede veicular, sua OBU deve-se registrar no servidor de autenticação (AS). Quando um usuário quer acessar um serviço, este deve realizar o login na OBU do veículo e então passa pelos procedimentos de autenticação geral. É importante destacar que os passos para autenticação geral (entre OBU e um VL) e para autenticação de confiança estendida (entre OBU não confiável e OBU confiável) são os mesmos.

Os autores não tratam o problema de nós que, após autenticados, passam a se comportar de forma maliciosa na rede e que por isto precisam ter o seu anonimato revogado. Ataques de negação de autenticação estendida também podem ser executados por estes nós maliciosos. Devidos às relações de confiança transitivas, conluios podem ser facilmente formados para atacar a rede.

LPP [Shen et al. 2012]

No LPP (*Lightweight Privacy-Preserving Protocol*), o mesmo modelo de rede veicular segura adotado no projeto do protocolo AOSA é assumido como premissa. O LPP provê autenticação mútua entre OBUs e RSUs e faz uso de assinatura de *hash chameleon* baseada em curvas elípticas. No esquema de assinatura proposto pelos autores, a chave pública é atualizada a cada sessão de autenticação (chaves públicas dinâmicas). O protocolo segue três fases: registro; autenticação mútua e rastreamento da Autoridade Certificadora (AC).

Na **fase de registro**, as RSUs e OBUs devem se cadastrar junto a uma AC e efetuar uma pré-carga com informações secretas. Na fase de registro de uma OBU, esta gera um número aleatório como sua chave secreta e a envia juntamente com parâmetros de inicialização do algoritmo de assinatura *chamelon* e a sua identidade real para a AC. A AC gera um certificado com um tempo de expiração e o assina. Este certificado e o identificador da OBU são armazenados na base de dados da AC e enviados à OBU.

Antes de efetuar alguma troca de mensagem, uma RSU e uma OBU devem se **autenticar mutuamente** com as informações pré-carregadas na fase de registro. Nesta fase, a RSU é quem incia a autenticação com a OBU e então estas estabelecem um par de chaves. A RSU gera uma nova chave privada com a chave pública correspondente, de modo a evitar a rastreabilidade. Finalmente, a informação é enviada para a OBU. Ao receber essa informação, a OBU usa a chave pública da AC para verificar a legitimidade da RSU. Caso ocorra um evento de disputa, a AC executa a **fase de rastreamento** para recuperar a identidade real da OBU. Para isto, a RSU deve enviar o certificado da OBU para a AC, para que a identidade da OBU possa ser encontrada no banco de dados da AC.

O protocolo LPP garante o anonimato e a não rastreabilidade devido às seguintes propriedades: (i) as informações enviadas pelas OBUs usam diferentes chaves públicas de diferentes sessões, desta forma não é possível rastrear um veículo; (ii) as informações relacionadas com os certificados são criptografadas utilizando o par de chaves da sessão, de tal forma que o certificado verdadeiro não possa ser extraído; e (iii) o par de chaves é atualizado em todas as sessões.

 ©2014 SBC — Soc. Bras. de Computação

PA-CTM [Amro et al. 2013]

De acordo com [Amro et al. 2013], os sistemas de monitoramento de tráfego colaborativo (CTM, *Collabortative Traffic-Monitoring*) são divididos em duas abordagens de acordo com a tecnologia de comunicação de dados subjacente. A primeira é baseada no uso de comunicação de curto alcance dedicada (DSRC) que suporta comunicações V2V e V2I, chamados de sistemas de infraestrutura dedicada (DI - *Dedicated Infrastructure*). A segunda se baseia no uso de tecnologias existentes, como tecnologias de comunicação celulares e outras utilizadas em redes sem fio locais, a fim de criar um sistema de transporte inteligente (ITS). Os sistemas aplicando esta abordagem, chamados de sistemas de infraestrutura existente (EI - *Existing Infrastructure*), seguem uma arquitetura cliente servidor, na qual os clientes enviam suas informações de localização para um servidor, podendo obter uma visão geral do tráfego a partir deste servidor.

O sistema PA-CTM (*Privacy Aware Collaborative Traffic Monitoring System*) [Amro et al. 2013], suportado pela abordagem EI, possibilita aos usuários autenticar-se em servidores de monitoramento de tráfego de forma anônima utilizando pseudônimos. O sistema também permite revelar as identidades por propósitos de força de lei, quando necessário. Os usuários são capazes de mudar seus pseudônimos e, portanto, ocultar suas informações de trajetória completa no servidor de tráfego. O sistema usa um mecanismo autônomo de atualização de localização (ALUM - *Autonomous Location Update Mechanism*) não dependente de uma terceira parte confiável, além de usar apenas parâmetros locais (velocidade e direção) para iniciar uma atualização de localização ou de pseudônimo.

A Figura 4.13 ilustra a arquitetura do PA-CTM. No passo 1, um veículo gera um número de identidades temporárias (pseudônimos) e envia para o sistema CoRPPS (*Collusion Resistant Pseudonym Providing System*) que é um sistema confiável resistente a ataques de conluio. O CoRPPS é composto por três unidades funcionais: i) unidade de registro; ii) unidade de autenticação; e iii) unidade de assinatura de pseudônimos, que cooperam para assinar os pseudônimos dos usuários (passo 2). No passo 3, o veículo se autentica no servidor de tráfego, usando um dos pseudônimos assinados. Os usuários são capazes de alterar os pseudônimos de tempos em tempos e então dividir sua trajetória real em pequenas trajetórias identificadas por seus pseudônimos. No passo 4, o servidor de tráfego verifica a assinatura do pseudônimo recebido e responde para o veículo com o

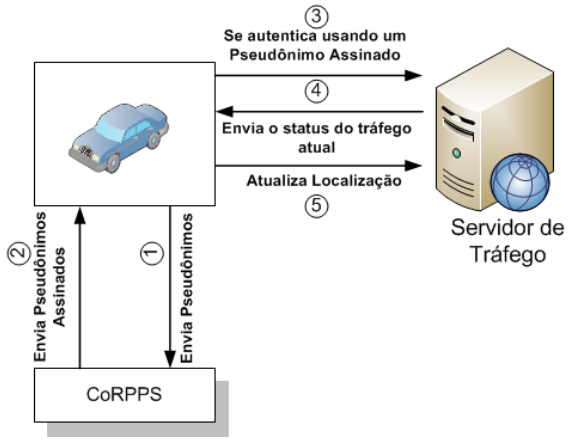

Figura 4.13. Arquitetura e Fluxo do PA-CTM [Amro et al. 2013]

 ©2014 SBC — Soc. Bras. de Computação

status do tráfego atual. Por fim, no passo 5, o veículo atualiza sua localização, utilizando apenas parâmetros locais (velocidade e direção).

Esses pseudônimos são gerados através do sistema CoRPPS (*Collusion Resistant Pseudonym Providing System*). O CoRPPS proporciona confiança entre todas as partes do sistema e é resistente contra ataques de conluio. Os usuários podem assinar seu primeiro pseudônimo e, assim, usar os pseudônimos assinados para autenticar-se no servidor.

Protocolo para Preservação de Privacidade e Confidencialidade [Xiong et al. 2013]

Em [Xiong et al. 2013], os autores apresentam um protocolo eficiente para preservação da privacidade e confidencialidade para redes veiculares baseado em *signcryption* de grupo, uma primitiva de chave pública que desempenha simultaneamente as funções de assinatura digital e cifragem. O modelo proposto apresenta as seguintes características: (i) oferece autenticação anônima condicional, na qual o emissor da mensagem pode autenticar-se anonimamente em nome de um grupo de assinantes (veículos), enquanto apenas uma autoridade confiável pode revelar a verdadeira identidade do remetente; (ii) oferece confidencialidade aos motoristas contra observadores não autorizados durante a comunicação; e (iii) é eficiente, uma vez que não necessita de um grande espaço para armazenar os dados do protocolo em cada veículo, pois a verificação de mensagens é rápida, e o rastreamento da identidade de um veículo tem um custo baixo.

Conforme ilustrado na Figura 4.14, o modelo de sistema seguro assumido no trabalho é composto pelo Gerente Membro (MM) (do inglês, *Member Manager*) e as unidades de bordo (OBUs) instaladas nos veículos. A solução não depende de unidades de acostamento (RSUs). Antes dos veículos (OBUs) se conectarem em uma rede veicular estes precisam pré-carregar os parâmetros públicos do sistema MM e gerar suas próprias chaves privadas que serão armazenadas em um TPD (*tamper-proof device*) do veículo. Estes veículos irão registra-se no MM como membros de um grupo (p.ex. envio). O MM é o responsável por registrar todas as OBUs instaladas nos veículos e por revelar a identidade real de um emissor de uma mensagem sempre que necessário. Por fim, um MM é uma entidade confiável equipada com ampla capacidade de armazenamento e processamento.

A Figura 4.14 ilustra a operação do protocolo. Quando um veículo quer enviar mensagens na rede veicular, após a fase de registro no MM como membro de um grupo de envio, o mesmo deve assinar e cifrar (*signcryption*) a mensagem em nome do seu grupo e transmiti-la em *broadcast*. Além disso, o grupo de recebimento deverá ser indicado quando a mensagem for cifrada. O protocolo de comunicação proposto está baseado no esquema de assinatura de grupo cifrada proposto em [Kwak et al. 2006].

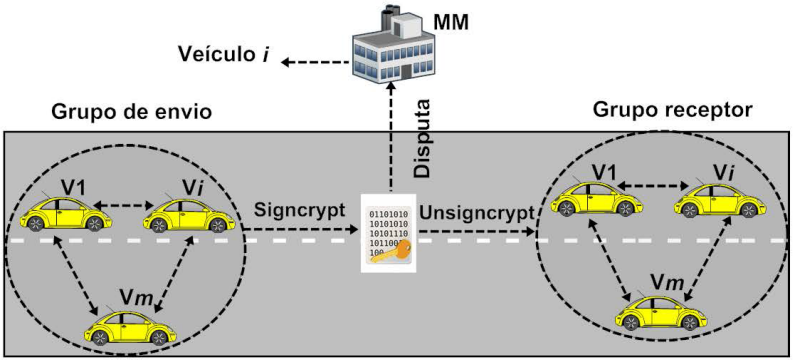

Figura 4.14. Operação do Protocolo Proposto por [Xiong et al. 2013]

 ©2014 SBC — Soc. Bras. de Computação

PPSCP [Mikki et al. 2013]

Em [Mikki et al. 2013], os autores propuseram o protocolo PPSCP (*Privacy Preserving Secure Communication Protocol*) para garantir a privacidade dos veículos em redes veiculares. Os objetivos do PPSCP incluem: autenticar mensagens de segurança de trânsito anonimamente para garantir a privacidade do veículo evitando assim o rastreamento do mesmo sem autorização; fornecer uma autoridade confiável (AC), capaz de identificar e reconhecer a identidade do veículo a partir de suas mensagens de segurança o que possibilita a rastreabilidade dos veículos; revogar chaves de veículos de forma eficiente, reduzindo o tamanho das listas de revogação; proteger contra ataques de negação de serviço (DoS) e *replay*; aumentar a eficiência do sistema, diminuindo o tempo necessário para autenticação dos veículos e verificação de mensagens dos veículos.

Cada veículo é equipado com o TPD (*Tamper-Proof Device*) que armazena as chaves criptográficas geradas pela AC. Além disso, o TPD executa todas as operações criptográficas necessárias pelo protocolo PPSCP. A identidade do veículo emissor de uma mensagem é cifrada com a chave pública da AC e somente esta pode revelar a identidade do veículo. A identidade cifrada, que é incluída na mensagem de segurança de trânsito, não está relacionada com a mensagem em si e pode ser pre-inicializada para reduzir o tempo. O PPSCP é composto por vários algoritmos. Parte dos algoritmos é usada na comunicação V2V, como por exemplo para proteger mensagens de segurança de trânsito (localização do veículo, velocidade e aceleração) e para verificar as mensagens recebidas. Outra parte dos algoritmos é aplicada na comunicação V2I, quando veículos solicitam um conjunto de chaves compartilhadas.

O gerenciamento de chaves no PPSCP é dado da seguinte forma: cada veículo (n) tem uma identidade única ($VIDn$) de 64bits. A AC é responsável por gerar e instalar as $VIDn$ em cada veículo (no TPD). A AC também gera um par de chaves pública e privada ($PubN$, $PrivN$) para cada veículo. Além do $VIDn$, a AC pré-instala o par de chaves do veículo e também a sua chave pública ($PubCA$) no dispositivo TPD de cada veículo. Para garantir o anonimato dos veículos, AC gera periodicamente um conjunto de chaves chamado de "conjunto de chaves compartilhadas", que contém N chaves simétricas. Estas chaves são usadas para autenticação de mensagens entre os veículos. Cada veículo solicita este conjunto de chaves a AC, enviando uma mensagem criptografada com a chave pública a AC. A AC responde com uma mensagem que contém o conjunto de chaves compartilhadas. Essas mensagens são então criptografadas com a chave do veículo.

A autenticação de mensagens é feita com o conjunto de chaves simétricas compartilhadas com todos os veículos, usando código de autenticação de mensagem (*Message Authentication Code - MAC*) de 128 bits. Este conjunto de chaves é gerado e distribuído pela AC , por meio das RSUs. Cada chave do conjunto tem uma validade pré-definida. Quando uma chave expira, a próxima chave do conjunto é usada por todos os veículos. No PPSCP, o conjunto de chaves tem tamanho 4 e o período de duração de uma chave é de uma semana. O algoritmo MAC utiliza chave secreta com tamanho de 128bits. Esse comprimento de chave faz com que um ataque de força bruta seja impraticável.

Quando um mau comportamento de um veículo é detectado, o mesmo deve ser revogado. O esquema de revogação proposto depende de chaves simétricas chamadas de chaves de revogação. Cada veículo possui chaves simétricas de revogação que são

 ©2014 SBC — Soc. Bras. de Computação

usadas para criptografar o *timestamp*. Quando um veículo precisa enviar uma mensagem de segurança, este adiciona o *timestamp* cifrado com esta chave. Quando um veículo recebe uma mensagem, este tenta decifrar o *timestamp* com todas as chaves da lista de revogação. A AC é responsável por manter e distribuir as listas de revogação. É possível reduzir o tamanho das listas de revogação, incluindo as chaves dos veículos revogados em vez de todos os pseudônimos ou todos os certificados. Quando a vida útil da chave de revogação expira, a mesma é removida da lista, e desta forma a lista se mantém pequena.

A mobilidade dos veículos entre diferentes cidades e países é uma situação frequente. Por isso, no PPSCP, os veículos são geridos por diferentes ACs com base em sua localização, sendo que estas ACs estão interconectadas. Quando um veículo N entra na região de uma nova AC, este se comunica com a AC usando sua chave pública PubN e o certificado. A nova AC verifica o certificado do veículo através da AC anterior e então gera e envia um novo conjunto de chaves para o veículo.

PACP [Huang et al. 2014]

De acordo com [Huang et al. 2014], muitos esquemas projetados para manter o anonimato em VANETs utilizam uma infraestrutura de chave pública baseada no protocolo RSA ou em criptosistemas de curvas elípticas (ECC). No entanto, segundo os autores, estes esquemas sofrem de uma desvantagem comum, as autoridades envolvidas no processo de geração pseudônimos conhecem os pseudônimos utilizados pelos veículos. Logo, estes esquemas não são verdadeiramente anônimos.

O PACP (*Pseudonymous Authentication With Conditional Privacy*) [Huang et al. 2014] permite que veículos em uma rede veicular usem pseudônimos ao invés de sua identidade real. Neste protocolo, os veículos interagem com as unidades de acostamento (RSUs) para gerar os pseudônimos para comunicação, sendo que estes são conhecidos apenas pelos veículos. O esquema provê ainda um mecanismo de revogação que permite que veículos com mau comportamento sejam identificados e revogados da rede se necessário. Logo, a privacidade condicional é garantida aos veículos até que estes sejam revogados (estes deixam de ser anônimos). PACP se baseia em uma estrutura matemática baseada em em um esquema ECC (*pairing*). O protocolo não necessita armazenar vários certificados pseudônimos emitidos por uma autoridade confiável ou fornecidos por uma RSU. Em vez disso, um veículo gera seus pseudônimos com a ajuda da RSU vizinha.

O modelo de rede assumido no sistema PACP define três tipos de entidades, a saber: veículos, a MVD (*Motor Vehicles Division*) e RSUs. A interação entre estas três entidades no protocolo PACP está representada na Figura 4.15. Um veículo fornece a MVD as informações de identidade requeridas como parte do processo de registro. Em seguida, a MVD emite um ticket para o veículo. O ticket identifica unicamente o veículo, no entanto, este não revela a verdadeira identidade do veículo. Ao mover-se sobre a estrada, o veículo se autentica na RSU mais próxima e obtém um *token* de pseudônimos. O veículo usa o *token* para gerar seus pseudônimos. No protocolo, a RSU só fornece a credencial (ou seja, a assinatura) e restrições (ou seja, um *timestamp*) para que o veículo possa gerar seus pseudônimos e não detém qualquer informação privada do veículo.

 ©2014 SBC — Soc. Bras. de Computação

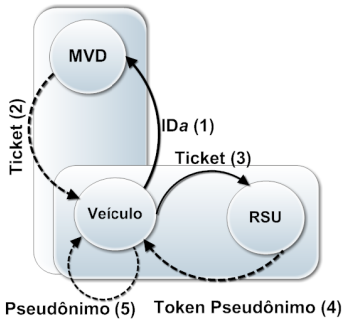

Figura 4.15. Diagrama de Interação das Entidades envolvidas no PACP [Huang et al. 2014]

4.4.4. Gerenciamento de Confiança e Sistemas de Reputação

Devido às suas características, as redes veiculares estão propensas à presença de nós maliciosos[4] [Raya et al. 2006a]. Os ataques ativos, provenientes desses nós, precisam ser evitados, já que estes podem enviar informações falsas na rede, bem como desviar pacotes, modificar seu conteúdo e até mesmo injetar novas mensagens na rede. Logo, torna-se necessário o desenvolvimento de soluções capazes de incentivar comportamentos cooperativos, mas que identifiquem a presença de nós maliciosos [Dai et al. 2013].

Segundo [Li et al. 2012], detectar nós maliciosos tornou-se um dos problemas mais difíceis no que diz respeito a segurança em VANETs. 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 segurança no trânsito (p.ex. disseminação de alertas). Para minimizar a ação de nós maliciosos, alguns métodos surgiram visando privilegiar os nós com comportamento correto na rede, dentre estes destacam-se os que utilizam **sistemas de reputação** [Li et al. 2013].

O conceito de reputação pode ser definido como uma medida coletiva de confiabilidade em um dispositivo baseado em indicações ou avaliações de membros de uma comunidade. Cada nó possui um valor de reputação que reflete o seu comportamento. De acordo com [Huang et al. 2014], um sistema de reputação tem por finalidade construir um valor de confiança para cada nó na rede. Essas opiniões são acertadas para formar a reputação que serve como referência para que outros nós possam identificar quais nós podem oferecer recursos confiáveis (confiança no nó). Assim, o nível individual de confiança em um dispositivo pode ser obtido a partir de uma combinação das indicações recebidas de outros dispositivos [Swamynathan et al. 2007].

Alguns sistemas de reputação para redes veiculares, ao invés de focar na confiabilidade dos nós, focam na confiabilidade dos dados [Ostermaier et al. 2007, Lo e Tsai 2009]. De acordo com [Karagiannis et al. 2011], para algumas aplicações veiculares, a confiabilidade dos dados é mais útil que a confiabilidade dos nós que estão se comunicando, para outras a confiabilidade dos nós deve ser provida. A seguir, serão analisados alguns trabalhos que descrevem sistemas de reputação específicos para VANETs (tratam da confiabilidade dos nós ou da confiabilidade dos dados).

[4]Nesta seção, utiliza-se o termo malicioso mesmo quando a ação maliciosa visa um ganho pessoal (chamado de racional).

 ©2014 SBC — Soc. Bras. de Computação

[Ostermaier et al. 2007]

Em [Ostermaier et al. 2007], os autores propuseram um sistema de reputação baseado em votação visando avaliar a credibilidade das mensagens (eventos) e aumentar a segurança das decisões tomadas pelos veículos sobre eventos reportados em aplicações LDW. O trabalho avaliou o resultado de quatro métodos de decisão da confiabilidade no perigo relatado com base no sistema de votação como segue:

- Últimas Mensagens: sempre que uma decisão precisa ser tomada, apenas a mensagem mais recente do alerta é considerada, cujo objetivo é atingir uma alta adaptabilidade em cenários livres de ataques, resultando em poucas decisões erradas.
- Maioria de vitórias: executa uma decisão local de voto sobre todas as mensagens recebidas sobre um determinado alerta. Caso a maioria das mensagens recebidas forem de alertas, uma decisão positiva é tomada; caso contrário, uma decisão negativa é considerada.
- Maioria das Últimas Mensagens: é uma combinação dos dois anteriores. Para uma tomada de decisão, um veículo irá realizar uma votação considerando apenas as últimas mensagens em relação ao alerta em questão.
- Maioria das Últimas x Mensagens com valor mínimo: é uma extensão do anterior, na qual o veículo utiliza apenas as últimas x mensagens recebidas com informações sobre o evento. Desta forma, é verificado um limite inferior, de forma que o mecanismo somente é utilizado caso o veículo receba ao menos um determinado número de mensagens. Quando esse mínimo de opiniões não é atingido, o veículo sempre se decide pela negação do evento.

O sistema de reputação proposto trata da credibilidade das mensagens. O custo computacional de processamento e a sobrecarga na rede decorrentes do uso deste mecanismo não foram avaliados pelos autores. As simulações realizadas comparam a eficácia dos quatro métodos de decisão com cenários livres de ataques [Fernandes et al. 2013].

DTT [Wang e Chigan 2007]

O mecanismo de confiança *Dynamic Trust-Token (DTT)* tem o objetivo de detectar a modificação de mensagens na rede por nós maliciosos e isolar estes nós de forma a prevenir que estes interfiram nas próximas mensagens. No mecanismo proposto pelos autores, são utilizadas técnicas de criptografia assimétrica e assinatura digital com o objetivo de garantir a integridade dos pacotes durante a comunicação. Quando um nó viola esta integridade, este é considerado malicioso.

No DTT, um emissor envia uma mensagem para seus vizinhos e caso este vizinho não seja o destinatário, este irá reencaminhar mensagem recebida. O emissor então monitora essas retransmissões e, caso o pacote não sofra nenhuma alteração, o emissor envia um *token* de confiança, assinado digitalmente, para o respectivo vizinho. Os vizinhos devem reencaminhar este *token*, que os certifica como confiáveis, para os veículos responsáveis pelo próximo salto. O processo de escuta e emissão do *token*, feito pelo emissor da mensagem, é agora realizado pelos vizinhos certificados. Esse ciclo se repete em todos os saltos

 ©2014 SBC — Soc. Bras. de Computação

até que a mensagem atinja seu destino. O mecanismo baseia-se apenas no comportamento dos veículos em tempo de execução, definindo desta maneira a reputação instantânea de um nós não mantendo portanto reputação histórica. Este mecanismo são trata do problema de nós que propagam mensagens falsas na rede.

RMDTV [de Paula et al. 2010]

No RMDTV (*Reputation Mechanism for Delay Tolerant Vehicular Networks*), os membros da rede qualificam as informações (corretas ou não) dos outros membros e emitem mensagens de qualificação que atestam a confiabilidade da mensagem (informação correta recebida). O emissor da mensagem armazena estas mensagens de qualificação e as usa quando forem propagar novas mensagens como se estas fossem suas credenciais que comprovam as mensagens corretas já propagadas na rede. Ou seja, o sistema faz uso de qualificações emitidas por terceiros (reputação global) para atestar a confiabilidade dos nós, porém estas qualificações são apresentadas pelos próprios nós emissores do alerta. Desta maneira, os membros da rede podem verificar previamente a confiabilidade de novos vizinhos, antes mesmo da troca de dados.

O mecanismo usa o conceito de redes tolerantes a atrasos e interrupções (*Delay and Disruption Tolerant Networks - DTNs*) para sanar os possíveis problemas de momento de desconexão total, visto que o nó armazena as mensagens recebidas até poder encaminhá-las a outros nós da rede. Cada veículo é responsável por armazenar localmente duas listas contendo os membros considerados confiáveis e os membros maliciosos. Desta forma, um emissor de um alerta pode ser classificado como: malicioso, confiável ou desconhecido. Os nós considerados confiáveis são aqueles aos quais suas mensagens informam o evento corretamente, ao contrário, quando estes eventos são incorretos o nó é punido e passa a ser considerado malicioso. Segundo os autores, o reconhecimento prévio e a exclusão de dados gerados por nós maliciosos é possível devido ao armazenamento de dados históricos sobre o comportamento dos veículos. Além disso, o compartilhamento de experiências permite estabelecer relações de confiança antes do início das transações.

As qualificações possuem pesos diferenciados no mecanismo de decisão e estas qualificações são adicionadas às mensagens de dados geradas pelo veículo. Entretanto, segundo os autores do mecanismo RMDTV, para evitar uma grande sobrecarga na rede, eles consideram que apenas um determinado número de qualificações deve ser adicionado e estas possuem prazo de validade. Desta forma, somente aquelas não expiradas devem ser utilizadas. Neste mecanismo, não existe um rebaixamento progressivo dos nós na rede. Desta forma, basta que o veículo apresente um comportamento malicioso uma única vez, para que este possa ser considerado 100% malicioso. Da mesma maneira, basta que envie uma mensagem de qualificação correta para ser considerado 100% confiável.

DMV [Daeinabi e Rahbar 2013]

O mecanismo DMV (*Detection of Malicious Vehicles*) [Daeinabi e Rahbar 2013] visa monitorar nós maliciosos que rejeitam ou duplicam pacotes recebidos de forma a isolá-los dos nós considerados honestos. Cada veículo é monitorado por vizinhos confiáveis chamados de nós verificadores. Um conjunto de veículos está localizado em um agrupamento e cada agrupamento possui um líder. Cada veículo possui duas listas: lista branca e lista negra. Os veículos que compõem a lista branca são aqueles cujos valores de desconfiança (Td)

 ©2014 SBC — Soc. Bras. de Computação

são inferiores a um *threshold* mínimo. Por outro lado, a lista negra contém os veículos na qual seu valor de desconfiança (Td) é mais elevados que o *threshold* mínimo. Cada veículo, ao entrar na rede pela primeira vez, tem seu valor de desconfiança igual a um (valor igual para todos os veículos) e está presente na lista branca.

Caso um nó verificador identifique um comportamento anormal de um veículo, este reporta para o líder do agrupamento para que o líder atualize o valor de desconfiança do veículo (ver Figura 4.16). Um nó é considerado malicioso quando o seu valor de desconfiança é superior a um *threshold* mínimo. Quando isto ocorre, este veículo deve ser retirado da lista branca e ser acrescentado na lista negra. Para isto, o líder verifica se valor de Td é menor ou igual que o *threshold* mínimo. Se for, atualiza a lista branca; se não for, notifica a Autoridade Certificadora para que esta atualize a lista negra. A AC transmite periodicamente estas listas para os líderes de agrupamento da rede.

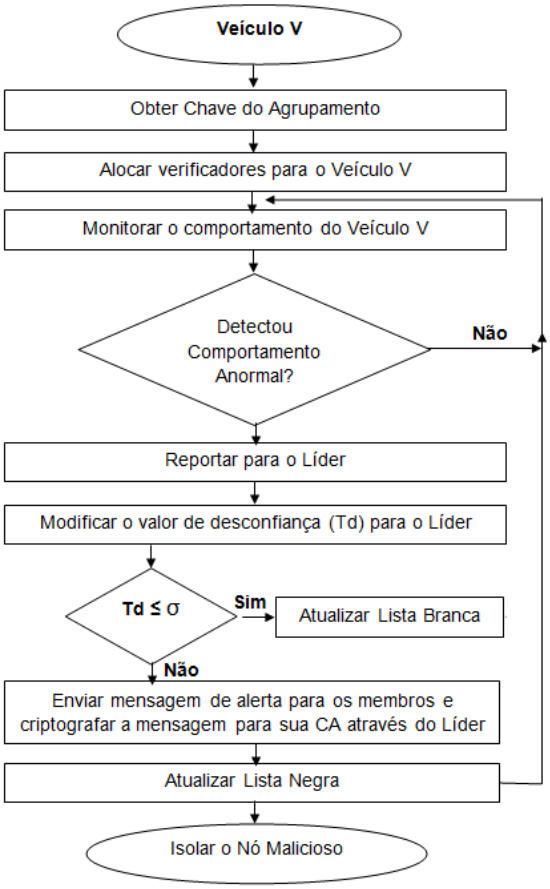

Figura 4.16. Processo de Monitoramento de Veículos no DMV [Huang et al. 2014]

Cada Autoridade Certificadora (AC) é uma terceira parte confiável que gerencia as identidades, as chaves criptográficas e as credenciais dos veículos dentro de sua região. Esta transmite sua lista negra periodicamente a todos os líderes de agrupamentos e, em seguida, estes as transmitem para todos os veículos localizados dentro do agrupamento. Os veículos pertencentes à lista negra são isolados da rede. Desta forma, outros veículos não aceitam mensagens vindas destes veículos. O líder de agrupamento é escolhido entre aqueles que têm o menor valor de desconfiança (Td), sendo este substituído quando apresentar

 ©2014 SBC — Soc. Bras. de Computação

comportamentos anormais, ou quando outro veículo possuir o valor de desconfiança (Td) menor após atualização.

[Li et al. 2012]

Em [Li et al. 2012], foi proposto um sistema de reputação para redes veiculares que permite avaliar a confiabilidade da mensagem recebida de acordo com a reputação do veículo gerador da mensagem. O sistema proposto faz uso de um servidor de reputação centralizado. Uma das finalidades deste servidor é armazenar a reputação dos veículos, isto inclui a coleta de relato de experiências para produzir a reputação, e a propagação desta reputação na rede. O modelo de rede do mecanismo assume ainda a existência de dispositivos de comunicação entre os veículos e o servidor de reputação (chamados de pontos de acesso). Segundo os autores, não é necessária a comunicação contínua entre os veículos e o servidor de reputação. Estes servidores ficam posicionados em locais frequentemente visitados pelos veículos, como postos de combustíveis e semáforos. Quando um veículo recebe uma mensagem, caso este ainda não tenha tido uma experiência anterior com o emissor, ele consulta o servidor de reputação para obter a reputação global calculada através da média ponderada das experiências anteriores dos demais nós da rede. Além dos problemas de falha e desempenho decorrentes da abordagem com servidor centralizado, os autores não tratam a situação quando um nó é desconhecido também para o servidor de reputação.

[Fernandes et al. 2013]

Em [Fernandes et al. 2013], foi proposto um sistema de reputação descentralizado para avaliar o nível de confiança dos nós. Com este sistema, é possível identificar a presença de nós maliciosos em uma aplicação LDW (*Local Danger Warning*) e descartar seus alertas, uma vez que o comportamento inadequado destes nós pode comprometer a segurança das redes veiculares. No modelo assumido de redes, as unidades de bordo dos veículos e as RSUs não dependem de um ponto central avaliador da confiança dos nós e armazenador da base de reputação dos nós participantes, sendo o sistema caracterizado como descentralizado. Com as informações sobre o comportamento dos veículos, armazenadas de forma distribuída, a disponibilidade deste conteúdo é garantida. O objetivo da solução descrita é identificar a presença de nós maliciosos em uma aplicação LDW, chamada de RAMS+, de forma a descartar seus alertas, mesmo diante da formação de conluios.

No sistema proposto, a reputação do nó é avaliada consultando outros nós participantes da rede, fazendo uso de uma estratégia otimista na qual os nós têm reputação boa até que se prove o contrário. Cada veículo possui uma base de conhecimento individual (BCI), que contém informações sobre as interações passadas que este teve com outros veículos. A BCI armazena as experiências passadas mais recentes e o veículo a utiliza para o cálculo da reputação direta. Para encontrar a reputação global do veículo emissor do alerta, o veículo que recebeu o alerta calcula ainda a reputação agregada (indireta), definida a partir de informações de terceiros (mensagens recebidas de seus vizinhos). A reputação agregada é muito importante para o cálculo da reputação de veículos desconhecidos. Outra informação que auxilia a tomada de decisão de um veículo que recebeu uma mensagem de alerta é uma Lista de Reputações (*LR*) propagada pelas RSUs. Esta lista se torna mais importante com a proximidade do veículo no local do evento, pois este pode não ter tempo suficiente para

 ©2014 SBC — Soc. Bras. de Computação

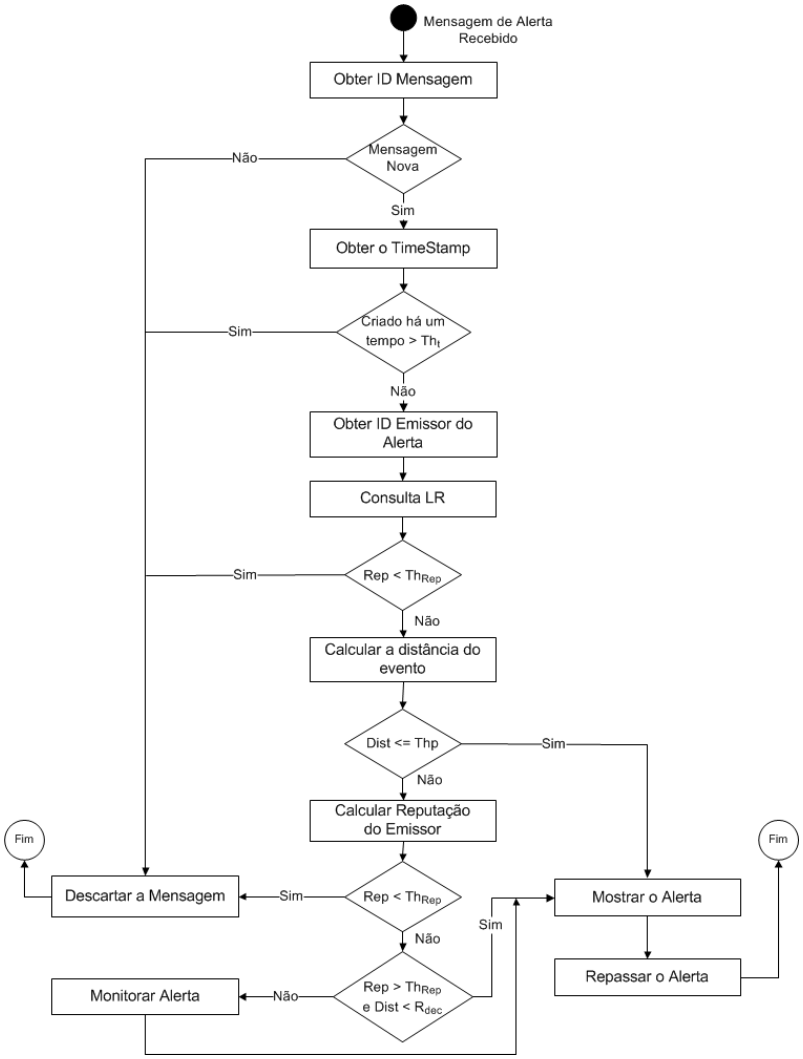

Figura 4.17. Passos do Sistema de Reputação [Fernandes et al. 2013]

calcular a reputação global, mantendo uma base de reputação mais abrangente e atualizada.

A Figura 4.17 ilustra os passos executados por um veículo ao receber uma mensagem de alerta (*MenAlert*). Após verificar que a mensagem *MenAlert* é uma mensagem nova e que esta foi criada a um tempo menor que o limiar de mensagem recente, o veículo, por meio do sistema de reputação, deve obter a reputação do emissor, consultando a Lista de Reputações (*LR*) recebida e avaliar se esta está acima de um limiar de reputação que considera este veículo confiável (e.g. 0,5). Caso este veículo seja considerado não confiável, a mensagem é descartada. Caso o veículo não esteja na lista de reputação ou caso este tenha sido considerado como confiável, a aplicação irá calcular a distância que o veículo está do evento relatado. Caso este veículo esteja muito próximo do local do evento (e.g. 100 metros), o alerta é mostrado para o condutor, pois pode não haver tempo hábil para a realização da consulta aos outros veículos. Caso contrário, a aplicação irá calcular a reputação global do emissor do alerta. Se o resultado da reputação for maior que o limiar de reputação, o emissor é avaliado como confiável. Caso este esteja na área de decisão, o alerta é mostrado para o condutor e repassado para os demais veículos. Quando o emissor

 ©2014 SBC — Soc. Bras. de Computação

for avaliado como confiável e a distância do veículo estiver fora da área de decisão, um novo processo é criado para monitorar a entrada do veículo na área de decisão, mostrando posteriormente o alerta ao condutor quando este entrar nesta área.

4.5. Considerações finais: tendências e problemas em aberto

De acordo com [Raya e Hubaux 2007, Karagiannis et al. 2011], as soluções de segurança existentes para redes sem fio e até mesmo para redes *adhoc* não são facilmente aplicadas nas VANETs, dada a natureza destas redes que impõem novos desafios, a saber: restrições de tempo, escala da rede, alta mobilidade dos nós, volatilidade [Engoulou et al. 2014]. Um bom exemplo são os mecanismos de autenticação que usam assinaturas digitais que nas VANETs precisam ser adaptados para diminuir a sobrecarga de computação e de comunicação, garantir a privacidade condicional dos condutores e fazer uso de uma infraestrutura de chaves públicas flexível aos requisitos das VANETs [Isaac et al. 2010].

Para construir uma arquitetura de segurança e soluções que suportem a robustez das VANETs, é necessário o avanço no estudo das características e dos impactos dos ataques que podem ocorrer nestas redes. A gestão e a análise de riscos em redes veiculares são usadas para identificar e gerenciar as ameaças e os ataques potenciais na comunicação veicular. Soluções para o gerenciamento e a análise de tais ataques têm sido propostas [Aijaz et al. 2006, Ren et al. 2011, Ganan et al. 2012], porém é necessário avançar na caracterização do comportamento dos atacantes a fim de construir modelos que identifiquem os limites fundamentais do impacto dos ataque na rede e nas comunicações de forma menos abstrata e que considere as características realistas da rede e da comunicação [Karagiannis et al. 2011, Engoulou et al. 2014].

Garantir a confiabilidade das mensagens trafegadas na rede é relevante a fim de suportar as aplicações de monitoramento, impedindo que os condutores assumam ou tomem ações a partir de informações falsas [Karagiannis et al. 2011]. Um receptor deve não só verificar a integridade da informação recebida (p.ex. verificar a assinatura da mensagem) mas também confirmar a confiabilidade do emissor (confiança centrada na entidade). Os sistemas de reputação podem ser utilizados para estabelecer a confiança tanto dos veículos (confiança centrada na entidade) quanto das mensagens (confiança centrada no dado) [Tangade e Manvi 2013], porém a natureza distribuída e abrangente das redes veiculares tornam estes sistemas complexos. Uma solução adaptativa e ciente de contexto pode ser uma alternativa para tratar esta complexidade, porém, testes em diferentes cenários precisam ser realizados para verificar a efetividade dos sistemas de reputação adaptativos.

A privacidade é um dos maiores desafios na implementação e uso das aplicações de redes veiculares [Engoulou et al. 2014]. Informações como identidade e comportamento do condutor, localização presente e passada do veículo, em muitos casos, devem ser privadas. Conforme analisado na Seção 4.4.3, prover a privacidade condicional é essencial para garantir a revogação da privacidade dos nós com comportamentos maliciosos. De acordo com [Karagiannis et al. 2011], a privacidade é um conceito específico do usuário e um bom mecanismo deve permitir que um usuário selecione a privacidade que este deseja ter (privacidade adaptativa). Usuários podem querer usar diferentes níveis de privacidade dependendo no nível de confiança com quem estão se comunicando. Um requisito de alto

 ©2014 SBC — Soc. Bras. de Computação

nível de privacidade geralmente resulta em um aumento na sobrecarga computacional e de comunicação, o que não pode ocorrer em VANETs. 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 VANETs.

Muitas soluções que visam prover comunicação anônima em VANETs adotam o modelo de confiança zero (veículos não confiam nos outros veículos), são baseados em criptografia assimétrica e fazem uso de uma infraestrutura de chaves públicas (ICP). Um conjunto de pesquisadores consideram como consenso o uso de criptografia de curvas elípticas (ECC) para manter o anonimato em VANETs (exemplos foram apresentados na seção 4.4). Diante das características e restrições das VANETs, a sobrecarga computacional e de comunicação, a complexidade para gestão da confiança em uma ICP podem dificultar o uso efetivo destas soluções.

Uma das questões em discussão no momento é como garantir que os veículos terão conexão com a ICP no momento da renovação do certificado, principalmente, quando pseudônimos estiverem sendo utilizados. Será que uma conexão via telefonia celular (4G, 3G, etc) poderia ser assumida? Ou será que comunicações esporádicas com outros veículos ou RSUs seriam suficientes para suportar a realização desta operação? Como tornar essa comunicação o mais leve e rápida a fim de permitir a renovação do certificado com uma baixa sobrecarga na comunicação?

Segurança em VANETs é um tema de pesquisa bastante atual e ativo conforme pode ser observado pelas inúmeras publicações nas principais conferências nacionais e internacionais e nos tópicos de interesse dos periódicos internacionais. Diversas soluções estão sendo providas para os inúmeros ataques que estas redes estão sujeitas. Com o objetivo de avaliar a aplicabilidade, eficiência e eficácia das soluções propostas, pesquisadores realizam diversos experimentos por meio de simulações. Nestes experimentos, simuladores de rede e de tráfego são comumente utilizados a fim de fornecer resultados mais próximos aos ambientes veiculares reais. Porém, apesar das vantagens do uso de simuladores, tais como custo mais baixo e ambiente controlado, esta abordagem apresenta limitações. As simulações podem não refletir totalmente um ambiente real e podem até levar a resultados errados devido a simplificação dos modelos de rede e de tráfego e suposições em relação a propagação e interferências [Qin et al. 2014]. Testes em cenários reais, com veículos (OBUs) e unidades de acostamento reais, são muitas vezes considerados uma avaliação adicional e necessária aos trabalhos de simulação.

Apesar dos diversos trabalhos na literatura que descrevem aplicações de VANETs, ainda é necessário superar uma série de desafios científicos e tecnológicos de segurança para que estas aplicações sejam utilizadas e difundidas em sua forma plena. A implementação e avaliação dos mecanismos e soluções apresentados neste capítulo em cenário reais, já que grande parte dos trabalhos carecem de implementação ou provas formais, é uma oportunidade de pesquisa.

Referências

[Ahlgren et al. 2012] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., e Ohlman, B. (2012). A survey of information-centric networking. *IEEE Communications Magazine*, 50(7):26–36.

[Aijaz et al. 2006] Aijaz, A., Bochow, B., Dötzer, F., Festag, A., Gerlach, M., Kroh, R., e Leinmüller, T.

 ©2014 SBC — Soc. Bras. de Computação

(2006). Attacks on Inter Vehicle Communication Systems - an Analysis. In *WIT*, pages 189–194.

[Al Falasi e Barka 2011] Al Falasi, H. e Barka, E. (2011). Revocation in VANETs: A survey. In *International Conference on Innovations in Information Technology (IIT)*, pages 214–219.

[Al-kahtani 2012] Al-kahtani, M. (2012). Survey on security attacks in vehicular ad hoc networks (VANETs). In *International Conference on Signal Processing and Communication Systems (ICSPCS)*, pages 1–9.

[Al-Sultan et al. 2014] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., e Zedan, H. (2014). A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications*, 37:380–392.

[Alves 2011] Alves, V. d. M. (2011). Protocolo de comprometimento de bit eficiente com segurança sequencial baseado no modelo de memória limitada.

[Amro et al. 2013] Amro, B., Saygin, Y., e Levi, A. (2013). Enhancing privacy in collaborative traffic-monitoring systems using autonomous location update. *Intelligent Transport Systems, IET*, 7(4):388–395.

[Aslam e Zou 2009] Aslam, B. e Zou, C. (2009). Distributed certificate and application architecture for VANETs. In *IEEE Military Communications Conference (MILCOM)*, pages 1–7.

[Avelar et al. 2014] Avelar, E., Marques, L., dos Passos, D., Macedo, R., Dias, K., e Nogueira, M. (2014). Interoperability issues on heterogeneous wireless communication for smart cities. *Computer Communications*.

[Biswas et al. 2011] Biswas, S., Misic, J., e Misic, V. (2011). ID-based safety message authentication for security and trust in vehicular networks. In *31st International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pages 323–331.

[Boneh et al. 2004] Boneh, D., Boyen, X., e Shacham, H. (2004). Short group signatures. In Franklin, M., editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55. Springer Berlin Heidelberg.

[Bononi et al. 2004] Bononi, L., Conti, M., e Gregori, E. (2004). Runtime optimization of IEEE 802.11 wireless LANs performance. *IEEE Transactions on Parallel and Distributed Systems*, 15(1):66–80.

[Chen et al. 2011] Chen, L., Ng, S.-L., e Wang, G. (2011). Threshold anonymous announcement in VANETs. *IEEE Journal on Selected Areas in Communications*, 29(3):605–615.

[Chuang e Lee 2011] Chuang, M.-C. e Lee, J.-F. (2011). TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks. In *International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pages 1758–1761.

[Daeinabi e Rahbar 2013] Daeinabi, A. e Rahbar, A. G. (2013). Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks. *Multimedia tools and applications*, 66(2):325–338.

[Dai et al. 2013] Dai, W., Moser, L., Melliar-Smith, P., Lombera, I. M., e team:, Y. (2013). The itrust local reputation system for mobile ad-hoc networks. In *International Conference on Wireless Networks*.

[de Paula et al. 2010] de Paula, W., de Oliveira, S., e Oliveira, J. M. (2010). Um mecanismo de reputação para redes veiculares tolerantes a atrasos e desconexões. In *Simpósio Brasileiro de Redes de Computadores (SBRC 2010)*, page 599.

[Engoulou et al. 2014] Engoulou, R. G., Bellaïche, M., Pierre, S., e Quintero, A. (2014). VANET security surveys. *Computer Communications*, 44(0):1 – 13.

[Faezipour et al. 2012] Faezipour, M., Nourani, M., Saeed, A., e Addepalli, S. (2012). Progress and challenges in intelligent vehicle area networks. *Communications of the ACM*, 55(2):90–100.

[Fernandes et al. 2013] Fernandes, C., de Simas, I., e Wangham, M. S. (2013). In *Simpósio Brasileiro de Segurança em Segurança da Informação e de Sistemas Computacioanais (SBSeg 2013)*, pages 157–169.

[Ganan et al. 2012] Ganan, C., Munoz, J., Esparza, O., Mata-Diaz, J., Alins, J., Silva-Cardenas, C., e Bartra-Gardini, G. (2012). RAR: Risk Aware Revocation Mechanism for Vehicular Networks. In *IEEE Vehicular Technology Conference (VTC Spring)*, pages 1–5.

 ©2014 SBC — Soc. Bras. de Computação

[Gerla 2012] Gerla, M. (2012). Vehicular cloud computing. In *The 11th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, pages 152–155.

[Gerla e Kleinrock 2011] Gerla, M. e Kleinrock, L. (2011). Vehicular networks and the future of the mobile internet. *Computer Network*, 55(2):457–469.

[Grassi et al. 2014] Grassi, G., Pesavento, D., Pau, G., Vuyyuru, R., Wakikawa, R., e Zhang, L. (2014). VANET via named data networking. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 410–415.

[Haas et al. 2011] Haas, J. J., Hu, Y.-C., e Laberteaux, K. P. (2011). Efficient certificate revocation list organization and distribution. *IEEE Journal on Selected Areas in Communications*, 29(3):595–604.

[Hartenstein e Laberteaux 2010] Hartenstein, H. e Laberteaux, K. (2010). *VANET: vehicular applications and inter-networking technologies*. Wiley Online Library.

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

[He et al. 2014] He, W., Yan, G., e Xu, L. D. (2014). Developing vehicular data cloud services in the IoT environment. *IEEE Transactions on Industrial Informatics*, 10(2):1587–1595.

[Hill e Garrett 2011] Hill, C. J. e Garrett, J. K. (2011). AASHTO connected vehicle infrastructure deployment analysis. Technical report.

[Hossain et al. 2010] Hossain, E., Chow, G., Leung, V., McLeod, R. D., Mišić, J., Wong, V. W., e Yang, O. (2010). Vehicular telematics over heterogeneous wireless networks: A survey. *Computer Communications*, 33(7):775–793.

[Huang et al. 2014] Huang, Z., Ruj, S., Cavenaghi, M. A., Stojmenovic, M., e Nayak, A. (2014). A social network approach to trust management in VANETs. *Peer-to-Peer Networking and Applications*, 7(3):229–242.

[Hussain et al. 2012] Hussain, R., Son, J., Eun, H., Kim, S., e Oh, H. (2012). Rethinking vehicular communications: Merging vanet with cloud computing. *International Conference on Cloud Computing Technology and Science*, 0:606–609.

[IEEE 2013] 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)*, pages 1–289.

[Isaac et al. 2010] Isaac, J., Zeadally, S., e Camara, J. (2010). Security attacks and solutions for vehicular ad hoc networks. *IET Communications*, 4(7):894–903.

[Juels e Wattenberg 1999] Juels, A. e Wattenberg, M. (1999). A fuzzy commitment scheme. In *ACM conference on Computer and communications security*, pages 28–36. ACM.

[Karagiannis et al. 2011] Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., e Weil, T. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Communications Surveys and Tutorials*, 13(4):584–616.

[Kherani e Rao 2010] Kherani, A. e Rao, A. (2010). Performance of node-eviction schemes in vehicular networks. *IEEE Transactions on Vehicular Technology*, 59(2):550–558.

[Kwak et al. 2006] Kwak, D., Moon, S., Wang, G., e Deng, R. H. (2006). A secure extension of the Kwak–Moon group signcryption scheme. *Computers & Security*, 25(6):435 – 444.

[Laberteaux et al. 2008] Laberteaux, K. P., Haas, J. J., e Hu, Y.-C. (2008). Security certificate revocation list distribution for VANET. In *ACM international workshop on VehiculAr Inter-NETworking*, pages 88–89. ACM.

[Laurendeau e Barbeau 2006] Laurendeau, C. e Barbeau, M. (2006). Threats to security in DSRC/WAVE. In *Ad-Hoc, Mobile, and Wireless Networks*, pages 266–279. Springer.

[Lee et al. 2014] Lee, E., Lee, E.-K., Gerla, M., e Oh, S. (2014). Vehicular cloud networking: architecture and design principles. *IEEE Communications Magazine*, 52(2):148–155.

 ©2014 SBC — Soc. Bras. de Computação

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

[Li et al. 2012] Li, Q., Malip, A., Martin, K. M., Ng, S.-L., e Zhang, J. (2012). A reputation-based announcement scheme for VANETs. *IEEE Transactions on Vehicular Technology*, 61(9):4095–4108.

[Li et al. 2013] Li, X., Liu, J., Li, X., e Sun, W. (2013). Rgte: A reputation-based global trust establishment in VANETs. In *5th International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, pages 210–214.

[Lima et al. 2013] Lima, A., Albano, W., Nogueira, M., e de Sousa, J. N. (2013). Influência de ataques jamming sobre protocolos de roteamento em redes veiculares. In *Workshop de Trabalhos de Iniciação Científica e de Graduação (WTICG) - SBSeg*.

[Lin et al. 2008] Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P.-H., e Shen, X. (2008). Security in vehicular ad hoc networks. *IEEE Communications Magazine*, 46(4):88–95.

[Lin et al. 2007] Lin, X., Sun, X., Ho, P.-H., e Shen, X. (2007). Gsis: A secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, 56(6):3442–3456.

[Lo e Tsai 2009] Lo, N.-W. e Tsai, H.-C. (2009). A reputation system for traffic safety event on vehicular ad hoc networks. *EURASIP Journal on Wireless Communications and Networking*, 2009:9.

[Lu et al. 2008] Lu, R., Lin, X., Zhu, H., Ho, P.-H., e Shen, X. (2008). Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications. In *IEEE Conference on Computer Communications (INFOCOM)*.

[Macedo et al. 2013] Macedo, R., Melo, R. G. d., Melnisk, L., Santos, A., e Nogueira, M. (2013). Uma avaliação experimental de desempenho do roteamento multicaminhos em redes veiculares. In *Workshop de Gerência e Operações de Redes - SBRC*.

[Mangold et al. 2002] Mangold, S., Choi, S., May, P., Klein, O., Hiertz, G., e Stibor, L. (2002). Ieee 802.11 e wireless lan for quality of service. In *European Wireless*, volume 2, pages 32–39.

[Mejri et al. 2014] Mejri, M. N., Ben-Othman, J., e Hamdi, M. (2014). Survey on {VANET} security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53 – 66.

[Mezghani et al. 2014a] Mezghani, F., Dhaou, R., Nogueira, M., e Beylot, A.-L. (2014a). Content dissemination in vehicular social networks: Taxonomy and user satisfaction. *IEEE Communications Magazine*.

[Mezghani et al. 2014b] Mezghani, F., Dhaou, R., Nogueira, M., e Beylot, A.-L. (2014b). Utility-based forwarder selection for content dissemination in vehicular networks. In *IEEE International Conference on Personal, Indoor and Mobile Radio Communications (PIMRC)*.

[Mikki et al. 2013] Mikki, M., Mansour, Y., e Yim, K. (2013). Privacy preserving secure communication protocol for vehicular ad hoc networks. In *Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, pages 188–195.

[Mohr 2007] Mohr, A. (2007). A survey of zero-knowledge proofs with applications to cryptography. *Southern Illinois University, Carbondale*, pages 1–12.

[Nogueira et al. 2009] Nogueira, M., dos Santos, A., e Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks. *IEEE Communications Surveys and Tutorials*, 11(1):66–77.

[Nowatkowski 2010] Nowatkowski, M. E. (2010). *Certificate Revocation List Distribution in Vehicular Ad Hoc Networks*. PhD thesis, Atlanta, GA, USA. AAI3414506.

[Ostermaier et al. 2007] Ostermaier, B., Dotzer, F., e Strassberger, M. (2007). Enhancing the security of local dangerwarnings in VANETs-a simulative analysis of voting schemes. In *International Conference on Availability, Reliability and Security (ARES)*, pages 422–431.

[Papadimitratos et al. 2008] Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., e Hubaux, J.-P. (2008). Secure vehicular communication systems: design and architecture. *IEEE Communications Magazine*, 46(11):100–109.

 ©2014 SBC — Soc. Bras. de Computação

[Papadimitratos et al. 2009] Papadimitratos, P., La Fortelle, A., Evenssen, K., Brignolo, R., e Cosenza, S. (2009). Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. *IEEE Communications Magazine*, 47(11):84–95.

[Paruchuri e Durresi 2010] Paruchuri, V. e Durresi, A. (2010). Paave: Protocol for anonymous authentication in vehicular networks using smart cards. In *IEEE Global Telecommunications Conference (GLOBECOM 2010)*, pages 1–5.

[Pathre et al. 2013] Pathre, A., Agrawal, C., e Jain, A. (2013). Identification of malicious vehicle in vanet environment from ddos attack. *Journal of Global Research in Computer Science*, 4(6):1–5.

[Pinto 2013] Pinto, A. C. B. (2013). Protocolos criptográficos de computação distribuída com segurança universalmente composta.

[Qin et al. 2014] Qin, Z., Meng, Z., Zhang, X., Xiang, B., e Zhang, L. (2014). Performance evaluation of 802.11p wave system on embedded board. In *International Conference on Information Networking (ICOIN)*, pages 356–360.

[Rawat et al. 2012] Rawat, A., Sharma, S., e Sushil, R. (2012). Vanet:security attacks and its possible solutions. *Journal of Information and Operations Management*, 3:301–304.

[Raya e Hubaux 2007] Raya, M. e Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. *Journal Computer Security*, 15(1):39–68.

[Raya et al. 2006a] Raya, M., Papadimitratos, P., e Hubaux, J.-P. (2006a). Securing vehicular communications. *IEEE Wireless Communications*, 13(5):8–15.

[Raya et al. 2006b] Raya, M., Papadimitratos, P., e Hubaux, J.-P. (2006b). Securing vehicular communications. *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, 13(LCA-ARTICLE-2006-015):8–15.

[Ren et al. 2011] Ren, D., Du, S., e Zhu, H. (2011). A novel attack tree based risk assessment approach for location privacy preservation in the VANETs. In *IEEE International Conference on Communications (ICC)*, pages 1–5.

[Ribeiro et al. 2004] Ribeiro, V., Campello, R., e Weber, R. F. (2004). Mecanismos de conhecimento zero empregados por esquemas de chave publica. In Solar, M., Fernandez-Baca, D., e Cuadros-Vargas, E., editors, *30ma Conferencia Latinoamericana de Informatica (CLEI2004)*, pages 644–650. Sociedad Peruana de Computacion. ISBN 9972-9876-2-0.

[Safi et al. 2009] Safi, S., Movaghar, A., e Mohammadizadeh, M. (2009). A novel approach for avoiding wormhole attacks in vanet. In *Second International Workshop on Computer Science and Engineering*, volume 2, pages 160–165.

[Samara et al. 2010] Samara, G., Al-Salihy, W., e Sures, R. (2010). Security issues and challenges of vehicular ad hoc networks (VANET). In *International Conference on New Trends in Information Science and Service Science (NISS)*, pages 393–398.

[Schleiffer et al. 2013] Schleiffer, C., Wolf, M., Weimerskirch, A., e Wolleschensky, L. (2013). Secure key management-a key feature for modern vehicle electronics. Technical report, SAE Technical Paper.

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

[Shen et al. 2012] Shen, A.-N., Guo, S., Zeng, D., e Guizani, M. (2012). A lightweight privacy-preserving protocol using chameleon hashing for secure vehicular communications. In *IEEE on Wireless Communications and Networking Conference (WCNC)*, pages 2543–2548.

[Sichitiu e Kihl 2008a] Sichitiu, M. e Kihl, M. (2008a). Inter-vehicle communication systems: a survey. *IEEE Communications Surveys and Tutorials*, 10(2):88–105.

[Sichitiu e Kihl 2008b] Sichitiu, M. L. e Kihl, M. (2008b). Inter-vehicle communication systems: a survey. *IEEE Communications Surveys and Tutorials*, 10(2):88–105.

 ©2014 SBC — Soc. Bras. de Computação

[Silva et al. 2014a] Silva, C., Cerqueira, E., e Nogueira, M. (2014a). Connectivity management to support reliable communication on cognitive vehicular networks (to appear). In *Wireless Days*.

[Silva et al. 2014b] Silva, C., Cerqueira, E., e Nogueira, M. (2014b). Mecanismo distribuído para seleção de canais em redes veiculares cognitivas. In *Workshop de Redes de Acesso em Banda Larga - SBRC*.

[Silva et al. 2008] Silva, E., Dos Santos, A., Albini, L., e Lima, M. (2008). Identity-based key management in mobile ad hoc networks: techniques and applications. *Wireless Communications, IEEE*, 15(5):46–52.

[Sukuvaara et al. 2013] Sukuvaara, T., Ylitalo, R., e Katz, M. (2013). Ieee 802.11p based vehicular networking operational pilot field measurement. *IEEE Journal on Selected Areas in Communications*, 31(9):409–417.

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

[Tangade e Manvi 2013] Tangade, S. e Manvi, S. (2013). A survey on attacks, security and trust management solutions in VANETs. In *International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pages 1–6.

[Toor et al. 2008] Toor, Y., Muhlethaler, P., e Laouiti, A. (2008). Vehicle ad hoc networks: Applications and related technical issues. *IEEE Communications Surveys and Tutorials*, 10(3):74–88.

[Uzcategui e Acosta-Marum 2009] Uzcategui, R. e Acosta-Marum, G. (2009). Wave: a tutorial. *IEEE Communications Magazine*, 47(5):126–133.

[Wang et al. 2012] Wang, L., Wakikawa, R., Kuntz, R., Vuyyuru, R., e Zhang, L. (2012). Data naming in vehicle-to-vehicle communications. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 328–333.

[Wang e Chigan 2007] Wang, Z. e Chigan, C. (2007). Countermeasure uncooperative behaviors with dynamic trust-token in VANETs. In *IEEE International Conference on Communications (ICC)*, pages 3959–3964. IEEE.

[Wasef et al. 2010] Wasef, A., Lu, R., Lin, X., e Shen, X. (2010). Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]. *IEEE Wireless Communications*, 17(5):22–28.

[Wasef e Shen 2009] Wasef, A. e Shen, X. (2009). Edr: Efficient decentralized revocation protocol for vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 58(9):5214–5224.

[Weerasinghe et al. 2010] Weerasinghe, H., Fu, H., e Leng, S. (2010). Anonymous service access for vehicular ad hoc networks. In *Sixth International Conference on Information Assurance and Security (IAS)*, pages 173–178.

[Wolf e Gendrullis 2012] Wolf, M. e Gendrullis, T. (2012). Design, implementation, and evaluation of a vehicular hardware security module. In *Information Security and Cryptology (ICISC)*, pages 302–318. Springer.

[Xiong et al. 2013] Xiong, H., Zhu, G., Chen, Z., e Li, F. (2013). Efficient communication scheme with confidentiality and privacy for vehicular networks. *Computers and Electrical Engineering*, 39(6):1717 – 1725.

[Xu et al. 2006] Xu, W., Ma, K., Trappe, W., e Zhang, Y. (2006). Jamming sensor networks: attack and defense strategies. *IEEE Network*, 20(3):41–47.

[Zhang 2011] Zhang, J. (2011). A survey on trust management for VANETs. In *IEEE International Conference on Advanced Information Networking and Applications (AINA)*, pages 105–112.

 ©2014 SBC — Soc. Bras. de Computação