Um Protocolo de Autenticação e Detecção de Ataques Sybil em Redes Ad Hoc Veiculares com Suporte ao Controle de Anonimato

Thiago Bruno Melo de Sales

Tese de Doutorado submetida à Coordenação do Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande - Campus de Campina Grande - como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências no Domínio da Engenharia Elétrica.

Área de Concentração: Processamento da Informação

Angelo Perkusich
Hyggo Oliveira de Almeida
Orientadores

Campina Grande, Paraíba, Brasil

Um Protocolo de Autenticação e Detecção de Ataques Sybil em Redes Ad Hoc Veiculares com Suporte ao Controle de Anonimato

Thiago Bruno Melo de Sales

Tese de Doutorado apresentada em Abril de 2015

Angelo Perkusich
Hyggo Oliveira de Almeida
Orientadores

Waslon Terllizzie Araújo Lopes, D.Sc., UFCG
Presidente da Banca
José Neuman de Souza, Dr., UFC
Examinador
Antonio Alfredo Ferreira Loureiro, Ph.D., UFMG
Examinador
Jaidilson Jó da Silva, D.Sc., UFCG
Examinador

Campina Grande, Paraíba, Brasil, Abril de 2015

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCG

S163p Sales, Thiago Bruno Melo de.

Um protocolo de autenticação e detecção de ataques sybil em Redes Ad Hoc veiculares com suporte ao controle de anonimato / Thiago Bruno Melo de Sales. – Campina Grande, 2015.

123 f. : il. color.

Tese (Doutorado em Engenharia Elétrica) - Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, 2015.

"Orientação: Prof. Dr. Angelo Perkusich, Prof. Dr. Hyggo Oliveira de Almeida".

Referências.

1. Redes Ad Hoc. 2. Veiculares. 3. Ataques Sybil. 4. Autenticação. 5. Anonimato. I. Perkusich, Angelo. II. Almeida, Hyggo Oliveira de. III. Título.

CDU 621.398(043)

"UM PROTOCOLO DE AUTENTICAÇÃO E DETECÇÃO DE ATAQUES SYBIL EM REDES AD HOC VEICULARES COM SUPORTE AO CONTROLE DE PRIVACIDADE"

THIAGO BRUNO MELO DE SALES

TESE APROVADA EM 17/04/2015

ANGELO PERKUSICH, D.Sc., UFCG
Orientador(a)

HYGGO OLIVEIRA DE ALMEIDA, D.Sc., UFCG
Orientador(a)

ANTONIO ALFREDO FERREIRA LOUREIRO, Ph.D., UFMG
Examinador(a)

JAIDILSON JÚDA SILVA, D.Sc., UFCG
Examinador(a)

JOSÉ NEUMAN DE SOUZA, Dr., UFC
Examinador(a)

WASLON TERLLIZZIE ARAÚJO LOPES, D.Sc., UFCG
Examinador(a)

CAMPINA GRANDE - PB

À minha esposa Lívia.
Aos meus pais Marcelo e Socorro.
Aos meus irmãos Junior e Leo.

Agradecimentos

A Deus, pelo dom da vida, e a minha mãe espiritual Chiara Lubich, por me ter apresentado Jesus Abandonado, fonte de recomeço e forças pra superar esse desafio.

À minha esposa Lívia Tereza (a minha pekena), pelo amor, pelas palavras de apoio, incentivo, e paciência em compreender minhas ausências durante essa fase.

Aos meus pais, Marcelo e Socorro, pelo apoio e suporte incondicionais, e aos meus irmãos Junior e Leo, pelo companheirismo e torcida.

À minha segunda família Bartolomeu, Bernadete, Lucas e Clara, pela torcida e suporte nas idas e vindas entre Arapiraca e Campina Grande, e toda família Ferreira/Lopes.

Aos meus orientadores, Angelo e Hyggo, pelas conversas, paciência, sugestões, oportunidades a mim concedidas e confiança depositada durante os últimos anos.

Aos meus colegas do laboratório Embedded, Ivo e Lenardo, e aos demais professores e companheiros de trabalho da UFAL/Arapiraca, Elthon, A. Paes, A. Barbosa, Patrick, Raquel, Fabiane, Mário, Afonso, Rodolfo, Rômulo e Tércio.

À minha família do Movimento dos Focolares de Alagoas e Paraíba, pelas orações, suporte e estímulo, em especial Rodrigo e Carol, Valtencir e Inês, e aos meus queridos amigos de Campina Grande, João Alfredo e Bruno Gama, pelo suporte desde o início dessa jornada.

Aos meus amigos de infância José Neto e Ana Lyvia, Alisson e Roberta, Arthur e Bárbara, pela torcida e orações.

À CAPES, pelo apoio financeiro.

Resumo

As Redes Ad Hoc Veiculares (ou VANETs) têm como principal objetivo a execução de sistemas de transporte inteligente, onde veículos são capazes de compartilhar informações entre si. Neste contexto, veículos transmitem basicamente dois tipos de mensagens (ou eventos), a saber: periódicas ou esporádicas. No primeiro caso, mensagens são transmitidas para informar a outros nós dados como velocidade, direção e posição atuais. Por outro lado, mensagens esporádicas podem ser transmitidas para anunciar acontecimentos, tais como acidentes, condições adversas de ruas e estradas, aproximação de veículos de emergência etc. Com efeito, as mensagens transmitidas devem incluir informações suficientes para garantir a autenticidade do nó transmissor, propriedade basilar e importante em todo sistema distribuído. Em contrapartida, se diferentes mensagens, em diferentes regiões geográficas, forem associadas e inferidas como oriundas de um mesmo veículo, torna-se assim possível a construção de um perfil de rotas desse veículo e, consequentemente, uma possível quebra do anonimato de um usuário. Uma forma de evitar esse monitoramento é permitir que um veículo utilize múltiplas identidades em diferentes momentos, uma estratégia denominada *pseudonimato*. Entretanto, apesar de proporcionar um meio simples para dificultar o monitoramento dos veículos, a estratégia de pseudonimato permite que um veículo malicioso faça uso de duas ou mais identidades (pseudônimos) ao mesmo tempo para anunciar um mesmo evento falso, o que caracteriza um ataque denominado *sybil*. Desta forma, propõe-se nesta tese o protocolo *ASAP*-V, cujo principal objetivo é prover autenticação de veículos e detecção de ataques *sybil* com suporte ao controle de anonimato dos usuários em redes VANETs. Para tal, é proposto um modelo de autenticação baseado no esquema de assinaturas de grupos que, combinado com uma arquitetura multinível de conjuntos anonimato, é possível detectar ataques *sybil* enquanto promovem-se os requisitos de segurança tais como não-repúdio e o controle de anonimato. Através de uma análise formal do protocolo de autenticação e do modelo de controle de anonimato, bem como de uma série de experimentos em simuladores, pôde-se comparar os resultados obtidos com outras abordagens encontradas na literatura. Observou-se, assim, como principais avanços da presente pesquisa, que o protocolo *ASAP*-V detecta veículos legítimos e maliciosos em um tempo médio 90% menor quando comparado a outras abordagens, e é resiliente a detecções *falso-positivo* e *falso-negativo*.

Abstract

The VANET (Vehicle Ad Hoc Networks) network aims at allowing the development of intelligent transportation systems, in which the vehicles are mobile nodes that can communicate with each other to share information. In order to make it possible, each vehicle may transmit two types of messages (or events): beacon messages and event-based messages. The former announces vehicle's current position, speed, and direction to neighbors, allowing other vehicles to perceive and predict the kinematics of the vehicle. The last one are sent in order to announce sporadic events, such as accident report, road hazard condition notification, emergency vehicle approaching etc. Within this context, each message must attach enough information in order to guarantee vehicle authentication, a fundamental security requirement to any distributed system. On the other hand, if different messages in different geographical areas are linked to the same vehicle, an intruder may build a vehicle's route profile, a potential threat to user's privacy. To avoid such threat, it is possible to allow a vehicle to keep multiple identities at different moment, a strategy called *pseudonymity*. However, although such an approach provides a simple security solution to avoid vehicle monitoring, the strategy of pseudonymity allows a malicious vehicle to use two or more identities (pseudonyms) at the same time to announce the same false event, a network attack called the *sybil* attack. In this perspective, this thesis proposes a privacy-preserving authentication and sybil attack detection protocol called $ASAP$-V. To this end, we propose an authentication model based on the group signature scheme and combines such approach with a multi-level k-anonymity set architecture to detect sybil attacks, while promoting message non-repudiation and users privacy control. Through a formal analysis of the authentication protocol and the anonymity control model, as well as through a series of experimental simulations, results suggest that $ASAP$-V is more efficient than the state of the art approaches, mainly because it detects legitimate and malicious vehicle faster, and is resilient to *false-positive* and *false-negative sybil* detections.

Sumário

Lista de Símbolos e Abreviaturas

ASAP-V *Authentication and Sybil Attack detection Protocol for VANETs*

C.A *Autoridade Certificadora* (do inglês, *Certificate Authority*)

C2C *Carro a carro* (do inglês, *Car-to-Car*)

dBm *decibels relative to one milliwatt*

DNT *Departamento Nacional de Trânsito*

DoS *Negação de Serviço* (do inglês, *Denial-of-Service*)

DSRC *Comunicação de Curto Alcance Dedicado* (do inglês, *Dedicated Short-Range Communications*)

ECDSA *Algoritmo de Assinatura Digital de Curvas Elipticas* (do inglês, *Elliptic Curve Digital Signature Algorithm*)

EEBL *Frenagem de Emergência* (do inglês, *Electronic Emergency Brake Light*)

FSM *Máquina de Estado Finito* (do inglês, *Finite-State Machine*)

gmsk *Chave de Gerenciamento de Grupo* (do inglês, *Group Management Singing Key*)

GPS *Sistema de Posição Global* (do inglês, *Global Positioning System*)

GPSR *Greedy Perimeter Stateless Routing*

grt *Group Revocation Token*

gsk *Group Signing Key*

LLC *Logical Link Control*

MAC *Controle de Acesso ao Meio* (do inglês, *Medium Access Control*)

MANET *Mobile Ad Hoc Networks*

MITM *Ataque de Homem do Meio* (do inglês, *Man-In-The-Middle Attack*)

OBU *On-Board Unit*

OFDM Modulação por Divisão Ortogonal de Frequência (do inglês, *Orthogonal Frequency-Division Multiplexing*)

P2P *Ponto a Ponto* (do inglês, *Peer-to-Peer*)

PKI *Infraestrutura de Chaves Públicas* (do inglês, *Public-key Infrastructure*)

QoS *Qualidade de Serviço* (do inglês, *Quality of Service*)

RFID *Identificação por Rádio Frequência* (do inglês, *Radio Frequency IDentification*)

RHCN *Notificação de Condição Adversa de Pista* (do inglês, *Road Hazard Condition Notification*)

RSA *Ron, Shamir, Adleman*

RSSF *Redes de Sensores Sem Fio*

RSU *Unidade de Acostamento* (do inglês, *Road Side Unit*)

SNR *Relação sinal-ruído* (do inglês, *Signal to Noise Ratio*)

TCP *Protocolo de Controle de Transporte* (do inglês, *Transport Control Protocol*)

TPD *Dispositivo Resistente a Prova de Falsificação* (do inglês, *Tamper-Proof Device*)

TRR *Teste de Recurso de Rádio*

UDP *Protocolo de Datagrama do Usuário* (do inglês, *User Datagram Protocol*)

V2I *Vehicular to Infrastructure*

V2V *Vehicular to Vehicular*

VANET *Redes Ad Hoc Veiculares* (do inglês, *Vehicular Ad Hoc Network*)

WANET *Rede Ad Hoc Sem Fio* (do inglês, *Wireless Ad Hoc Network*)

WAVE *Wireless Access in Vehicular Environment*

WSM *WAVE Short Messages*

WSMP *WAVE Short Message Protocol*

Lista de Tabelas

Lista de Figuras

Capítulo 1

Introdução

O trabalho relatado neste documento de tese está num contexto que envolve a concepção e o desenvolvimento de um protocolo de segurança para redes veiculares. Mais especificamente na temática sobre autenticação, ataques *sybil* e o controle de anonimato dos usuários em ambientes veiculares. Tais aspectos formam o cerne desta pesquisa.

Neste capítulo, apresenta-se uma visão geral desta tese. Inicia-se por uma breve contextualização sobre redes *ad hoc* móveis e, mais especificamente, sobre redes *ad hoc* veiculares. Em seguida, relatam-se os principais problemas de segurança que podem ser explorados nas futuras redes veiculares. Prossegue-se com uma discussão sobre a problemática que permeia os trabalhos desenvolvidos na área onde está inserida esta pesquisa, com a apresentação das hipóteses consideradas para a solução proposta, das delimitações de pesquisa e dos objetivos do trabalho. Finalmente, conclui-se com a relevância do problema abordado, das principais contribuições da tese, e da organização geral deste documento.

1.1 Contextualização e Motivação

As Redes Ad Hoc Móveis (*Mobile Ad Hoc Networks* ou MANETs) [1] são caracterizadas por nós móveis que se comunicam através de redes sem fio e não demandam uma infraestrutura centralizada. Tal comunicação pode ser direta entre os nós ou através de múltiplos saltos, quando a distância entre os nós transmissor e receptor for maior que o alcance do sinal transmitido. Em cenários com múltiplos saltos, os nós intermediários entre o transmissor e o receptor implementam um roteamento colaborativo dos pacotes fim a fim. Devido à mobilidade dos nós, as redes MANETs possuem conexões transientes e podem tornar a topologia da rede muito dinâmica.

No contexto de MANETs, as Redes Ad Hoc Veiculares (*Vehicular Ad Hoc Networks* ou

VANETs) [2] têm como principal objetivo permitir que veículos[1] se comuniquem e formem redes de comunicação *ad hoc* ao longo das estradas, proporcionando uma gama de novas aplicações voltadas para a segurança no transporte, eficiência de tráfego e disseminação de informações em tempo real. A arquitetura geral das VANETs pode ser observada na Figura 1.1. Conexões podem ser estabelecidas diretamente entre os veículos ou entre os veículos e unidades de acostamento (RSU, do inglês, *Road Side Unit*) ao longo das estradas, as quais podem exercer funções de pontos de acesso para outras redes ou de auxílio para serviços tal como a disseminação de informações em ambientes veiculares esparsos.

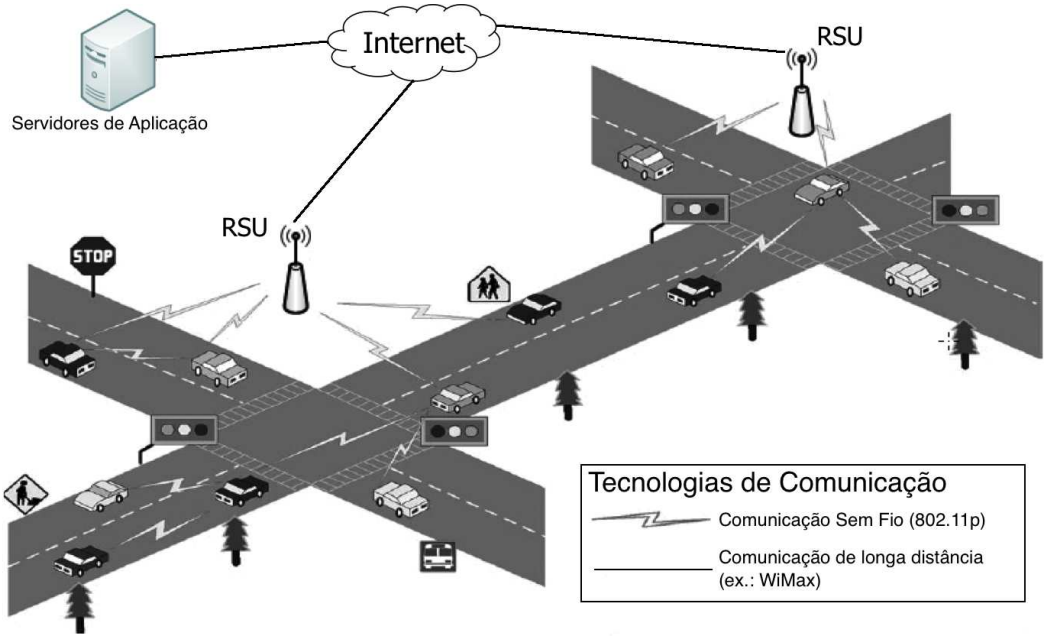


Figura 1.1: Cenário de Comunicação em Redes Ad Hoc Veiculares (Adaptada de [3]).

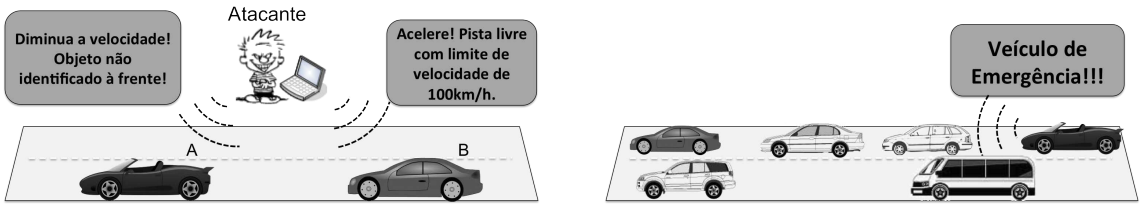
Com efeito, em redes VANETs é possível encontrar características peculiares quando comparadas a outras redes *ad hoc* móveis sem fio. Devido à natureza dos nós, eles podem se mover em altas velocidades e em trajetórias que acompanham os limites das estradas; possuem maiores recursos de energia e tempo reduzido em contato com outros nós, porém, demandam baixa latência e alta confiabilidade [4]. Estas características tornam um nó previsível quanto ao seu trajeto, bem como as conexões entre as entidades muito transientes, porém, permitem projetar nós com maior poder computacional quando comparado a nós presentes em outras redes sem fio.

Dentre os diversos documentos que especificam as redes VANETs, estão definidos no IEEE P1609.2 [5] os requisitos de segurança, tais como algoritmos de criptografia e formatos de mensagens seguras, como também a necessidade de suporte à autenticação, confidencialidade, integridade e não-repúdio de mensagens. Proporcionar tais requisitos

[1] Os termos "veículo" e "nó" serão utilizados indistintamente.

são desafiadores, pois o meio de comunicação sem fio, a ausência de uma infraestrutura centralizada e o roteamento colaborativo em múltiplos saltos são aspectos que tornam as redes VANETs alvos de diversos tipos de ataques.

Ataques às redes veiculares podem ser críticos em muitos casos devido às proporções alcançadas em caso de sucesso. Os cenários da Figura 1.2 ilustram potenciais ataques explorados pela falta de mecanismos de autenticação, introduzindo riscos à segurança dos passageiros. Mecanismos de autenticação e não-repúdio devem permitir que veículos determinem a autenticidade do emissor, garantindo que as mensagens recebidas são oriundas de uma entidade certificada como autêntica por terceiros (ex.: Autoridades Certificadoras, ou C.A, do inglês *Certification Authority*).

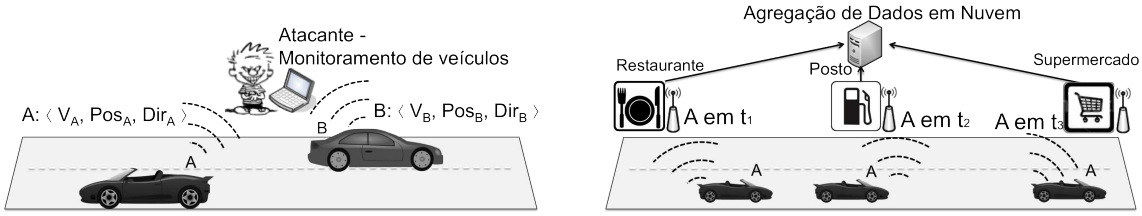


(a) Potencial colisão entre veículos devido a mensagens falsas.

(b) Veículo visa obter pista livre desfarçando-se de veículo de emergência.

Figura 1.2: Representação de mecanismos de autenticação, os quais devem garantir a autenticidade, a integridade e o não-repúdio das mensagens transmitidas.

Em redes VANETs, os veículos enviam mensagens periódicas para a rede com o objetivo de informar sua localização, direção e velocidade em um determinado instante. Estas mensagens são sensíveis ao acesso indevido e podem ser monitoradas por nós mal-intencionados, possibilitando a violação de anonimato do motorista [6]. Os cenários da Figura 1.3 ilustram potenciais formas de monitoramento de veículos, ocorrendo de maneira centralizada ou distribuída [7]. No primeiro caso, as mensagens periódicas são monitoradas em um único local através de um atacante situado ao longo da via. No segundo caso, as mensagens periódicas são monitoradas em diferentes lugares, permitindo que os dados de monitoramento sejam agregados e um perfil de rotas seja construído para uma análise a *posteriori*.



(a) Monitoramento de mensagens periódicas de forma centralizado. Veículos transmitem mensagens periódicas com informações sobre velocidade (V), posição (Pos) e direção (Dir), respectivamente.

(b) Monitoramento de mensagens periódicas de forma distribuída. Informações sobre velocidade, posição e direção do veículo A são coletadas para posterior processamento.

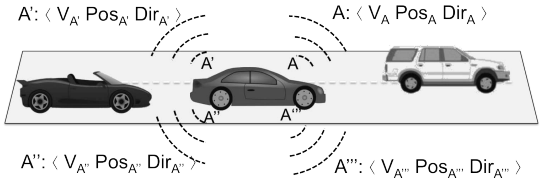
Figura 1.3: Representação de potenciais ataques contra o anonimato dos motoristas em VANETs.

Uma forma de evitar tais monitoramentos é permitir que um veículo utilize múltiplas identidades (pseudônimos) em diferentes momentos [8–11], uma estratégia denominada *pseudonimato* [12]. Sob a ótica do controle de anonimato dos usuários e do gerenciamento de identidades, estudos realizados mostram que a abordagem de pseudonimato é a mais adequada para a distribuição de identidades em redes VANETs [13].

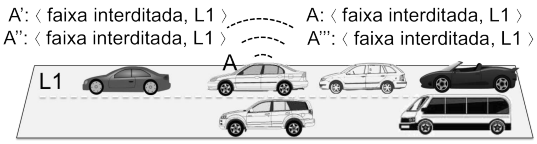
Porém, apesar de proporcionar um meio simples e direto para dificultar o monitoramento dos veículos, a estratégia de pseudonimato permite que um veículo faça uso de duas ou mais identidades ao mesmo tempo para anunciar um evento falso, o que pode caracterizar um ataque denominado *sybil*[2] [14, 15]. Como ilustrado na Figura 1.4, um veículo malicioso (*sybil*) envia mensagens periódicas autenticadas com diferentes identidades (A, A', A", A"'), ou mensagens de eventos falsos sobre informações adversas como acidentes ou pontos interditados. Desta forma, como as mensagens são autênticas, veículos no raio de transmissão do veículo malicioso poderão considerar as mensagens como oriundas de quatro veículos legítimos diferentes, o que pode aumentar a probabilidade de que tais veículos considerem os eventos como verdadeiros [16]. Ataques *sybil* em redes VANETs têm sido considerados tão perigosos quanto ataques de negação de serviços, uma vez que a execução de um ataque *sybil* também poderá impedir o funcionamento correto da rede [17].

Os mecanismos para o controle de anonimato e modelos para a prevenção de ataques *sybil* são requisitos importantes [18], porém, contraditórios se garantidos por completo. Isto é, garantir controle total do anonimato de um veículo pode abrir oportunidades para ataques *sybil*, bem como garantir detecção de ataques *sybil* pode permitir a violação do anonimato de um veículo. De acordo com Douceur [14], a única forma de garantir a

[2]A expressão *Sybil* é título de um livro publicado em 1973 e que trata sobre Shirley Ardell Mason, o caso mais famoso de uma pessoa diagnosticada com o problema de múltiplas personalidades.



(a) Mensagens periódicas oriundas do mesmo veículo, porém, alternadas com diferentes identidades.



(b) Mensagens esporádicas sobre faixa interditada oriundas do mesmo veículo, porém, com diferentes identidades.

Figura 1.4: Representação de veículo malicioso *sybil* A que autentica diferentes mensagens com diferentes identidades (A, A', A", A"').

detecção de um nó malicioso *sybil* em um sistema distribuído é através de uma entidade centralizada confiável que assegure a relação de apenas uma identidade para cada nó da rede, ou que duas ou mais identidades utilizadas para garantir anonimato sejam detectadas como pertencentes ao mesmo nó. Entretanto, devido à preocupação dos usuários no tocante à violação de anonimato[3], impedir e detectar ataques *sybil* em redes móveis, em especial, em redes VANETs, trazem interessantes desafios, uma vez que a falta de uma infraestrutura centralizada pode impedir tal procedimento.

Nesta perspectiva, o presente trabalho situa-se na área que envolve autenticação com suporte ao controle entre o anonimato dos usuários e a detecção de ataques *sybil* inseridos no contexto de redes veiculares. Nas seções a seguir, são discutidos a problemática que motivou a elaboração deste trabalho, assim como as delimitações da pesquisa, os objetivos do trabalho, a relevância do tema abordado e, finalmente, as principais contribuições alcançadas e a organização geral deste documento.

1.2 Problemática

Em um ataque *sybil*, um nó malicioso declara múltiplas identidades para o sistema a fim de burlar e obter mais recursos[4] do que merece, ou simplesmente com o objetivo de desestabilizar o sistema e/ou os demais usuários participantes. Esse tipo de ataque ocorre mais facilmente em sistemas nos quais uma identidade é obtida a um baixo custo e não há uma infraestrutura centralizada para garantir a unicidade da relação entre uma identidade e um nó. No contexto das redes VANETs, garantir tal unicidade pode levar

[3]Em pesquisa realizada pela Pew Research, os cidadãos norte-americanos parecem estar mais preocupados com temas como violação aos direitos civis e privacidade do que com a ameaça do terrorismo. Mais detalhes em`http://www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew`

[4]O termo "recurso" pode referir-se a quaisquer serviços oferecidos pelo sistema em uma rede de computadores.

a problemas inerentes à violação do anonimato dos usuários, uma vez que detectar um ataque *sybil* e promover o controle de anonimato podem ser visualizados como requisitos contraditórios. Além disso, em redes *ad hoc* não se pode garantir que uma infraestrutura centralizada de suporte à tomada de decisões (ex.: RSU) estará sempre disponível.

Como exemplo, considere o cenário ilustrado na Figura 1.5. O veículo com identidade E trafegando na via R1-R3 possui múltiplas identidades válidas (E, E', E_n) capazes de proporcioná-lo anonimato. Entretanto, mensagens periódicas com posições e, possivelmente, com velocidades e direções diferentes, são enviadas com n identidades diferentes (Etapa 1). Neste momento, os pontos de acesso RSU_1 e RSU_2, ao detectarem que há diferentes identidades com diferentes dados sobre posição, velocidade e direção, poderão inferir que há grande densidade de veículos na região. Desta forma, uma mensagem de evento sobre congestionamento (*Traffic Jam*) na via R1-R3 é gerada e enviada para os pontos de acesso RSU_3 e RSU_4 (Etapa 2). Tais pontos de acesso reenviam o evento para os veículos que trafegam na via R4-R6, o que poderá fazer com que tais veículos evitem a região R1-R3 através da região R2-R5 (Etapa 3). Nesse contexto, o recurso considerado são as vias públicas de acesso.

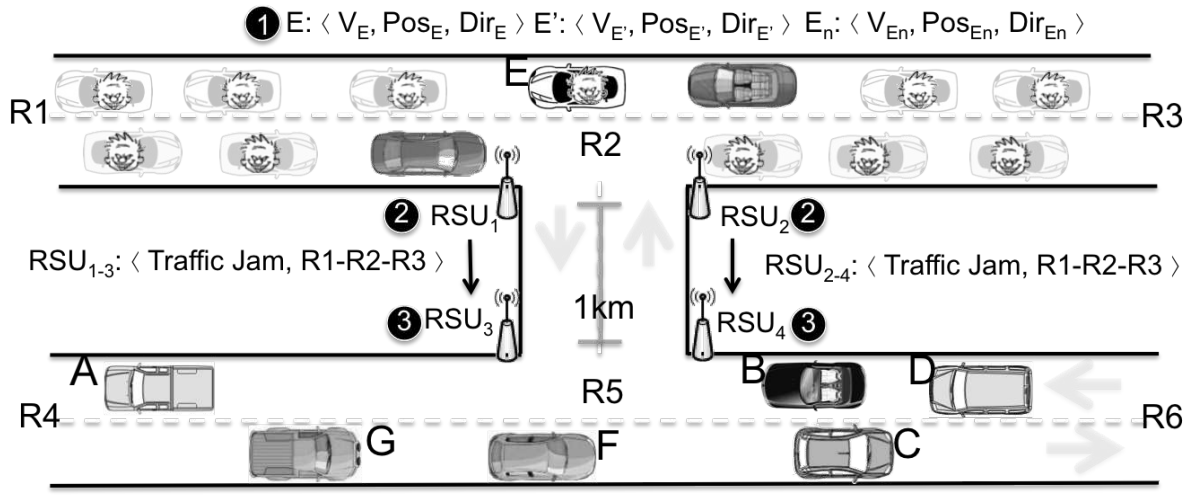


Figura 1.5: Representação de veículo *sybil* que gera mensagens periódicas com múltiplas identidades, permitindo a geração de evento falso sobre congestionamento.

Um dos principais objetivos das redes VANETs é diminuir as estatísticas cada vez maiores no tocante ao número de acidentes nas estradas e vias públicas. Tal objetivo pode ser vislumbrado a partir da comunicação bidirecional entre veículos e RSUs. No entanto, diversas categorias de aplicações poderão fatalmente pôr vidas em risco se a presença de veículos maliciosos *sybil* não for detectada. Como exemplo, considere o cenário ilustrado na Figura 1.6. Mensagens de eventos esporádicos, normalmente transmitidas através de mensagens *broadcasts*, podem ser exploradas por veículos maliciosos a fim de distribuir

informações falsas.

Na Figura 1.6 dois contextos são considerados: no *Contexto 1*, mensagens sobre pista escorregadia (*Road Hazard Condition Notification* - RHCN) nas posições Pos_{L1} e Pos_{L2} são enviadas aos veículos que se aproximam; e no *Contexto 2* mensagens de frenagem brusca (*Electronic Emergency Brake Light* - EEBL) também são transmitidas aos veículos que se aproximam. Em ambos os contextos, um veículo malicioso faz uso de n identidades (E', E", E_n) diferentes. Como consequência, os veículos que se aproximam tendem a desacelerar de forma brusca e rapidamente, o que pode ocasionar graves acidentes em diversos cenários, tal como em enfileiramento otimizado (*vehicle platooning* [19]). A probabilidade de aceitação de que tais eventos são verdadeiros é potencializada devido ao número de mensagens autênticas transmitidas pelo veículo malicioso para o mesmo evento. Diversas abordagens para detecção de mau comportamento de nós são suscetíveis a ataques *sybil* [20–22], como detalhado em [23].

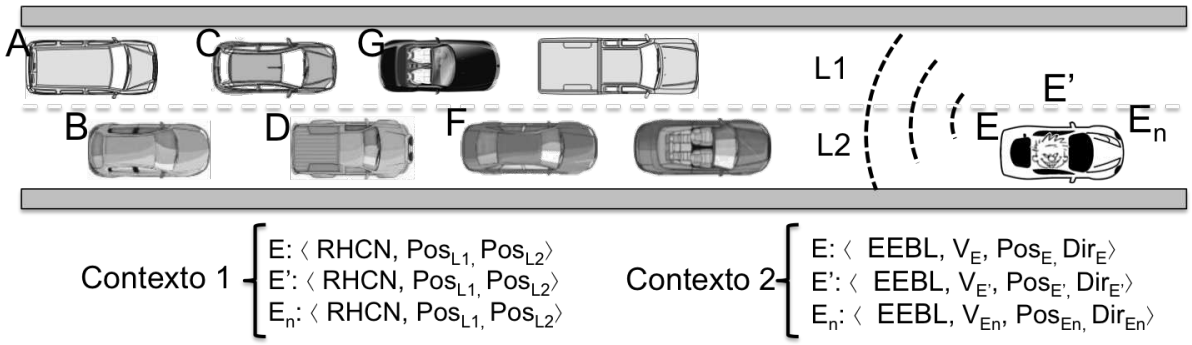


Figura 1.6: Representação de diferentes contextos de ataques que podem ser explorados por veículos *sybil* em mensagens esporádicas.

A presença de um veículo malicioso *sybil* também pode gerar impactos significativos em diversos serviços de rede. Em algoritmos de roteamento, um atacante pode criar várias identidades se fazendo passar por vários nós legítimos para criar falsos caminhos de roteamento [24], evitando que mensagens sejam entregues a um determinado nó [25], diminuindo a razão de entrega de pacotes (*Packet Delivery Ratio*) [24], a vazão total (*throughput*) e aumentando a perda de pacotes [26]. Ademais, evita-se também que outros nós participem do roteamento e consigam obter créditos por ter feito o roteamento em sistemas guiados por mecanismos de reputação [27, 28].

Como exemplo, considere o cenário ilustrado na Figura 1.7 no qual o veículo malicioso *sybil* E envia múltiplas mensagens periódicas com identidades E' e E". Supondo que os veículos A e D, separados a uma distância maior que o raio de transmissão dos respectivos rádios, enviem pacotes entre si, estes devem considerar os veículos vizinhos para o roteamento dos pacotes. Algoritmos de roteamento reativo baseados em posição/-

geográfico, tais como o GPSR (*Greedy Perimeter Stateless Routing*) [29, 30] e o MDDV (*Mobility-centric Data Dissemination Algorithm for Vehicular Networks*) [31] têm sido considerados promissores para redes VANETs, uma vez que tais protocolos consideram os nós vizinhos mais próximos do nó destino como potenciais roteadores [32]. Esta abordagem é interessante pois a alta mobilidade presente em redes VANETs altera a topologia da rede e, consequentemente, afeta o desempenho dos protocolos baseados em topologia (ex.: AOVD, do inglês *Ad-hoc on-demand distance vector* [33]) quando executados em redes VANETs. Desta forma, para o cenário em questão, tanto o veículo A quanto o veículo D deverão considerar os potenciais veículos E_1 e E_2, respectivamente, para o processo de roteamento dos pacotes, uma vez que ambas as posições encontram-se próximas aos destinos. Assim, pacotes enviados de A para D ($A \rightarrow E_1 \rightarrow D$) e pacotes enviados de D para A ($D \rightarrow E_2 \rightarrow A$) são, na verdade, entregues ao veículo malicioso *sybil* E, o qual poderá, por exemplo, descartá-los.

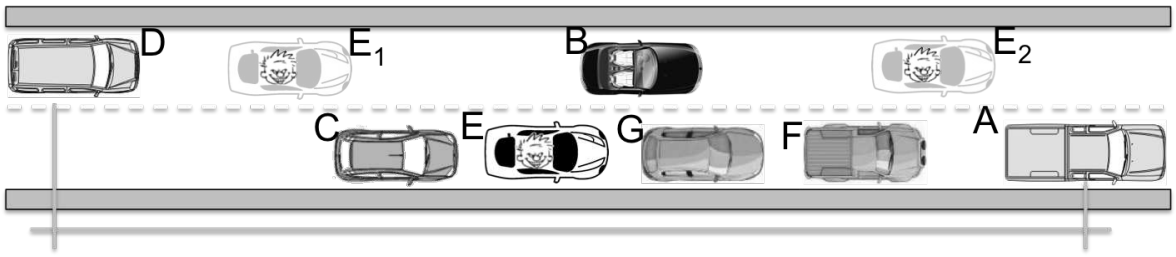


Figura 1.7: Representação de posições falsas geradas por veículo *sybil*, as quais podem aumentar a probabilidade do atacante participar do processo de roteamento e, consequentemente, receber mensagens originadas para outros veículos.

Uma forma de garantir que pacotes trafegados de um veículo a outro alcancem seus destinos mesmo com a presença de veículos maliciosos é através de (re)transmissões *broadcasts*, onde todos os veículos obrigatoriamente receberão os pacotes transmitidos. Uma forma de implementação dessa abordagem é através de *flooding*, na qual cada nó retransmite para a rede a mensagem recebida. Tal abordagem[5] funciona relativamente bem em um ambiente de baixa densidade de nós, porém, pode degradar a qualidade da rede em diversos fatores, a saber: se todo veículo retransmitir a mesma mensagem recebida (*broadcast storm*), então todos os veículos receberão mensagens redundantes; maior contenção no acesso ao meio, onde todos os veículos participantes da fase de retransmissão tentarão acesso ao meio (aproximadamente) ao mesmo tempo; congestionamento na rede devido ao maior tráfego de dados na rede; e, por fim, maior probabilidade de colisão de pacotes [35], uma vez que haverá tentativas simultâneas de acesso ao meio. Mesmo com a existência de outras abordagens para a disseminação de dados em redes VANETs que

[5]Amplamente conhecida como *broadcast storm* [34].

não apresentam problemas relacionados ao *broadcast storm* [35–41], um nó malicioso *sybil* poderá ser selecionado para o repasse de dados. Desta forma, é importante que veículos maliciosos sejam detectados antecipadamente.

Ataques *sybil* podem ocorrer em diferentes tipos de redes. Em redes P2P (*peer-to-peer*), Douceur [14] propõe uma abordagem para detectar ataques *sybil* a partir de testes de recursos computacionais, tais como processamento (fatoração de números grandes, por exemplo), memória e largura de banda. Para tal, parte-se da hipótese que um nó *sybil* E, com n ($n \geq 2$) identidades diferentes, não é capaz de processar um determinado trabalho em nome das n identidades em um intervalo de tempo Δt. Essa abordagem tem sido utilizada em redes P2P para combater ataques *sybil* em sistemas de reputação. Entretanto, um nó avaliador deve conhecer os limites dos recursos computacionais do nó avaliado *a priori* [42, 43], procedimento muitas vezes impossível em redes móveis devido à heterogeneidade de recursos computacionais e à dinâmica de entrada e saída de nós na rede [43]. No contexto de VANETs, um veículo a ser avaliado poderia ficar ocupado na execução de diferentes tarefas para cada veículo avaliador. Esta situação pode se agravar à medida que o número de veículos na rede aumenta.

Um outro tipo particular de teste de recursos é denominado teste de recurso de rádio (TRR) [44, 45], uma abordagem para lidar com ataques *sybil* em redes de sensores sem fio (RSSF). Parte-se da hipótese que um nó possui apenas um rádio de transmissão e é capaz de transmitir e receber quadros em apenas um canal do espectro por vez. Ao detectar n identidades diferentes, um nó avaliador requisita, para cada identidade n_i, a transmissão de quadros em um canal de transmissão específico. Se um potencial nó *sybil* gerou as n identidades, então esse nó não poderá transmitir dados em diferentes canais ao mesmo tempo e este é julgado como *sybil* com uma certa probabilidade p. No contexto de redes *ad hoc*, e mais especificamente em VANETs, não será possível garantir que um nó possua apenas um único rádio de transmissão. Além disso, essa abordagem pode sofrer com problemas de escalabilidade, uma vez que o processo de testes deverá ocorrer para cada (novo) veículo a ser avaliado no raio de transmissão.

Em VANETs, um ataque *sybil* pode ser explorado em abordagens que visam prover o controle de anonimato de um veículo [8–11], uma vez que múltiplas identidades são utilizadas para dificultar a construção de perfis de rotas de um veículo específico. Tais abordagens permitem que veículos armazenem múltiplas identidades autenticadas por uma C.A no momento do registro do veículo no sistema (ex.: sistema do departamento nacional de trânsito). O uso de cada identidade pode ocorrer em um intervalo de tempo específico e a renovação do conjunto de identidades pode ser realizada à medida que se esgotem as possibilidades de uso das identidades armazenadas. Tal renovação pode ser executada através das RSUs disponíveis ao longo das estradas ou durante procedimentos

de revisão do veículo [8].

Nesse contexto, para evitar o armazenamento de múltiplas identidades (ou pseudônimos) e, consequentemente, o uso descontrolado destas identidades para realizar ataques *sybil*, há soluções [3, 6, 46–49] que permitem a negociação de uma única identidade por veículo através das RSUs disponíveis ao longo das vias, e cada identidade sendo válida apenas na região da RSU, como ilustrado na Figura 1.8. Por outro lado, para cada RSU_i, um veículo deve autenticar-se para obter uma nova identidade, procedimento que permitiria construir um perfil de rotas a partir da agregação das informações de autenticação deste veículo em cada RSU_i. Além disso, a não disponibilidade de uma RSU pode facilitar o monitoramento e a associação dos serviços utilizados por um veículo específico e, como consequência, uma possível violação à privacidade.

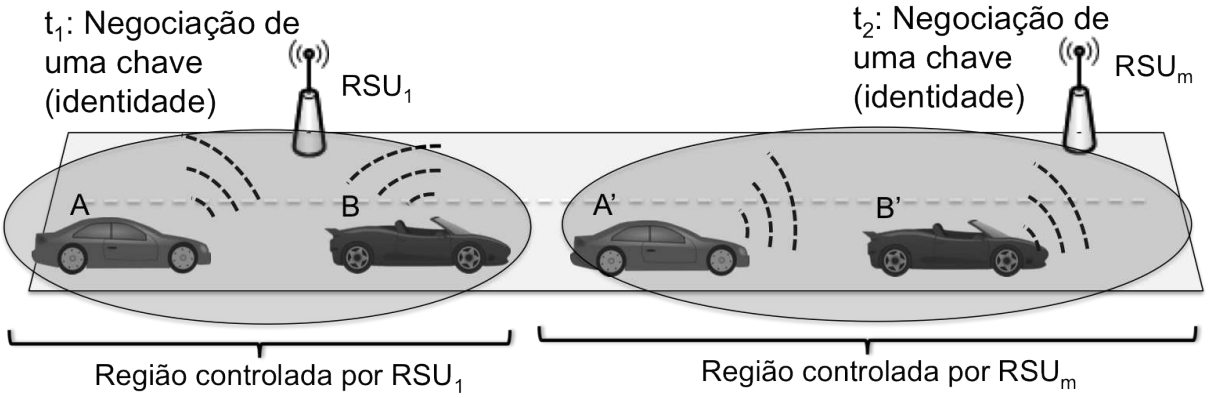


Figura 1.8: Representação de negociação de identidades temporárias através de RSUs.

O uso de RSUs como suporte para detecção de ataques *sybil* também é bastante explorado na literatura [50–52]. A abordagem proposta por Zhou et al [53, 54], chamada P^2DAP, permite o prévio armazenamento de múltiplas identidades e faz uso de RSUs e C.As para detectar potencial ataque *sybil*. Todavia, a detecção de ataques *sybil* através de RSUs é, evidentemente, dependente da presença de tal infraestrutura. Nesta perspectiva, estudos apontam que a distribuição uniforme das RSUs ao longo das vias poderá reduzir a vazão agregada total da rede veicular na região [55], além de provocar gargalos à rede [26]. Outros trabalhos sugerem a alocação de RSUs apenas nas intersecções entre vias [56, 57], proporcionando maior potencial de disseminação de informações. Desta forma, os modelos de comunicação entre veículos que dependem exclusivamente da disponibilidade de uma RSU não se mostram adequados para serem utilizados em ambientes veiculares reais.

Uma outra categoria de soluções para prover autenticação, controle de anonimato e detecção de ataques *sybil* busca explorar a relação espaço/tempo [58, 59]. Parte-se da hipótese que dois ou mais veículos não enviarão requisições para uma mesma RSU ao mesmo tempo, considerando que o deslocamento de cada veículo nas rodovias é distinto de

qualquer outro veículo. As soluções baseadas nesta categoria possuem limitações quanto ao fluxo de veículos nas rodovias. Como discutido em [60] e detalhado na Figura 1.9, um veículo poderá obter duas sequências de marcas de tempo diferentes caso uma RSU_i possua diferentes RSUs adjacentes (ex.: RSU R_1 e RSU R_2 são adjacentes a RSU R_3), e explorar essa característica de fluxo para realizar ataques *sybil*, gerando resultados de detecção *falso-negativo*, ou seja, quando um veículo malicioso *sybil* não é detectado como tal.

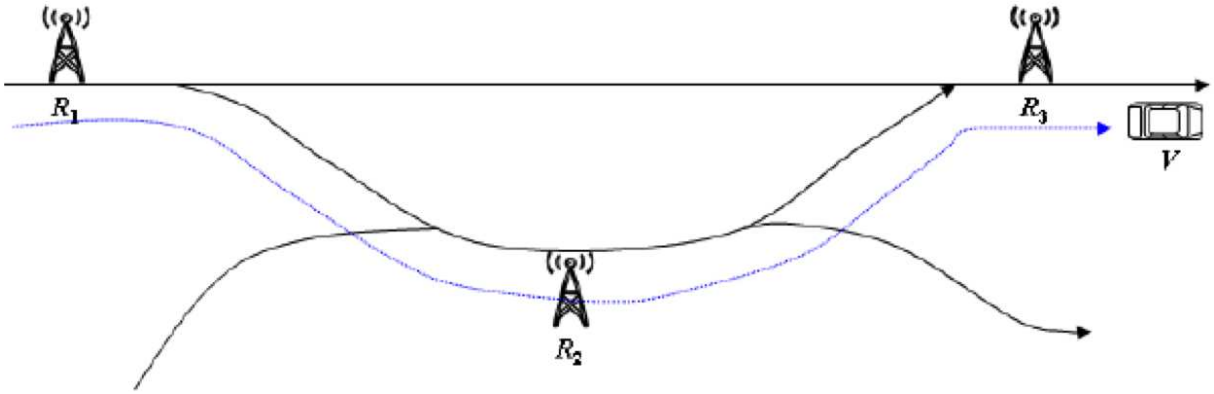


Figura 1.9: Representação de veículo V que pode obter duas sequências de marcas de tempo diferentes após trafegar pela RSU R_3: marcas de tempo sequenciais R_1 e R_3; e marcas de tempos sequenciais R_2 e R_3.

Outras abordagens para detecção de ataques *sybil* são baseadas no monitoramento e colaboração dos veículos vizinhos [61–65]. Nestas abordagens, parte-se de duas hipóteses, a saber: à medida que os nós se deslocam, identidades oriundas de um nó *sybil* são continuamente apresentadas durante a fase de transmissão de mensagens periódicas para um dado intervalo de tempo; e nós vizinhos a um nó *sybil* receberão mensagens periódicas possuindo as mesmas identidades (oriundas de um potencial nó *sybil* presente na região). Entretanto, as soluções baseadas em monitoramento dos nós vizinhos apresentam uma deficiência simples. Resultados *falso-positivo* - ou seja, quando um veículo legítimo é detectado como malicioso - poderão ser gerados quando diferentes identidades pertencentes a diferentes veículos deslocam-se em conjunto por um longo período de tempo. Da mesma forma, resultados *falso-negativo* também poderão ser gerados à medida que um veículo malicioso alterna diferentes identidades para diferentes intervalos de monitoramento.

O desafio de pesquisa, ora veiculado neste documento, reside em proporcionar um equilíbrio entre 4 requisitos de segurança, a saber: autenticação, não-repúdio, detecção de ataques *sybil* e controle de anonimato dos usuários. Como ilustrado na Figura 1.10, os requisitos tradicionais de segurança, tais como autenticação e não-repúdio, podem exigir a coleta de dados que identificam unicamente um nó na rede. Em redes VANETs, a autenticação de mensagens periódicas oferece a garantia de que há um veículo real

situado na região; por sua vez, o não-repúdio de mensagens transmitidas pelos veículos deve proporcionar um meio para execução de aplicações tais como emissão automática de multas (ex.: por excesso de velocidade) e investigação de crimes e acidentes. Por outro lado, tais requisitos podem permitir que um perfil de rotas de um dado veículo seja construído, o que pode expor o anonimato dos usuários. Assim, faz-se necessário proporcionar um equilíbrio entre autenticação e não-repúdio, e o controle de anonimato dos usuários.

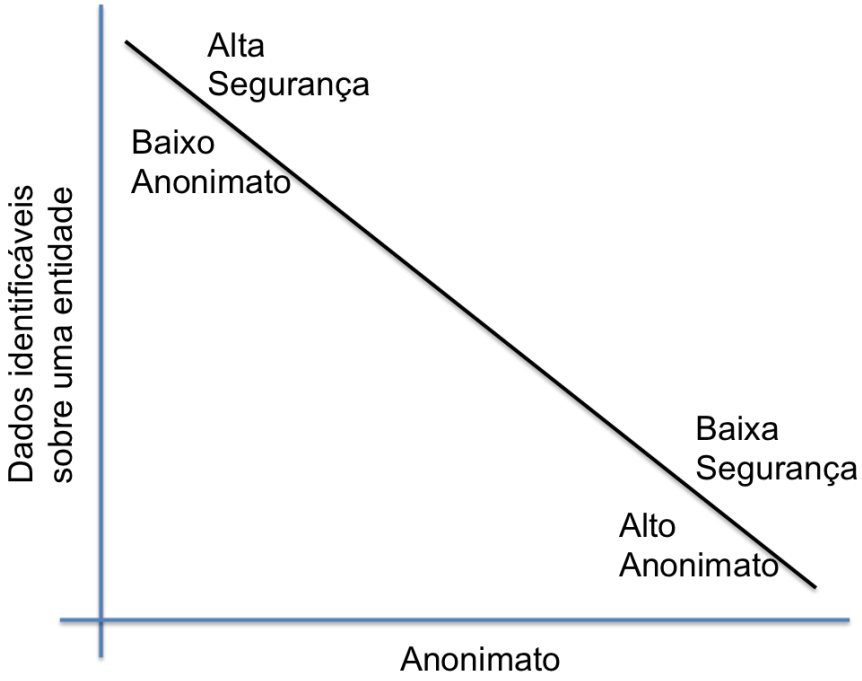


Figura 1.10: Autenticação, não-repúdio e detecção de ataques *sybil* exigem dados que identificam unicamente uma entidade, diminuindo o seu nível de anonimato. Por outro lado, anonimato requer menos dados identificáveis sobre a entidade, diminuindo o grau de segurança.

Outro requisito que pode expor o anonimato de um veículo é concernente à detecção de ataques *sybil*, ponto central desta pesquisa. Isso deve-se ao fato de que para garantir que um veículo seja *sybil*, as mensagens apresentando as múltiplas identidades devem unicamente identificá-lo. Porém, o fato de garantir que as múltiplas identidades unicamente identifica um veículo poderá expor o anonimato do usuário.

Nesta perspectiva, pretende-se responder a seguinte pergunta de pesquisa: como detectar e impedir ataques *sybil* sem afetar o anonimato dos usuários e sem a participação direta de uma infraestrutura fixa de suporte à decisão, tais como RSUs e C.A, garantindo também as propriedades de autenticação, integridade e não-repúdio de mensagens? Ademais, tentativas de ataques *sybil* sejam detectadas localmente, evitando resultados *falso-positivo* e *falso-negativo*, com participação apenas dos veículos na região e em tempo

relativamente curto devido à característica dinâmica da rede. Cumpre mencionar que não foram encontradas na literatura soluções cujos requisitos fossem combinados e contemplados.

1.3 Hipóteses

Para o problema exposto, adotam-se as seguintes hipóteses:

- H_0 - A partir do esquema de *assinaturas de grupo* [66] e dos conceitos de pseudonimato, é possível prover requisitos de autenticação de mensagens com suporte ao controle de anonimato dos usuários, bem como o não-repúdio de mensagens trafegadas na rede;
- H_1 - O modelo de *conjuntos anonimatos* [67] pode proporcionar meios para garantir anonimato dos usuários durante a fase de detecção de ataques *sybil*;
- H_2 - É possível detectar ataques *sybil* sem a presença de infraestruturas fixas ou mecanismos de confiança e reputação se existir uma combinação de atributos para cada veículo específico que o diferencie, temporariamente, dos demais veículos na região.

Em linhas gerais, mensagens transmitidas na rede e autenticadas através de assinaturas de grupo devem garantir os requisitos de não-repúdio e anonimato de um veículo. A partir de duas mensagens arbitrárias quaisquer, apenas entidades autorizadas (ex.: C.A) podem determinar a real identidade de um veículo e avaliar se ambas as mensagens são oriundas de um mesmo veículo. Além disso, o uso de pseudônimos proporciona meios para o controle de anonimato e para minimizar o impacto no processamento de mensagens periódicas através do esquema de criptografia de chaves assimétricas, tais como RSA [68] ou Curvas Elípticas [69].

Para a fase de detecção de ataques *sybil* seguindo a restrição de manter o anonimato de um veículo e não depender de serviços de reputação e confiança, parte-se da hipótese de que veículos devem compartilhar um conjunto de atributos com outros veículos, porém, deve possuir um atributo específico diferente de qualquer outro veículo do sistema. Portanto, se duas ou mais mensagens descrevendo o mesmo evento apresentam o mesmo conjunto de atributos, então as mensagens são oriundas de um ataque *sybil*.

1.4 Delimitação da Tese

Como discutido na seção anterior, o presente trabalho situa-se no contexto de autenticação, detecção de ataques *sybil* e controle de anonimato dos usuários em redes *ad hoc*

veiculares. Entretanto, o leitor deve atentar-se às seguintes delimitações de pesquisa:

1. um ataque *sybil* limita-se apenas ao uso de múltiplas identidades por um nó da rede com o objetivo de burlar serviços de aplicação e de rede. Ou seja, objetiva-se detectar o uso de múltiplas identidades em mensagens periódicas ou esporádicas. Desta forma, não é foco deste trabalho verificar a consistência das posições geográficas contidas nas mensagens periódicas enviadas pelos veículos, ou determinar a veracidade de ocorrência de um determinado evento esporádico;

2. o controle de anonimato dos usuários se restringe aos modelos de autenticação e distribuição de identidades aos veículos com base numa arquitetura de distribuição de chaves de criptografia. Ou seja, não é foco deste trabalho realizar ou garantir mecanismos de autenticação e controle de anonimato através de outros serviços, tais como análises de imagens de câmeras de segurança para monitoramento de placas de veículos [70].

1.5 Objetivos da Tese

Nesta seção são apresentados os principais objetivos do presente trabalho de tese.

1.5.1 Objetivo Principal

Neste trabalho, o objetivo principal é a especificação, o projeto e o desenvolvimento de um protocolo de autenticação de veículos e detecção de ataques *sybil* com suporte ao controle de anonimato dos usuários em redes VANETs denominado *ASAP*-V (do inglês, *Authentication and Sybil Attack detection Protocol for VANETs*). Para tal, os seguintes aspectos são considerados:

- Autenticação com suporte ao anonimato condicional: é fundamental que o protocolo de autenticação de veículos garanta que apenas entidades tais como C.As e governos possam associar as mensagens transmitidas por veículos a uma identidade única (ex.: dono do veículo), promovendo anonimato condicional. Ou seja, o anonimato condicional ocorre quando a relação entre mensagem e identidade manifesta-se apenas em casos específicos, tais como na investigação de crimes ou acidentes, processos similares à quebra de sigilos telefônico ou bancário. Além disso, o protocolo de autenticação também deve garantir que uma mensagem originada de um veículo específico seja impossível de ter sido transmitida por um veículo diferente senão aquele, proporcionando mecanismos de não-repúdio;

- Detecção de ataques *sybil* sem afetar o anonimato condicional: a detecção de um possível ataque *sybil* não pode afetar o anonimato condicional de veículos legítimos, isto é, a relação entre mensagem e a identidade real de um veículo legítimo não pode ser estabelecida durante o processo de detecção de ataque *sybil*, buscando eliminar também as chances de resultados *falso-positivo*, ou seja, quando um veículo legítimo é avaliado como malicioso;

- Detecção de ataques *sybil* na região de ataque: é essencial que a detecção de ataques *sybil* seja realizada na região onde o ataque ocorre e sem a necessidade de uma infraestrutura fixa, tais como RSUs ou C.As. Desta forma, mensagens suspeitas devem ser simplesmente descartadas ou armazenadas para posterior processamento;

- Detecção de ataques *sybil* sem necessidades de mecanismos de reputação, e resiliente ao conluio entre veículos *sybil*: o protocolo para detectar ataques *sybil* deve atuar de forma distribuída em cada veículo e sem a necessidade de mecanismos de reputação de veículos, uma vez que tais mecanismos podem ser afetados por ataques *sybil* [71]. Além disso, o conluio de veículos maliciosos não pode afetar a confiabilidade de mensagens oriundas de veículos legítimos;

- Exclusão do veículo malicioso da rede: uma vez detectado um veículo *sybil*, este deve ser excluído da rede. Objetiva-se minimizar o impacto de futuros ataques deste veículo na rede. Este processo deve ocorrer através de um procedimento de acusação, nos quais veículos que detectaram o ataque enviam para a C.A cópias de mensagens oriundas do veículo *sybil* utilizadas durante o ataque;

- Garantias de detecção de veículos maliciosos: a solução proposta deve garantir que um veículo malicioso seja detectado (resiliência a resultados *falso-negativo*, e veículos legítimos não sejam detectados como maliciosos (resiliência a resultados *falso-positivo*).

1.5.2 Objetivos Específicos

Para alcançar os objetivos delineados anteriormente, as seguintes atividades foram consideradas:

1. Compreender os modelos e protocolos de autenticação e detecção de ataques *sybil* em redes MANETs, especialmente em redes VANETs, bem como as diretrizes e modelos para controle de anonimato em sistemas computacionais;

2. Definir um protocolo para detectar e impedir ataques *sybil* em redes VANETs e, ao mesmo tempo, oferecer suporte ao controle de anonimato dos veículos. Para

tal, devem-se garantir as propriedades de autenticação de veículos, integridade e não-repúdio de mensagens, ao passo em que tentativas de ataques *sybil* devem ser detectadas mesmo com a ausência de RSUs e sem expor o anonimato de veículos legítimos;

3. Implementar o protocolo proposto em um simulador de rede e realizar experimentos considerando diferentes cenários. Objetiva-se, assim, avaliar o protocolo;

4. Avaliar e discutir os resultados obtidos considerando as seguintes métricas: confiabilidade do protocolo de autenticação, grau de anonimato oferecido pela solução, sobrecarga imposta pelo protocolo com relação ao gerenciamento, processamento, armazenamento e comunicação, e o tempo médio de detecção de ataques *sybil*. Tais métricas são avaliadas considerando diferentes topologias de rede;

5. Discutir e comparar os principais resultados obtidos com as abordagens encontradas na literatura.

1.6 Relevância da Tese

O uso de múltiplas identidades para prover autenticação e controle de anonimato em redes VANETs permite que um veículo realize um ataque denominado *sybil*. Em um ataque *sybil*, o veículo pode utilizar as múltiplas identidades para construir uma fração de veículos inexistentes, objetivando inúmeros ganhos e causando impactos na execução de diversos serviços da rede. De modo geral, sistemas que possuem um controle fraco do esquema de criação e associação de identidades são suscetíveis a ataques *sybil* [72].

A complexidade de equilibrar os requisitos de controle de anonimato dos veículos e a detecção de um nó malicioso está no fato de que um potencial nó *sybil* é autêntico, isto é, as múltiplas identidades possuem propriedades que o garantem ser uma entidade autenticada por terceiros. Mensagens oriundas de um nó *sybil* não apresentam diferenças no tocante à autenticidade de outras mensagens oriundas de nós legítimos, o que torna o problema ainda mais desafiador. Ademais, detectar um ataque *sybil* e prover controle de anonimato de veículos podem ser visualizados como requisitos contraditórios, ou seja, garantir a execução com sucesso[6] de um, poderá afetar o outro.

Como discutido na Seção 1.2, ataques *sybil* em redes VANETs podem trazer impactos significativos em serviços de rede, tais como em algoritmos de roteamento, evitando que mensagens sejam entregues a um determinado nó, bem como impactar na razão de entrega de pacotes, na vazão e na perda de pacotes. Em uma outra vertente, algoritmos

[6]Nesse contexto, o termo "sucesso" refere-se à execução do requisito de forma que ele realize a tarefa completa para a qual foi projetado.

de predição de percurso que utilizam as mensagens periódicas oriundas de um veículo malicioso *sybil* poderão tomar decisões errôneas, uma vez que não há a existência real do veículo associado às identidades presentes nas mensagens periódicas [73–75].

Outros tipos de ataques são passíveis de serem executados com a presença de um veículo malicioso *sybil*, incluindo ataques de negação de serviço e injeção de eventos falsos [76]. Por fim, como discutido em [13, 77], se o mecanismo de revogação de certificados digitais for baseado em sistemas de votação, por exemplo, um ataque *sybil* poderá distorcer os resultados e influenciar na revogação de certificados de veículos legítimos. Dentro do contexto de VANETs, a proposta de Raya et. al. [78] segue o modelo de revogação de certificados por votações e, caso uma entidade central não seja considerada, um ataque *sybil* pode fatalmente comprometer os resultados de revogação.

Nesta perspectiva, devido às consequências de um ataque *sybil* em redes VANETs, a construção de modelos e mecanismos para combinar requisitos de autenticação, detecção de ataques *sybil* e o controle de anonimato de um veículo é de real valia para prover confiabilidade em futuros ambientes veiculares, sendo estes requisitos apenas um dos pilares para a segurança das redes VANETs. Por fim, a partir do desenvolvimento deste trabalho, espera-se contribuir para uma lacuna no estado da arte que envolve pesquisas relacionadas à autenticação, detecção de ataques *sybil* e controle de anonimato em VANETs.

1.7 Resumo das Contribuições da Tese

- **Uma nova abordagem para autenticação de veículos**: foi desenvolvido um novo protocolo para autenticação de veículos com suporte ao controle de anonimato, não-repúdio, e identificação correta de veículos maliciosos;

- **Uma arquitetura multinível para agrupamento de veículos**: foi definida uma arquitetura multinível de conjuntos anonimato, permitindo que veículos compartilhem um subconjuto de atributos e torne mais complexa a identificação de uma mensagem transmitida na rede;

- **Um protocolo para acusação de veículos maliciosos**: foi definido um protocolo para informar a um sistema de gerenciamento de redes veiculares potenciais ataques detectados na rede;

- **Descentralização do processo de detecção de ataques *sybil***: foi desenvolvida uma abordagem para detectar ataques *sybil* de forma distribuída e independente da presença de uma infraestrutura fixa. Desta forma, o protocolo *ASAP*-V é capaz de detectar ataques *sybil* mesmo sem a presença física de uma RSU e conectividade com uma C.A;

- **Resiliência a detecções *falso-positivo* e *falso-negativo***: a abordagem proposta para detectar ataques *sybil* é imune a resultados *falso-positivo* e *falso-negativo*.

1.8 Estrutura do Documento

Este documento está estruturado em capítulos, organizados como descritos a seguir:

- **Capítulo 1**: apresentou-se uma visão global da tese, seguindo uma direção que partiu inicialmente de uma contextualização sobre o tema e da problemática que permeia os trabalhos encontrados na literatura. Em seguida, foram descritas as hipóteses para solucionar o problema, abordados o escopo e as delimitações do trabalho, bem como delineados os objetivos e a relevância do tema e do trabalho. Por fim, foram descritas, de forma sucinta, as principais contribuições da presente pesquisa;

- **Capítulo 2**: apresentam-se conceitos relacionados ao tema abordado neste trabalho. Assim, é realizada uma síntese sobre as VANETs, delineando os principais conceitos, cenários de aplicação, padrões e projetos existentes. Prossegue-se abordando as potenciais vulnerabilidades e ataques em redes VANETs, com foco especial em conceitos sobre controle de anonimato e ataques *sybil*. Conclui-se apresentando potenciais ataques *sybil* em outras aplicações de redes;

- **Capítulo 3**: discute-se as abordagens existentes na literatura e é realizada uma comparação arquitetural entre as abordagens e o presente trabalho de tese. Em seguida, descrevem-se as principais limitações de cada abordagem e, ao fim, apresenta-se um quadro comparativo entre as abordagens através de um conjunto de requisitos que devem ser contemplados em soluções com foco em autenticação e detecção de ataques *sybil* em VANETs;

- **Capítulo 4**: descrevem-se a concepção e o projeto do protocolo $ASAP$-V. Em linhas gerais, são apresentados o método utilizado, a arquitetura principal do protocolo, o funcionamento geral da solução proposta e, por fim, cenários de aplicação;

- **Capítulo 5**: apresentam-se os principais resultados alcançados. É realizada uma análise detalhada do protocolo de autenticação proposto, bem como do grau de anonimato provido pelo protocolo, e uma análise dos custos computacionais exigidos pelo protocolo. Prossegue-se apresentando os parâmetros de rede considerados nos experimentos e os principais resultados alcançados relacionados à fase de detecção de ataques *sybil*. Finaliza-se com um breve comparativo dos resultados alcançados com outras abordagens disponíveis na literatura;

- **Capítulo 6**: são apresentadas as considerações finais. Inicia-se com uma breve apresentação sobre o problema e o tema abordados. Prossegue-se delineando os objetivos alcançados e as etapas executadas para contemplar os objetivos do trabalho proposto. Por fim, são descritas as principais contribuições da presente pesquisa e das perspectivas futuras do trabalho.

Capítulo 2

Fundamentação

Neste capítulo são apresentados conceitos sobre as Redes Ad Hoc Veiculares (VANETs), descrevendo as características fundamentais para a compreensão do restante do documento. Assim, inicia-se com a introdução de conceitos básicos sobre Redes Ad Hoc Veiculares, suas principais características, projetos e cenários que podem ser vislumbrados. Prossegue-se com uma breve apresentação sobre os potenciais problemas relativos a alguns tipos de ataques que podem ser explorados em redes veiculares, com maior foco em ataques *sybil* e controle de anonimato. Por fim, é discutido como os ataques *sybil* são explorados em outras arquiteturas de aplicação.

2.1 Introdução

Diversos avanços tecnológicos presentes nos atuais veículos automotores visam melhorar a experiência do condutor e dos passageiros. Exemplos de tais tecnologias incluem a utilização de sistemas de frenagem, sensores capazes de detectar e advertir o condutor da proximidade de obstáculos, alarmes de velocidade acima do permitido e ajustes automáticos de bancos e retrovisores com base nas características físicas do motorista [79]. De modo geral, essas tecnologias são baseadas em sensores e atuadores que detectam e coletam sinais do ambiente e informam ao condutor. Entretanto, tais tecnologias são restritas à interação entre o veículo e o condutor.

A próxima etapa desse avanço tecnológico consiste no desenvolvimento de sistemas que permitem a interação entre diferentes veículos. O principal objetivo desses sistemas é permitir o desenvolvimento de uma rede através da qual seja possível executar sistemas de transporte inteligentes onde os veículos são nós capazes de trocar informações entre si. Nesse contexto, diversos serviços poderão ser executados, tais como localização de vagas em estacionamentos, alerta de aproximação de veículo de emergência, alerta cooperativo de acidentes, sistemas anticolisão, entre outros [2]. Ademais, vislumbra-se também o

acesso à internet e o compartilhamento de conteúdos multimídia entre os veículos.

A interação entre veículos é possível através das chamadas Redes Ad Hoc Veiculares (VANETs) [2]. Essas redes são compostas de veículos automotores e infraestruturas fixas localizadas às margens das vias. Devido à natureza dos nós, estas redes diferem de outras redes móveis em diversos fatores, a saber: os nós se movem em altas velocidades e em trajetórias que acompanham os limites das estradas; os nós possuem muitos recursos de energia e tempo reduzido em contato com outros nós, o que torna as conexões muito transientes; por fim, demandam baixa latência e alta confiabilidade. Devido a essas características particulares, os protocolos criados para outras redes sem fio, como as redes *ad hoc* móveis (MANETs), não são, em geral, adequados para redes VANETs.

As redes VANETs apresentam características importantes que devem ser consideradas ao projetar novas soluções para ambientes veiculares. Tais características incluem [2]:

- A natureza de comunicação: a comunicação entre os nós pode ser de forma *ad hoc*, onde veículos estabelecem comunicação entre si para a troca de informações e eventos, ou entre veículos e infraestruturas centralizadas ao longo das vias;

- Mobilidade e dinamismo: veículos modificam a localização com uma frequência maior que outros nós presentes em redes MANETs. Devido à alta velocidade de deslocamento, a conexão entre veículos pode se tornar muito transiente e a topologia da rede dinâmica. Como exemplo, o desenvolvimento de protocolos que envolvem agrupamento de nós, como ilustrado na Figura 2.1 torna-se ainda mais desafiador;

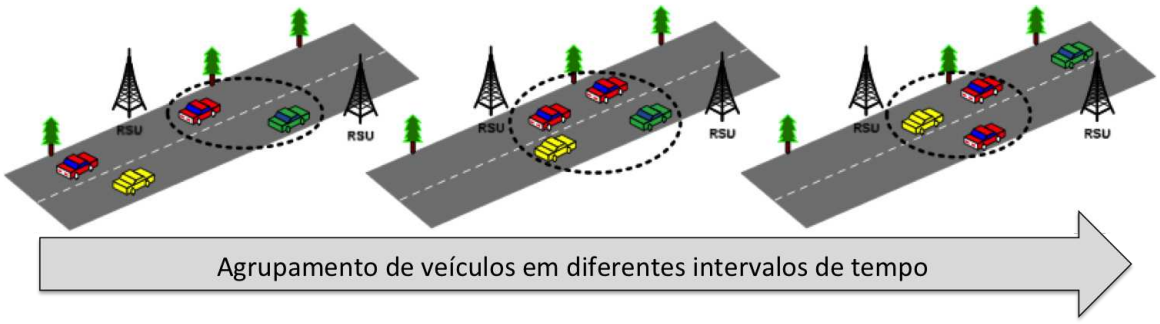


Figura 2.1: Representação de agrupamento de veículos em redes VANETs.

- Processamento de dados em tempo real: devido à dinamicidade de alteração de estado dos nós e às aplicações que podem pôr a vida de motoristas em risco, as redes VANETs impõem restrições quanto ao tempo de processamento das mensagens recebidas pelos veículos, que devem ser processadas em poucos milisegundos;

- Valor do Dado Vs. Distância: dados e eventos são importantes apenas para uma região específica. Como exemplo, a divulgação de um evento de colisão entre dois

veículos será relevante apenas para outros veículos em um raio de poucos quilômetros (Figura 2.2).

Figura 2.2: Informações sobre eventos são relevantes apenas para uma dada região.

2.2 Arquitetura das Redes Veiculares

A arquitetura das redes veiculares define a forma como os nós se organizam e se comunicam e é ilustrada na Figura 1.1. Atualmente, existem duas arquiteturas principais: *ad hoc* puro e infraestruturada/híbrida [2]. Na arquitetura *ad hoc*, os veículos se comunicam diretamente entre si sem qualquer entidade centralizada, provendo roteamento de mensagens quando a distância entre os veículos transmissor e receptor for maior que o alcance do sinal transmitido. A comunicação entre veículos é comumente chamada de comunicação V2V (*Vehicle-to-Vehicle*).

Embora não seja necessária uma infraestrutura intermediária para comunicação entre os veículos, a abordagem puramente *ad hoc* tem como principal desvantagem a conectividade da rede que depende da densidade e do padrão de mobilidade dos veículos. Para evitar problemas de conectividade, a arquitetura infraestruturada/híbrida inclui nós estáticos, denominados Unidades de Acostamento, ou simplesmente RSU (do inglês *Roadsite Units*) ao longo das margens das ruas e estradas, servindo como nós intermediários para comunicação. A vantagem desta abordagem é o aumento da conectividade entre os nós em rodovias com baixa densidade e a possibilidade da comunicação com outras redes, como por exemplo, a internet. Entretanto, a conectividade da rede é apenas garantida mediante um número grande de elementos fixos, o que pode elevar os custos da rede. O modo infraestruturado tem como sinônimo o termo V2I (*Vehicle-to-Infrastructure*).

2.3 Padrões de Redes Veiculares

Os primeiros esforços para a definição de padrões para redes VANETs foram realizados nos EUA em 1999. A Comissão Federal de Comunicações dos EUA (*U.S. Federal Communication Commission*) reservou para o país um espectro de 75 MHz da largura de banda

na faixa de 5,9 GHz (5,850-5,925 GHz) para aplicações DSRC (*Dedicated Short-Range Communications*) focada exclusivamente em comunicações V2V e V2I [80]. A alocação de canais DSRC está ilustrada na Figura 2.3. O espectro reservado está organizado em 7 canais de 10 MHz, sendo 1 canal de controle e 6 canais de serviços. O canal de controle é reservado para a transmissão de mensagens periódicas de alta prioridade, denominada *beacon* [80] (ver Seção 2.3.1) e mensagens de segurança no transporte, tais como sistemas de anticolisão. Por outro lado, os canais de serviço são utilizados para transmissão de conteúdos de áudio, vídeo e dados de aplicações.

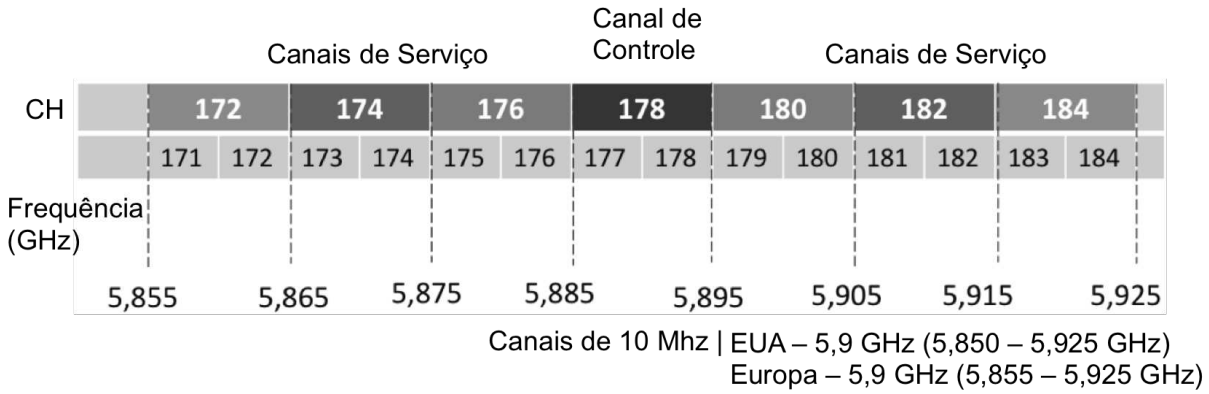


Figura 2.3: Representação de alocação de frequências de canais para aplicações DSRC no padrão 802.11p (Adaptada de [81]).

2.3.1 A Arquitetura WAVE

A fim de prover mecanismos escaláveis e eficientes, bem como adequar futuras soluções de acordo com as restrições e necessidades das redes VANETs, fez-se necessário aplicar mudanças nas tecnologias de redes sem fio, em especial no padrão 802.11. O padrão que está sendo especificado é definido como IEEE 802.11p WAVE (*Wireless Access in Vehicular Environment*) [82]. Estão definidos no padrão IEEE 802.11p as camadas físicas e de controle de acesso ao meio (MAC) para redes veiculares. Entretanto, a arquitetura WAVE não está restrita apenas a estas camadas, como ilustrada na Figura 2.4. Estão definidas nos padrões da família IEEE 1609 outras camadas da pilha de protocolos, incluindo uma camada de rede alternativa à camada IP, características de segurança para aplicações DSRC e operação em múltiplos canais de comunicação.

O padrão WAVE está definido em seis documentos, a saber: IEEE P1609.1, IEEE P1609.2, IEEE P1609.3, IEEE P1609.4, IEEE 802.11 e IEEE 802.11p. Estão descritos nos documentos todos os requisitos para proporcionar comunicações V2V e V2I. O objetivo é prover interoperabilidade entre diferentes fabricantes de automóveis e soluções a serem executadas nos ambientes veiculares. A seguir são descritos os principais aspectos

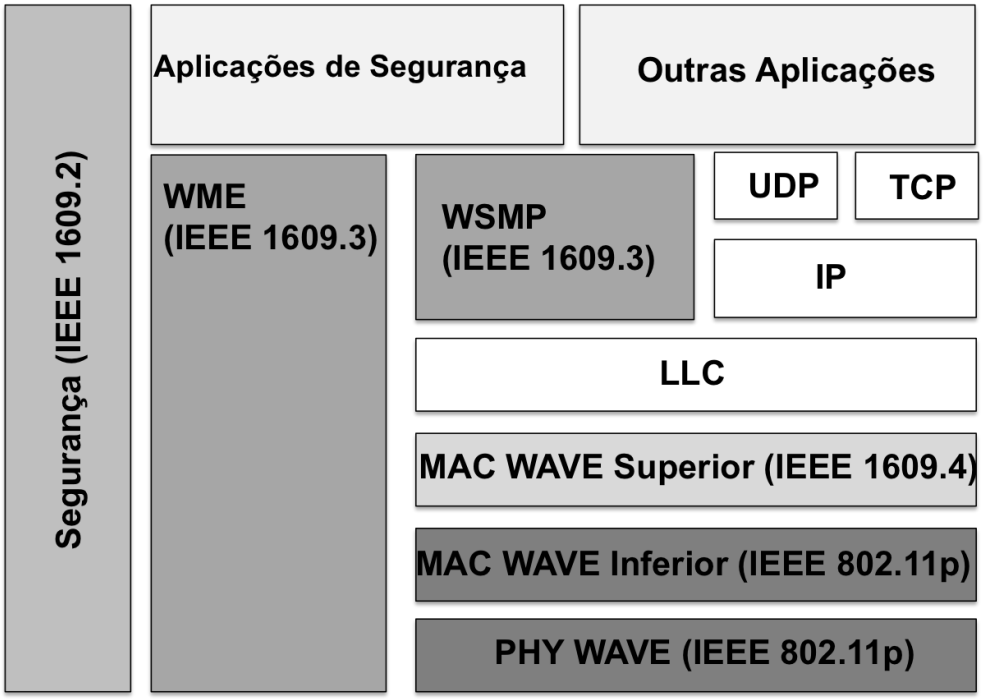


Figura 2.4: Pilha de Protocolos WAVE (Adaptada de [83]).

presentes em cada especificação.

- IEEE P1609.1: são definidos os serviços e interfaces da aplicação de Gerenciamento de Recursos da arquitetura WAVE;
- IEEE P1609.2: são definidos os formatos e processamento seguros de mensagens. Para tal, são delineados aspectos como Infraestrutura de Chaves Públicas (PKI) e certificação digital. Nesse contexto, Autoridades de Certificação são propostas, cujo objetivo é autorizar/desautorizar outras entidades da rede através da emissão ou revogação de certificados digitais. Tais certificados têm como base algoritmos assimétricos, mais especificamente o modelo de Curvas Elípticas (ECDSA) [69]. Além disso, é especificado um conjunto de veículos de segurança pública, denominado OBUs (do inglês, *On-Board Unit*) de Segurança Pública (*Public Safety OBUs* - PSOBUs). As PSOBUs serão embarcados em veículos relacionados à segurança pública, tais como viaturas de polícia e bombeiros;
- IEEE P1609.3: são especificados os serviços de controle de enlace lógico (*Logical Link Control* - LLC), de rede e de transporte, incluindo endereçamento e roteamento. A comunicação WAVE pode utilizar o IPv6 ou mensagens curtas WAVE (*WAVE Short Messages* - WSM), uma alternativa que tem como objetivo proporcionar maior eficiência. O plano de dados definido no padrão 1609.3 consiste em quatro serviços: controle de enlace lógico, o protocolo de rede IPv6, os protocolos de transporte

UDP e TCP, e o protocolo WSMP (*WAVE Short Message Protocol*), que ocupam as camadas de transporte e de rede;

- IEEE P1609.4: são propostas modificações no padrão IEEE 802.11 para a operação em múltiplos canais, uma vez que está definida na arquitetura WAVE a utilização de um canal de controle e múltiplos canais de serviço. Um dispositivo que segue o padrão WAVE deve monitorar o canal de controle à espera de requisições de serviços WAVE que contém o número do canal de serviço a ser utilizado pelo serviço WAVE;

- IEEE 802.11p: O padrão IEEE 802.11p é uma extensão da família de protocolos IEEE 802.11 e baseia-se, principalmente, na extensão IEEE 802.11a, porém, opera na faixa DSRC de 5,9 GHz. Mais detalhes sobre o padrão podem ser encontrados em [81, 84–86].

  A camada física define como os dados são modulados em sinais que são transmitidos em ondas eletromagnéticas. O padrão 802.11 faz uso do esquema de multiplexação por divisão de frequência (OFDM, do inglês *Orthogonal frequency-division multiplexing*), com taxas de transferência entre 3 e 27 Mbps (para canais de 10 MHz). São detalhadas na Tabela 2.1 as taxas de dados, tipos de modulações, e potência mínima recebida de acordo com o padrão IEEE 802.11. Como exemplo, com taxas de transmissão de 3 Mbps, utilizando modulação BPSK e taxas de codificação 1/2 deve ser viável com potência mínima recebida igual a -85 dBm.

Tabela 2.1: Taxas de dados, modulações e potências mínimas recebidas no padrão IEEE 802.11 para canais de 10 MHz.

Taxas (Mbps)	Modulação	Taxa de Codificação	Potência Mínima Recebida (dBm)
3	BPSK	1/2	-85
4,5	BPSK	3/4	-84
6	QPSK	1/2	-82
9	QPSK	3/4	-80
12	16-QAM	1/2	-77
18	16-QAM	3/4	-73
24	64-QAM	2/3	-69
27	64-QAM	3/4	-68

Uma rede VANET pode ser constituída a partir da transmissão de dois tipos de men-

sagens definidos pelo padrão WAVE, a saber: periódicas (*beacon*) e baseadas em eventos (esporádicas) [87, 88]. No primeiro caso, veículos transmitem mensagens periodicamente para informar dados como velocidade, direção e posição atuais. Tais mensagens são transmitidas a partir do modelo de único salto (*one-hop*) e para todos os nós no raio de transmissão Rt do veículo transmissor.

Por outro lado, mensagens esporádicas têm como objetivo alertar veículos sobre possíveis situações de perigo, tais como pistas escorregadias, frenagens brusca de veículos à frente, obstáculos nas vias - tais como veículos parados -, notificação de limites de velocidade nas vias, entre outras. Tais mensagens são consideradas de alta prioridade e devem ser transmitidas considerando com baixa latência e alta confiabilidade.

Formalmente, uma rede VANET constituída por mensagens periódicas pode ser representada pela tupla $G = \langle V, E \rangle$ em que V representa o conjunto de nós (veículos e RSUs) no espaço euclidiano e $E \subseteq V^2$. Todos os links de comunicação diretos entre pares de nós n_i e n_j $(i \neq j)$, representado por $edge(n_i, n_j)$ são constituídos a partir da Definição 1:

Definição 1. *Dada uma rede $G = \langle V, E \rangle$, existirá um par de nós comunicantes $(n_i, n_j) \in E$ se, e somente se, a distância euclidiana entre as posições de n_i e n_j, representadas por POS_{n_i} e POS_{n_j} é menor que o raio de transmissão Rt dos rádios de n_i e n_j, isto é, $E = \{(n_i, n_j) \in V^2 | (POS_{n_i} - POS_{n_j}) \leq Rt\}$.*

Do ponto de vista de um nó n_c, uma rede VANET constituída a partir da Definição 1 pode ser estendida a partir da Definição 2.

Definição 2. *Do ponto de vista de um veículo arbitrário n_c, uma rede G_c é constituída por todos os nós $n_j \in V$ que satisfazem a condição que constituem o conjunto E. Desta forma, E_c é o conjunto de pares de nós comunicantes com o nó n_c, formando a rede $G_c = \langle V, E_c \rangle$.*

Devido à velocidade dos veículos, a periodicidade de transmissão de mensagens *beacon* deve variar entre 100 *ms* e 300 *ms*, dependendo de parâmetros de qualidade de serviço (QoS) desejados. Nesse contexto, Nguyen et al [89] observaram que o envio demasiado de mensagens periódicas em redes com alta densidade de veículos pode implicar em maiores atrasos e baixa recepção de mensagens.

Nesta mesma linha de raciocínio, Sommer et. al. [90] também avaliaram que a periodicidade de envio de mensagens dependerá da qualidade do canal de transmissão, a qual considera parâmetros como o número de nós no raio de transmissão, o número de colisões de pacotes que ocorreram, e o valor da relação sinal-ruído (SNR, do inglês, *Signal to Noise Ratio*).

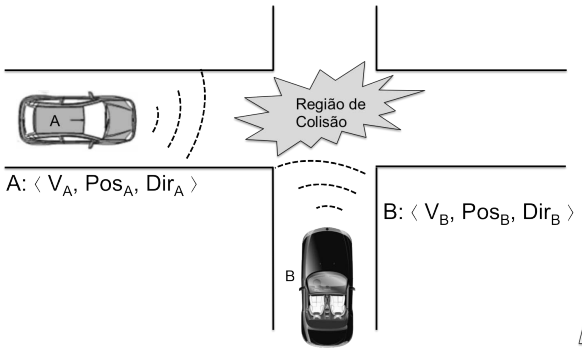
Nas seções a seguir são apresentados potenciais cenários de aplicação e projetos existentes para redes veiculares que têm como base o uso de mensagens periódicas, bem como

de mensagens baseadas em eventos.

2.4 Aplicações e Projetos

Podem-se vislumbrar três potenciais categorias de aplicações voltadas para ambientes veiculares, a saber: segurança no trânsito, entretenimento, e assistência ao motorista.

As aplicações para segurança no trânsito são focadas em situações emergenciais e preventivas, visando informar rapidamente os condutores sobre eventos de perigo. Nesta classe de aplicação destacam-se a divulgação de informações sobre acidentes, sobre potenciais perigos de colisão entre veículos e sobre condições adversas de ruas e estradas. Estão ilustrados na Figura 2.5 os potenciais cenários de anticolisão (*collision avoidance*) para redes VANETs. No geral, a divulgação é limitada aos veículos próximos aos eventos de ocorrência. Essa classe de aplicação impõe baixa latência e alta confiabilidade para as mensagens transmitidas, e devem ser robustas à inserção de mensagens falsas e mensagens conflitantes. Nesse contexto, há diversas pesquisas sendo desenvolvidas, tais como abordagens colaborativas para evitar colisões entre veículos e alerta de possíveis colisões em mudanças de faixas [91–93] e cruzamentos entre vias.



(a) Mensagens periódicas podem evitar colisões em cruzamentos.

(b) Evento de frenagem brusca de B permite que D reaja ao evento antes de C também parar.

(c) Mensagens periódicas podem alertar perigos em ultrapassagens.

(d) Mecanismos de predição de percurso podem evitar colisões em mudanças de faixa devido ao "ponto cego" (*blind spot*).

Figura 2.5: Representação de potenciais cenários de segurança no trânsito propostos para ambientes veiculares.

As aplicações de entretenimento são baseadas em aplicações existentes na internet, porém, adaptadas às restrições dos ambientes veiculares. Nesta classe destacam-se os

serviços de mensagens instantâneas e os serviços de compartilhamento de conteúdos multimídia, tais como áudio e vídeo [94]. De forma similar às aplicações típicas da internet para compartilhamento de conteúdos baseados em sistemas P2P, vislumbram-se em ambientes veiculares os serviços denominados carro a carro (*Car-to-Car* - C2C) [95], permitindo que veículos troquem partes de arquivos entre si da mesma forma como ocorre no protocolo BitTorrent [96] usado na Internet. Nesse contexto, projetos como SPAWN [97], CarTorrent [98] e CodeTerrent [99] foram desenvolvidos para ambientes veiculares, uma vez que o protocolo BitTorrent não se mostrou adequado para esses ambientes [98].

Por fim, as aplicações de assistência ao motorista visam dar suporte aos motoristas na busca por informações disponíveis nas vias e estradas. Nessa classe destacam-se aplicações de alertas de vagas em estacionamentos, pagamento automático de pedágios, controle de tráfego, entre outras. Como exemplo, um estudo realizado em um distrito da cidade de Munique, na Alemanha, revela que a busca por vagas nos estacionamentos causa 44% de todo tráfego [100], o que torna este tipo de serviço foco de diversos trabalhos [100–104].

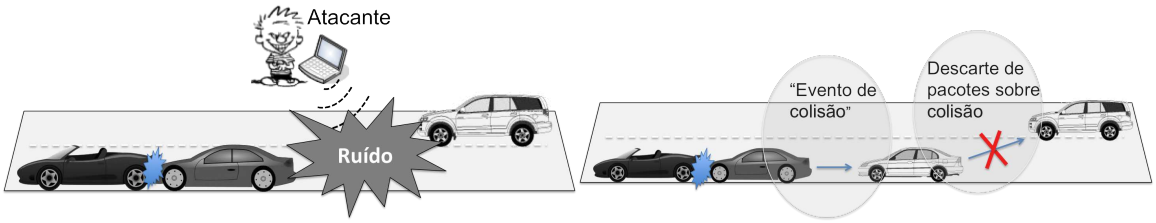
À luz das características e restrições dos ambientes que envolvem as redes veiculares, diversas pesquisas têm sido propostas pela comunidade científica. Do ponto de vista da pilha de protocolos de rede, há abordagens para modelagem de canais no meio físico [105–108], alocação e gerenciamento de canais [109–111], protocolos de controle de acesso ao meio [112–115], protocolos de roteamento geográfico [116–120], mudanças nos modelos de controle de congestionamento [121–124], protocolos de endereçamento [125,126], entre outras. No nível de aplicação, as redes VANETs implicam em diversos desafios, com propostas existentes para transmissão de conteúdo multimídia [127–133], predição de possíveis rotas futuras para veículos [73–75], protocolos de descoberta de serviços [134], disseminação de anúncios e propagandas [135, 136], disseminação de informações [35, 137], integração de redes VANETs com infraestruturas de computação na nuvem [138] e geradores de mobilidade de veículos para dar suporte a simulações experimentais para ambientes VANETs [139–145]. No contexto deste trabalho, a segurança em redes VANETs também tem sido foco de uma gama de pesquisas [2, 21, 146–153], uma vez que diversos tipos de ataques maliciosos podem pôr em risco a vida de motoristas e passageiros. Nas seções a seguir, são apresentados conceitos introdutórios sobre segurança em redes VANETs.

2.5 Segurança em Redes VANETs

As redes VANETs são suscetíveis a diversos tipos de ataques originados por usuários ou nós mal-intencionados. Grande parte desses ataques são conhecidos em outras redes de computadores, porém, o que torna a segurança das redes VANETs como um dos aspectos

mais críticos de pesquisa são as possíveis consequências em caso de sucesso de um ataque malicioso, os quais podem pôr em risco a vida de motoristas e pedestres.

Por exemplo, ataques de negação de serviço (DoS) [154] através de interferências do sinal de rádio (*Wireless Signal Jamming*) [155] ou através dos descartes de pacotes em transmissões *multi-hop* (buraco negro - *Black Hole*) [156, 157], como ilustrados na Figura 2.6, poderão impedir que veículos recebam informações sobre eventos importantes ocorridos nas estradas e impossibilitar o funcionamento correto dos sistemas em execução nessas redes, pondo em risco a vida de motoristas e pedestres.



(a) Interferência do sinal de rádio. (b) Buraco negro através de descartes de pacotes.

Figura 2.6: Cenários de ataques de negação de serviço (DoS) em redes VANETs podem impedir o recebimento de informações sobre eventos importantes, tal como colisões entre veículos à frente (Adaptadas de [158]).

Ataques em VANETs podem variar de um simples monitoramento das mensagens trocadas entre veículos, até ataques mais sofisticados, como no caso de um conjunto de diversos veículos maliciosos. Aspectos como autenticação, integridade, não-repúdio, anonimato e confidencialidade são de suma importância para garantir a segurança das redes VANETs.

Os potenciais ataques realizados em redes VANETs são basicamente contra os aspectos de autenticação, disponibilidade de serviços e confidencialidade, como ilustrado na Figura 2.7. A partir dessa categorização, considera-se o seguinte axioma.

Axioma 1. *Usuários em redes VANETs poderão ser maliciosos*[1] *quando não se comportam, de forma intencional, de acordo com as especificações de cada serviço disponível na rede, ou possuem equipamentos instalados em seus veículos que não funcionam de acordo com os requisitos para os quais foram projetos, tais como sensores de posicionamento.*

A presença de veículos maliciosos na rede pode degradar a qualidade das aplicações ou até mesmo impedir a efetiva execução de serviços de rede, o que pode trazer inúmeros riscos aos usuários, tais como motoristas e pedestres. Desta forma, é de suma importância que tais veículos sejam detectados, identificados e excluídos da rede. Tal procedimento é definido pelo axioma a seguir.

[1]Os termos "usuário malicioso" e "veículo malicioso" serão utilizados de forma indistinguível.

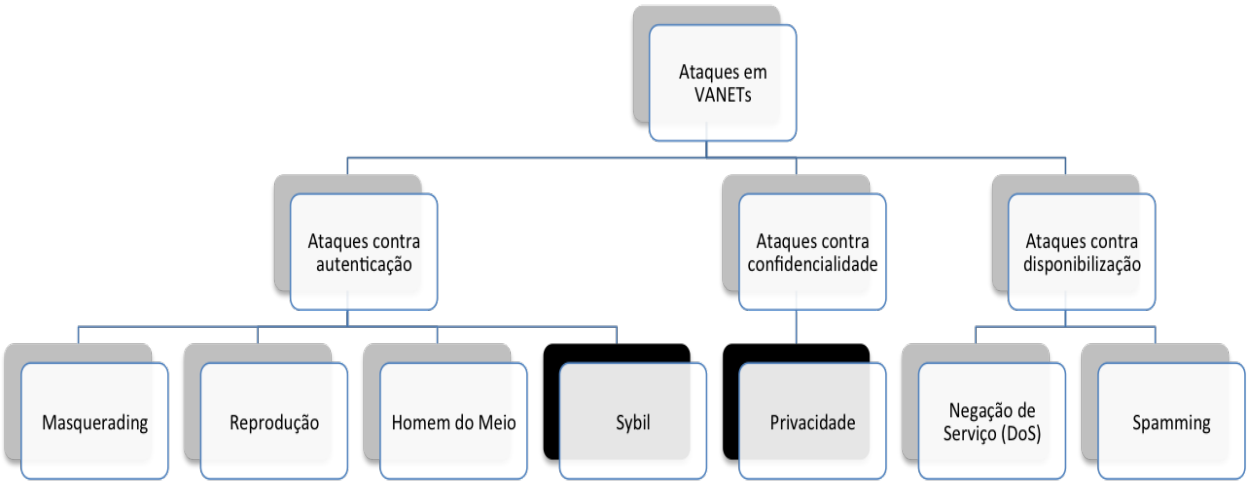


Figura 2.7: Categorias de ataques em redes VANETs.

Axioma 2. *Veículos maliciosos devem ser detectados, identificados e excluídos da rede, buscando minimizar as consequências e os impactos sob os serviços de rede e os potenciais perigos contra a integridade física dos demais usuários.*

Raya et al [8] classificam os tipos de usuários maliciosos em redes VANETs de acordo com três aspectos, a saber: seu estado de adesão à rede, a sua motivação e o seu método de ataque. O estado de adesão define se o atacante é *interno*, ou seja, autêntico na rede, ou *intruso*. Um atacante *interno* comunica-se com outros usuários através do envio de mensagens autenticadas, ao passo que atacantes *intrusos* são mais limitados e não podem gerar mensagens autênticas, restringindo-os a certos tipos de ataques. O aspecto motivacional pode ser classificado como *racional* ou *malicioso*. No primeiro caso, o atacante *racional* visa obter benefícios, ao passo que um atacante *malicioso* tem como objetivo perturbar os serviços da rede. Por fim, um atacante pode utilizar um método de ataque *ativo* ou *passivo*. Enquanto um atacante *ativo* pode criar novas mensagens e modificar mensagens durante transmissão, um nó *passivo* limita-se apenas à escuta do canal de comunicação.

Estão descritos nas seções a seguir cada tipo de ataque o qual está estritamente relacionada a este trabalho de pesquisa. São apresentadas as principais consequências em redes VANETs e os tipos de atacantes interessados conforme a classificação de Raya. Maior ênfase é dada para os ataques do tipo *sybil* e contra o anonimato dos usuários em redes VANETs, ambos focos de estudo deste trabalho.

2.5.1 Ataques contra Autenticação

O processo de autenticação de veículos em redes VANETs tem como objetivo garantir a autenticidade de mensagens oriundas de veículos legítimos para a rede e impedir que outros nós enviem mensagens falsas ou alteradas, utilizem identidades falsas, reproduzam mensagens antigas etc. De acordo com Riley et al [159], os tipos de ataques contra a autenticação podem ser classificados como:

- *Personificação (Masquerading)*: esse tipo de ataque é realizado a partir do uso de identidades falsas ou roubadas. Como exemplo, um veículo pode enviar mensagens periódicas para rede informando que é um veículo de emergência (ex.: ambulância) a fim de obter acesso livre na rodovia ou estrada. Esse ataque pode ser realizado por usuários classificados como intruso ou interno, racional e ativo ou passivo;

- Reprodução: em um ataque de reprodução [160], mensagens autênticas originadas por nós autênticos são armazenadas por um atacante para posteriormente serem reproduzidas na rede. Um possível cenário é um veículo reproduzir mensagens periódicas antigas, obtidas em uma região e pertencentes a outros veículos. Esse tipo de ataque pode ser realizado por usuários classificados como interno ou intruso, racional e passivo;

- Homem do Meio: Em um ataque de Homem do Meio (MITM, do inglês *man-in-the-middle*), um usuário malicioso M monitora a comunicação entre duas entidades A e B a fim de alterar (adicionar, remover etc.) os dados nas mensagens trafegadas. Objetiva-se fazer com que A e B recebam mensagens modificadas por M sem que ambos percebam;

- *Sybil*: em um ataque *sybil*, múltiplas identidades são utilizadas ao mesmo tempo para dar a ilusão que há múltiplos veículos diferentes na região. O ataque pode ocorrer através do envio de mensagens periódicas ou através de mensagens esporádicas. Em ambos os casos, múltiplas identidades autênticas são utilizadas para o envio das mensagens. Esse tipo de ataque pode ser executado por usuários internos, racional ou malicioso, e passivo. Tal categoria de ataque é o principal foco de pesquisa deste trabalho e é discutido com mais detalhes na Seção 2.5.3.

Há ainda outros potenciais ataques contra autenticação em redes VANETs, incluindo GPS *Spoofing* [161] e tunelamento [8, 162].

2.5.2 Ataques contra Confidencialidade: anonimato em redes VANETs

Em segurança da informação, a confidencialidade tem como objetivo impedir que entidades não autorizadas tenham acesso ao conteúdo original das mensagens trocadas entre as entidades comunicantes, garantindo apenas que a origem e o destino possuam conhecimentos do conteúdo original. Para tal, algoritmos de criptografia são utilizados para embaralhar as mensagens e dificultar a leitura do conteúdo. No contexto das redes VANETs, a preocupação com a confidencialidade está além do acesso não autorizado às mensagens, e inclui também o aspecto da possível violação do anonimato dos usuários (ex.: motoristas).

Em redes VANETs, mensagens trafegadas para uso de propósito geral, tais como as mensagens periódicas para aplicações de segurança no trânsito e predição de percursos, são enviadas à rede de forma autêntica, porém, sem suporte a confidencialidade. Ou seja, uma vez que tais mensagens são utilizadas para propósito geral, permite-se que quaisquer entidades conectadas na rede possam monitorar o canal de comunicação e obter os dados presentes nas mensagens. Ademais, permitir que apenas certas entidades (ex.: veículos específicos) fossem capazes de ter acesso aos dados contidos em mensagens periódicas exigiria mecanismos de negociação de chaves de criptografia, inviável para certos cenários devido à grande dinamicidade de entrada e saída de (novos) veículos na rede. Desta forma, não é viável garantir confidencialidade do conteúdo de tais mensagens contra entidades não autorizadas (ex.: atacantes passivos), o que pode facilitar o monitoramento de rotas de veículos e, consequentemente, a possível violação do anonimato dos motoristas.

A principal motivação do monitoramento das mensagens periódicas e, como consequência, a possível violação do anonimato dos motoristas reside especialmente em fatores comerciais. Na Web, por exemplo, empresas de diversos seguimentos realizam investimentos maciços para monitorar as atividades e o comportamento dos usuários a fim de maximizar a probabilidade de oferecer serviços com maior relevância. Essa motivação também deverá ser considerada em redes veiculares. Outro fator determinante para assegurar o anonimato dos veículos está na integridade física das pessoas envolvidas (ex.: possíveis ações de sequestros), uma vez que usuários maliciosos podem construir um perfil de rotas de um veículo específico a fim de encontrar um padrão de mobilidade.

Nesta perspectiva, em [13] pesquisadores analisaram diferentes formas de distribuição de identidades para veículos a fim de analisar o nível de anonimato e, em contrapartida, o impacto em requisitos de segurança, tais como revogação de certificados digitais de veículos maliciosos e não-repúdio. As três potenciais formas de distribuição de identidades analisadas são descritas a seguir:

1. **Todos os veículos registrados no sistema compartilham as mesmas identidades**: este é o modelo de distribuição de identidades mais simples para garantir total anonimato, em contrapartida, sob a ótica dos requisitos de segurança, é o modelo que traz os maiores problemas. A identidade pode ser representada por chaves simétricas, uma vez que o compartilhamento dessa chave, nesse contexto, é simples. Por outro lado, uma vez detectado um veículo mal-comportado, não será possível identificá-lo unicamente no sistema, o que também impedirá sua exclusão através da revogação de chaves;

2. **Grupos de veículos compartilham uma mesma identidade**: essa abordagem proporciona anonimato para os grupos, porém, o nível de anonimato dependerá do tamanho do grupo de veículos que compartilham as mesmas identidades. Resultados da análise mostram que a identificação e exclusão de veículos maliciosos podem ser demoradas e comprometer uma quantidade substancial de veículos não maliciosos, a depender do tamanho dos grupos. Ou seja, para um grupo com um número de veículos maior (maior anonimato), a exclusão de um veículo malicioso pertencente a esse grupo poderá comprometer os demais veículos do grupo;

3. **Cada veículo armazena um conjunto de identidades (pseudônimos) e nenhum veículo compartilha nenhuma identidade**: além de permitir o controle individual do anonimato de cada veículo; veículos maliciosos serão revogados sem afetar os demais veículos no sistema. Dentre as três abordagens avaliadas, essa se apresenta como a mais viável de acordo com as métricas avaliadas. Por outro lado, os autores ainda defendem que essa abordagem identifica unicamente um veículo do ponto de vista da autoridade certificadora, a qual também poderá violar o anonimato dos usuários. Entretanto, tal argumento é excessivo, uma vez que a responsabilidade da autoridade certificadora é justamente gerenciar e organizar a autenticidade dos veículos, papel similar a outros serviços tradicionais e consolidados, tais como sistemas bancários e de telefonia, os quais armazenam dados pessoais como transações financeiras e ligações telefônicas.

Dentro da perspectiva de redes VANETs, é importante enfatizar que uma identidade é representada por um certificado digital. Desta forma, com base na análise realizada por Haas et al [13], verificou-se que o uso de múltiplas identidades para cada veículo é a mais adequada sob a ótica do controle de anonimato dos usuários e, principalmente, observando dentro da perspectiva da revogação de certificados digitais. Como consequência desta abordagem, o uso de diferentes identidades no nível de aplicação também deve refletir em mudanças de identidades (neste caso, endereços) em todos os níveis da camada de rede, tais como endereços IP e físico (MAC), como proposto por Fonseca *et al* [163]. Entretanto,

o intervalo de tempo mínimo/máximo que uma identidade deve ser utilizada, bem como quando a troca de identidades deve ser realizada ainda são pontos a serem definidos.

A primeira proposta remete ao trabalho de Raya [8], onde o tempo considerado para mudança de identidade ocorre com base na distância entre dois potenciais pontos de violação de anonimato e a troca das identidades ocorre antes do segundo ponto. Neste caso, a troca de identidade ocorre de forma arbitrária para cada veículo, ou seja, cada nó realiza a troca de identidades independentemente que outros nós o façam. No entanto, uma análise apresentada em [164] detalha que tal abordagem facilita o monitoramento de troca de identidades e, consequentemente, a associação de diferentes identidades para o mesmo veículo, um procedimento denominado *vinculação* ou *associação* (*linkability*) [12].

Desta forma, diversos trabalhos foram propostos com o objetivo de dificultar a associação das múltiplas identidades de um veículo. As abordagens propostas partem do conceito denominado conjunto anonimato (*Anonimity Set*) ou *k-anonymity* [67,165] e zonas mistas (*mix-zones*) [166]. O conceito de conjunto anonimato é um modelo em que um elemento e, de um conjunto de elementos E que compartilham as mesmas propriedades, não pode ser identificável por pelo menos *k-1* elementos do conjunto, para $k = |E|$. O conjunto E é denominado *conjunto anonimato*. Como exemplo, estão ilustrados na Figura 2.8 dois conjuntos anonimatos, o conjunto dos potenciais remetentes, e o conjunto dos potenciais destinatários. Ou seja, através do monitoramento das mensagens trafegadas, não deve ser possível associar uma mensagem específica a um remetente ou um destinatário específico. Dentro do contexto do controle de anonimato em sistemas de geolocalização, o conceito de zonas mistas visa formar conjuntos anonimatos em regiões geográficas, permitindo que entidades dentro daquela região não sejam unicamente identificáveis.

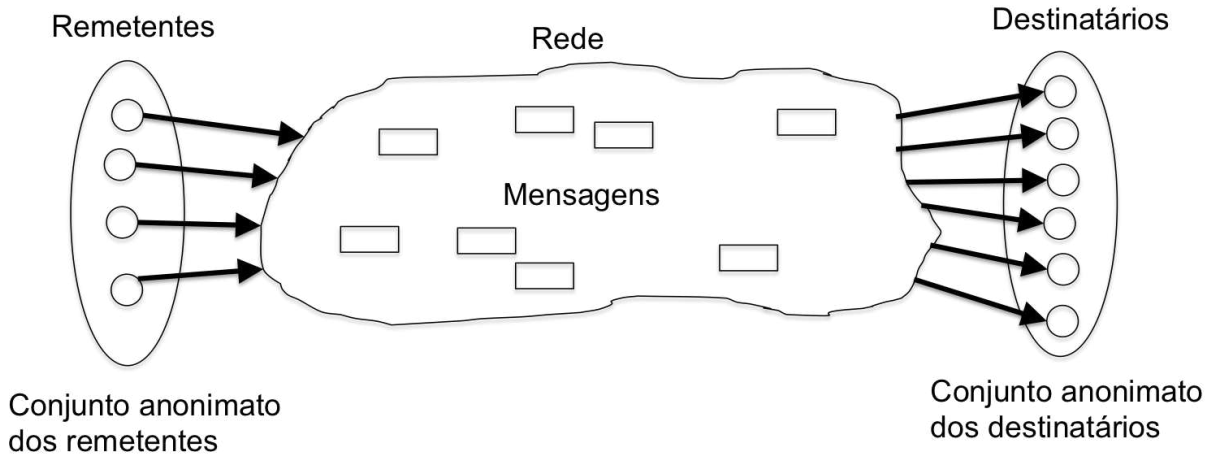


Figura 2.8: Mensagens transmitidas e recebidas não podem ser associadas ao nó transmissor pertencente ao conjunto anonimato dos remetentes e/ou ao nó receptor pertencente ao conjunto anonimato dos destinatários (Adaptada de [12]).

Desta forma, existem na literatura abordagens que têm como base o conceito de conjunto anonimato e zonas mistas para troca de identidades. Tais abordagens diferem apenas em como os conjuntos anonimatos são constituídos e o momento de troca de identidades. Como exemplo, as intersecções entre vias ou regiões onde há grande aglomerado de veículos, tais como estacionamentos, podem ser consideradas zonas mistas para troca de identidades [167–169]. Nesse caso, todos os veículos devem alterar suas identidades ao mesmo tempo. Além disso, a troca de identidades dos veículos pertencentes a uma mesma zona mista pode ocorrer após um período de silêncio (*silent period*), onde veículos interrompem a transmissão de mensagens periódicas, alteram as identidades, e voltam a transmitir [164, 170].

2.5.3 Definição de Ataques *Sybil*

Na maioria dos sistemas de computação, identidades são utilizadas como uma abstração para facilitar a identificação de uma entidade. Em um ataque *sybil*, um nó pode utilizar múltiplas identidades para construir uma fração de nós inexistentes, objetivando inúmeros ganhos e causando impactos na execução de diversos serviços da rede. De modo geral, sistemas que possuem um controle fraco do esquema de criação e associação de identidades, e não oferecem uma infraestrutura que assegure a unicidade da relação entre entidades e identidades, são suscetíveis a ataques *sybil* [72]. Como definido em [43], um nó que usa múltiplas identidades para realizar um ataque *sybil* é denominado *nó malicioso sybil*, ao passo que as múltiplas identidades são chamadas de *nós sybil*.

Como detalhado por Douceur [14] e delineado nas seções a seguir, em diferentes aplicações de redes, tais como sistemas P2P e sistemas de armazenamento distribuído, um ataque *sybil* pode ocorrer através do uso de múltiplas identidades de forma não simultânea, ou seja, em que cada identidade do nó *sybil* é utilizada por vez. Entretanto, como discutido na seção anterior, o uso de múltiplas identidades de forma não simultânea em redes veiculares não necessariamente caracteriza um ataque *sybil*, uma vez que tal abordagem pode ser utilizada para proporcionar anonimato aos nós. Desta forma, a visão inicial de Douceur não se mostra totalmente adequada quando aplicada ao contexto de redes veiculares. Assim, para este trabalho de pesquisa, propõe-se, em linhas gerais, a seguinte definição de ataques *sybil* em redes veiculares:

Definição 3. *Um ataque sybil ocorre quando um veículo (usuário malicioso), com o uso de múltiplas identidades, envia mensagens à rede para disseminar um mesmo evento falso.*

Nesse sentido, é importante ressaltar que, para caracterizar um ataque *sybil*, duas ou mais identidades devem ser utilizadas pelo veículo para declarar a ocorrência de um mesmo evento, sendo este definido da seguinte forma:

Definição 4. *Um evento em redes veiculares descreve um acontecimento numa determinada região geográfica, em um determinado intervalo de tempo, para uma mensagem do tipo periódica ou esporádica.*

Ataques *sybil* podem ser explorados em diversos tipos de rede. A seguir são apresentados potenciais cenários de ataques *sybil* e como esses podem ser explorados em diversas categorias de aplicação.

Ataques *sybil*: Redes Ad Hoc Veiculares

Em redes VANETs, um ataque *sybil* pode ser explorado através de mensagens periódicas ou através de mensagens para disseminar eventos esporádicos, como detalhado na Seção 1.2. Desta forma, tais mensagens podem perturbar serviços de rede, tais como protocolos de roteamento, e permitir que motoristas tomem decisões errôneas devido ao impacto do ataque em algoritmos de detecção de mensagens falsas [171, 172].

Ataques *sybil*: Spam

A distribuição indiscriminada de mensagens eletrônicas (*spam*) é o exemplo mais conhecido de um ataque *sybil*. Nessa categoria de ataque, um usuário gera inúmeras contas de correio eletrônico, na maioria das vezes inativas, com o objetivo de enviar e disseminar mensagens indesejadas, dificultando a ação de filtros que têm como parâmetro de filtragem o endereço do remetente. Atacantes normalmente utilizam ferramentas para automatizar a obtenção de endereços dos destinatários, bem como o envio das mensagens indesejadas, o que pode resultar em um ataque de maiores proporções. A principal motivação para esta categoria de ataque *sybil* é o baixo custo associado à obtenção de uma identidade (endereço eletrônico).

Ataques *sybil*: Redes de Sensores Sem Fio

Rede de Sensores Sem Fio (RSSF) é um tipo especial de *Rede Ad Hoc Sem Fio* (WANET) constituída de sensores (nós) cujo papel é coletar, processar e transmitir dados em tempo real entre si, ou entre pontos de coletas que devem utilizar as informações para tomada de decisões. Como sensores possuem restrições de consumo de energia e de processamento, a utilização de infraestruturas de segurança quase nunca é considerada. Como consequência, as redes de sensores sem fio estão também propícias a ataques *sybil*, como detalhado por *Newsome et al.* [43]. Como exemplo, um nó *sybil* pode acabar com a divisão equitativa dos tempos de acesso ao meio e conseguir um maior tempo de utilização do canal, o que pode ocasionar desde pequenos inconvenientes até graves acidentes.

Ataques *sybil*: Algoritmos de Roteamento

Em algoritmos de roteamento, um atacante pode criar várias identidades se fazendo passar por vários nós legítimos para criar falsos caminhos de roteamento. Ademais, evita-se também que outros nós participem do roteamento e consigam obter créditos por ter feito o roteamento em sistemas guiados por mecanismos de reputação. Por fim, como detalhado em [173], a presença de veículos *sybil* aumenta a porcentagem de perdas de pacotes ocasionada pelo descarte de pacotes e pela formação de *loops* de roteamento.

Ataques *sybil*: Sistemas de Armazenamento Distribuído

Sistemas de Armazenamento Distribuído têm como objetivo replicar dados em diferentes nós para evitar perdas de dados, ou fragmentar os dados para controle de anonimato. Como analisado em [14], se um nó *sybil* for escolhido para receber um dado replicado ou partes desses dados fragmentados, este pode eliminar por completo os dados replicados ou evitar que eles sejam reconstituídos a partir dos fragmentos armazenados. A presença de um nó *sybil* aumenta a probabilidade de que ele receba todas as cópias ou fragmentos dos dados, uma vez que os demais nós visualizam-no como diferentes nós (diferentes identidades).

Ataques *sybil*: Sistemas de Votação On-line

Em sistemas de votação *on-line* cujas identidades são definidas a um baixo custo, um ataque *sybil* pode comprometer os resultados finais de votação [174]. Como exemplo, um dos critérios utilizados pelo motor de busca da *google* (*PageRank*) para classificação de páginas *Web* é a quantidade de *hiperlinks* (votos) que uma página é referenciada [175]. Desta forma, um atacante pode gerar várias páginas contendo *hiperlinks* para uma página específica, melhorando a colocação dessa nos resultados de pesquisas realizadas [71, 176].

Ataques *sybil*: Sistemas de Compartilhamento de Recursos

Sistemas de compartilhamento de recursos em redes P2P também estão sujeitos a ataques *sybil*, os quais podem comprometer mecanismos de incentivo à colaboração e aumentar a probabilidade de um nó *sybil* utilizar os recursos sem contribuir com o sistema ou até evitar que eles sejam compartilhados [174]. A rede de favores (ou NoF, do inglês *Network of Favors*) [177] é um sistema autônomo de reputação cujo objetivo é incentivar o compartilhamento de recursos computacionais ociosos para outros nós da rede, bem como detectar nós caronas na rede (*free-rider*), ou seja, o nó que não doa recurso algum. Em resumo, usuários que são os maiores colaboradores possuem as mais altas pontuações e devem ter maior prioridade para consumir recursos computacionais da comunidade.

Entretanto, se dois ou mais nós possuem as mesmas pontuações, então um sorteio deve ser realizado para decidir quem irá receber o recurso. Um ataque *sybil* pode aumentar a probabilidade de um nó *sybil* ser escolhido para receber o recurso, uma vez que esse terá mais identidades participando do processo de seleção.

2.6 Considerações Finais

Neste capítulo foram apresentados conceitos sobre as Redes Ad Hoc Veiculares (VANETs), descrevendo as características fundamentais para a compreensão do restante do documento. Assim, foram introduzidos conceitos básicos sobre Redes Ad Hoc Veiculares, suas principais características, projetos e cenários que podem ser vislumbrados. Prosseguiu-se com uma breve apresentação sobre os potenciais problemas relativos a alguns tipos de ataques que podem ser explorados em redes veiculares, com maior foco em ataques *sybil* e controle de anonimato. Por fim, foi discutido como os ataques *sybil* são explorados em outras arquiteturas de aplicação.

Capítulo 3

Trabalhos Relacionados

Neste capítulo são apresentadas as abordagens correlatas ao protocolo *ASAP*-V. Assim, inicia-se com uma breve descrição dos parâmetros de comparação entre as abordagens. Tem-se, então, as principais características que devem ser contempladas em protocolos de autenticação e detecção de ataques *sybil* em VANETs. Em seguida são apresentadas as abordagens encontradas na literatura, agrupadas de acordo com o método utilizado para detecção de ataques *sybil*. Por fim, é apresentado um quadro comparativo entre o protocolo *ASAP*-V e as demais abordagens, considerando os parâmetros de comparação.

3.1 Parâmetros de Comparação

A seguir são apresentados os parâmetros utilizados para comparação entre o presente trabalho e as abordagens encontradas na literatura. Desta forma, tem-se as principais características que devem ser contempladas em um protocolo de detecção de ataques *sybil* com suporte ao controle de anonimato em VANETs.

1. **Detecção de ataques *sybil* na região geográfica de ocorrência e no momento do ataque**: é essencial que a detecção de ataques *sybil* seja realizada na região onde o ataque ocorre. Desta forma, é possível que veículos determinem a confiabilidade das mensagens recebidas na região durante um potencial ataque *sybil* e tomem decisões pelo descarte total das mensagens suspeitas;

2. **Independência de uma infraestrutura fixa para detecção de ataques *sybil***: é essencial que o processo de tomada de decisão sobre um potencial ataque *sybil* seja distribuído entre os veículos, independentemente da presença de infraestruturas fixas, tais como C.A ou RSUs, durante um ataque. Desta forma, é possível garantir a detecção de um ataque *sybil* em regiões geográficas sem a presença de tais infraestruturas. Consequentemente, é possível também impedir que ataques *sybil* mais

sofisticados, tais como acompanhados de DoS e DDoS contra essas infraestruturas fixas, comprometam a comunicação entre veículos;

3. **Independência da característica de fluxo de veículos e/ou da topologia das estradas para detecção de ataques *sybil***: como consequência do item anterior, é importante que a detecção de ataques *sybil* ocorra em quaisquer regiões e estruturas de vias e estradas, independentemente de como as vias de acesso são interconectadas;

4. **Resiliência a resultados falso-positivo e falso-negativo**: devido ao *trade-off* entre os requisitos controle de anonimato e detecção de ataques *sybil*, é possível gerar resultados de detecções *falso-positivo*, ou seja, quando um veículo não-*sybil* é detectado como malicioso, bem como resultados de detecções *falso-negativo*, ou seja, quando a presença de um veículo *sybil* não é detectada durante o ataque. Desta forma, é importante que a abordagem para detectar ataques *sybil* minimize ao máximo ambas as formas de resultados;

5. **Detecção de ataques *sybil* oriundos de mensagens periódicas e esporádicas**: pretende-se analisar se a abordagem proporciona detecção de ataques *sybil* quando explorados através de mensagens periódicas e/ou esporádicas. Como detalhado na Seção 2.3.1, ambos os tipos de mensagens diferem quanto à periodicidade de transmissão, o que requer estratégias diferenciadas para detectar um ataque *sybil*;

6. **Autenticação com suporte à não-repúdio**: é essencial que a abordagem permita identificar um veículo malicioso. Desta forma, avalia-se o suporte à não-repúdio de mensagens e como este processo é realizado até que os veículos na rede sejam informados.

3.2 Descrição dos Trabalhos

Nesta seção, faz-se uma análise das abordagens encontradas na literatura, organizadas de acordo com o método de detecção de ataque *sybil*, a saber: método baseado em PKI (*Public Key Infrastructure*); método baseado na relação espaço/tempo; e método baseado no monitoramento de nós vizinhos.

3.2.1 Abordagens Baseadas em PKI

As abordagens baseadas no método de infraestruturas de chaves pública/privada (PKI) têm como objetivo basilar determinar se duas ou mais identidades, representadas por chaves pública/privada, pertencem ao mesmo veículo e atribuir a uma C.A a responsabilidade

de gerenciamento de chaves. O protocolo $ASAP$-V, proposto neste trabalho, faz uso deste método.

P^2DAP

A abordagem proposta por Zhou et al [53, 54], chamada P^2DAP, permite o prévio armazenamento de múltiplas identidades e faz uso de RSUs e C.As para detectar potencial ataque *sybil*. Para tal, a arquitetura proposta agrupa as identidades (ou chaves) em M conjuntos organizados em dois níveis; para o primeiro nível, cada conjunto $m_{1,i} \in M$ associa as identidades com os mesmos x *bits*, os quais são gerados através de colisões de funções de *hash*. Para o segundo nível, cada conjunto $m_{2,j} \in M$ possui apenas as identidades com y *bits* únicos. Desta forma, dois ou mais veículos podem apresentar chaves que apresentam os mesmos x *bits*, mas apenas um único veículo possui chaves com os mesmos y *bits*. Após o processo de definição de identidades, cada veículo v armazena, durante o processo de registro na C.A, um conjunto de k identidades p_v^k.

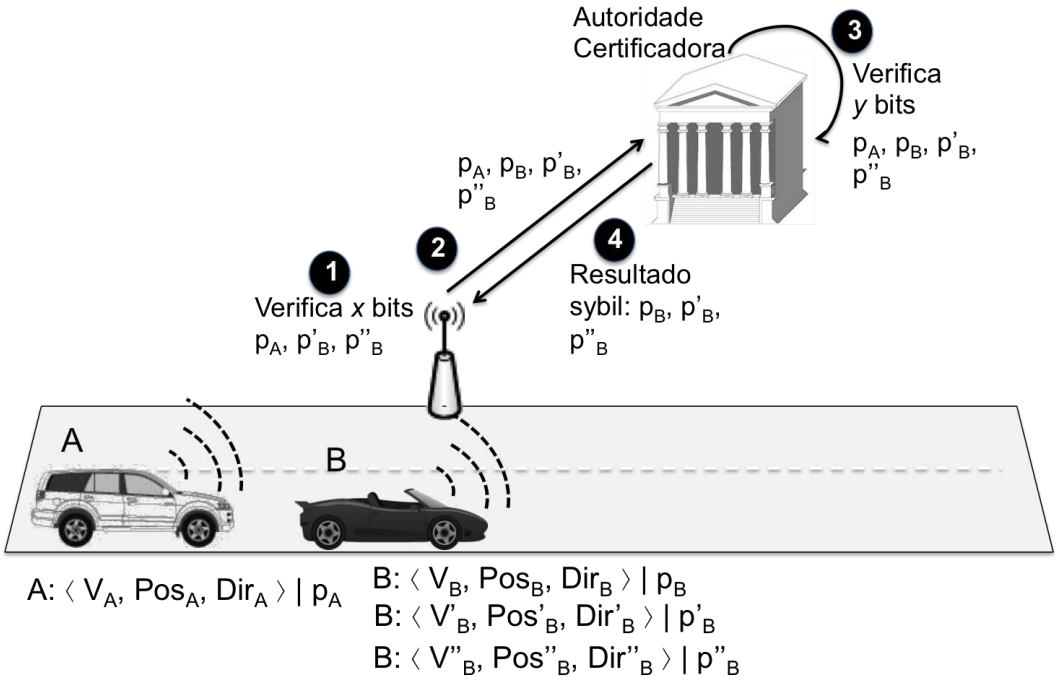


Figura 3.1: Representação de cenário de controle entre anonimato e detecção de ataques *sybil* proposta por Zhou et al [53, 54].

Como ilustrada no cenário da Figura 3.1, a detecção de um ataque *sybil* ocorre da seguinte forma: quaisquer mensagens transmitidas na rede são capturadas pela RSU mais próxima. Na Etapa 1, a RSU determina se as mensagens possuem o mesmo conjunto de x *bits*, a partir de uma chave conhecida apenas pelas RSUs aplicado a um algoritmo de *hash*. Considerando que as identidades $p_A, p_B, p_B^{'}$ e $p_B^{''}$ possuem tais *bits* em comum, na

Etapa 2 a RSU deve repassar tais mensagens para a C.A, uma vez que a RSU não pode determinar se as mensagens são originadas de diferentes veículos, porém, com identidades apresentando os mesmos x *bits*, ou se são oriundas de um mesmo veículo numa tentativa de realizar um ataque *sybil*. Na Etapa 3, a C.A poderá determinar que apenas mensagens com identidades p_B, p'_B e p''_B são originadas do veículo B e, consequentemente, de um ataque *sybil*. Desta forma, o anonimato de um veículo pode ser garantida uma vez que apenas a C.A poderá determinar a identidade real do veículo. Por outro lado, a detecção de um veículo *sybil* pode ser comprometida devido a uma possível não disponibilidade de pelo menos uma RSU. Ademais, resultados mostram que a detecção de um potencial ataque *sybil* poderá ter duração de pelo menos 20 segundos em regiões com grande densidade de veículos, tempo inviável para diversos cenários reais para redes veiculares. Na Seção 5.6 é realizado um comparativo entre o P^2DAP e o $ASAP$-V com relação ao tempo de detecção de ataques *sybil*.

A seguir são apresentadas as características do protocolo P^2DAP com relação aos parâmetros de comparação considerados:

1. **Detecção de ataques *sybil* na região geográfica e no momento de ocorrência do ataque**: a detecção será realizada no local de ataque quando os x *bits* a ser comparados não são iguais. Caso contrário, a detecção não será realizada no local de ataque devido ao atraso de comunicação em cenários onde os y *bits* devem ser comparados na C.A;

2. **Independência de uma infraestrutura fixa para detecção de ataques *sybil***: o protocolo P^2DAP depende exclusivamente da disponibilidade de RSUs e C.As para detectar ataques *sybil*, uma vez que *bits* em comum devem ser verificados. Como consequência, em regiões onde RSUs não estão disponíveis - tanto do ponto de vista físico devido a roubos de equipamentos e fase inicial de instalação de equipamentos, bem como do ponto de vista lógico devido a ataques DoS/DDoS -, veículos não podem determinar a confiabilidade das mensagens, comprometendo mecanismos de tomadas de decisão sobre a veracidade de eventos;

3. **Independência da característica de fluxo de veículos e/ou da topologia das estradas para detecção de ataques *sybil***: a abordagem não depende de um padrão de fluxo de veículos;

4. **Resiliência a resultados falso-positivo e falso-negativo**: a abordagem pode evoluir para detecções falso-positivo quando os primeiros x *bits* de duas ou mais chaves pertencentes a veículos diferentes são avaliados pela mesma RSU. Entretanto, a abordagem elimina quaisquer possibilidades de resultados falso-negativo se houver

uma RSU na região de ataque, uma vez que a C.A garante detectar um veículo *sybil*. Por outro lado, caso uma RSU não esteja disponível na região de ataque, resultados falso-negativo serão possíveis.

5. **Detecção de ataques *sybil* oriundos de mensagens periódicas e esporádicas**: a abordagem permite detectar ataques *sybil* oriundos de ambos os tipos de mensagens.

6. **Autenticação com suporte à não-repúdio**: oferece suporte à não-repúdio a partir dos bits únicos de cada par de chaves utilizada.

A detecção de ataques *sybil* através de RSUs é, evidentemente, dependente da presença de tal infraestrutura. Nesta perspectiva, estudos apontam que a distribuição uniforme das RSUs ao longo das vias poderá reduzir a vazão agregada total da rede veicular na região [55], além de trazer gargalos à rede [26]. Outros trabalhos sugerem a alocação de RSUs apenas nas intersecções entre vias [56, 57], proporcionando maior potencial de disseminação de informações. Desta forma, os modelos de comunicação entre veículos que dependem exclusivamente da disponibilidade de uma RSU não se mostram adequados para serem utilizados em ambientes veiculares reais.

RFID-based

A abordagem proposta por Triki et al [49] faz uso da tecnologia RFID (do inglês *Radio Frequency IDentification*) para permitir a obtenção de identidades temporárias a partir de RSUs disponíveis nas vias. Em linhas gerais, a abordagem propõe a divisão das regiões geográficas em zonas, onde cada zona possui um conjunto de RSUs, e uma das RSUs (chamada RSC, do inglês *Road Side Controller*) sendo responsável pelo gerenciamento de identidades dentro da zona. Uma RSC mantém conexão direta com uma C.A. Como ilustrado na Figura 3.2, as RSUs 1A e 2A formam uma zona, e as RSUs 1B e 2B formam uma segunda zona. As RSUs 2A e 2B executam o papel de RSCs em cada uma das zonas.

O processo de obtenção de identidades permite que um veículo obtenha apenas um único par de chaves (e o respectivo certificado digital) por zona. Desta forma, a partir de um sensor RFID, veículos conectam-se a uma RSU de uma zona e solicita o par de chaves. A RSU em questão repassa a solicitação a RSC responsável pela zona, a qual verificará se o veículo requisitante já possui um par de chaves nesta zona. Caso negativo, a RSC libera a requisição e a RSU retorna um novo par de chaves; caso contrário, a RSC revoga o certificado do par de chaves atual e gera um novo par de chaves para o veículo requisitante, o que permite que um veículo armazene apenas um certificado válido por vez. Esse par de chaves deve ser utilizado em todas as vias que formam a zona. Se um veículo desloca-se de uma zona para uma nova zona, este processo se repete.

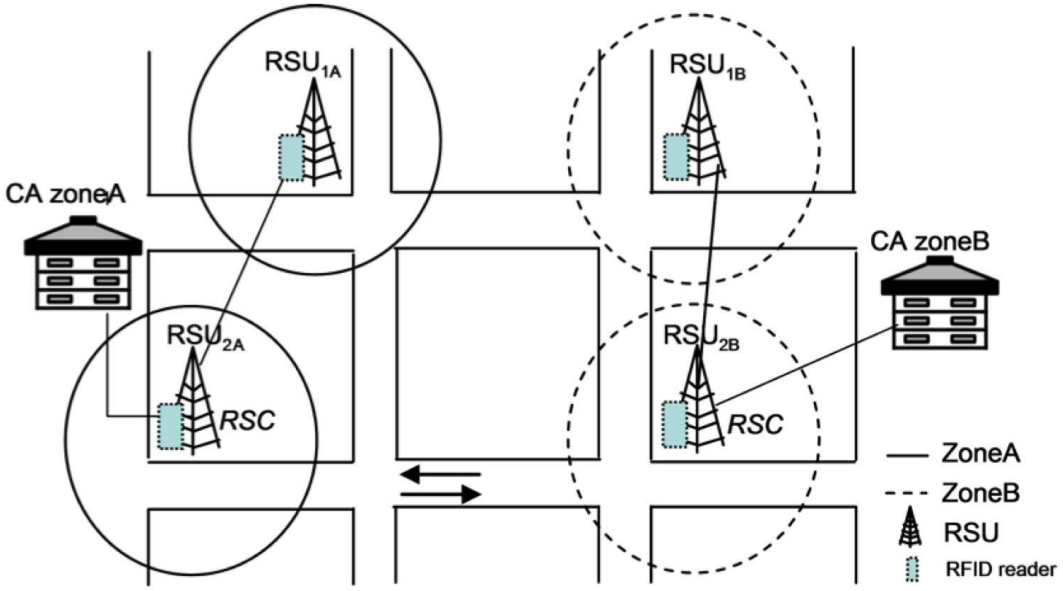


Figura 3.2: Representação de regiões divididas em zonas, onde cada zona possui associado três entidades: um conjunto de RSUs, uma RSC, e uma C.A.

A seguir são apresentados os parâmetros de comparação com relação à abordagem em questão:

1. **Detecção de ataques *sybil* na região geográfica e no momento de ocorrência do ataque**: nem sempre será possível detectar um ataque na região de ocorrência. Ao deslocar-se entre duas diferentes zonas, um veículo poderá obter dois certificados digitais válidos e executar um ataque onde não há formação de zonas. Veículos que recebem mensagens oriundas de um ataque *sybil* só poderão detectar o ataque ao entrar em uma nova zona, o qual deverá repassar para uma RSU as mensagens recebidas fora de uma zona. Como consequência, não será possível determinar a confiabilidade de uma mensagem recebida fora de uma zona;

2. **Independência de uma infraestrutura fixa para detecção de ataques *sybil***: a solução depende das RSUs para detectar ataques *sybil*, uma vez que só é possível detectar ataques dentro de uma zona;

3. **Independência da característica de fluxo de veículos e/ou da topologia das estradas para detecção de ataques *sybil***: a solução não depende da estrutura das estradas ou características de fluxo de veículos;

4. **Resiliência a resultados falso-positivo e falso-negativo**: apenas dentro de zonas. Um ataque *sybil* não será detectado quando ocorrido fora das zonas, uma vez que não há interconexão entre zonas para garantir que um veículo utiliza diferentes chaves obtidas ao trafegar por diferentes zonas;

5. **Detecção de ataques *sybil* oriundos de mensagens periódicas e esporádicas**: a solução é capaz de detectar ataques *sybil* oriundos de ambos os tipos de mensagens.

6. **Autenticação com suporte à não-repúdio**: não oferece suporte à não-repúdio, uma vez que as chaves temporárias não possuem associação um a um com cada veículo. Ademais, adicionar mecanismos de não-repúdio exigiria que a cada nova chave associada a um veículo, a RSC teria que manter um registro por um período indeterminado, visando garantir identificar um veículo malicioso quando um ataque fosse detectado.

3.2.2 Abordagens Baseadas na relação Espaço/Tempo

Uma outra categoria de soluções para prover autenticação, controle de anonimato e detecção de ataques *sybil* busca explorar a relação espaço/tempo [58, 59]. As abordagens baseadas na relação espaço/tempo exploram a dinâmica dos veículos nas vias para detectar ataques *sybil*. Para tal, parte-se da hipótese que dois ou mais veículos não passarão, ao mesmo tempo, em um mesmo ponto da via. Este método pode fazer uso também de infraestruturas de chaves pública para registrar a trajetória de um veículo. Está ilustrada na Figura 3.3 a ideia geral utilizada pelas abordagens. A principal desvantagem desta abordagem reside na falta de mecanismos de não-repúdio no mecanismo de autenticação, uma vez que o histórico de certificados de marcas de tempo deve ser enviado em mensagens transmitidas na rede, o que permitiria a construção de um perfil de rotas de um veículo.

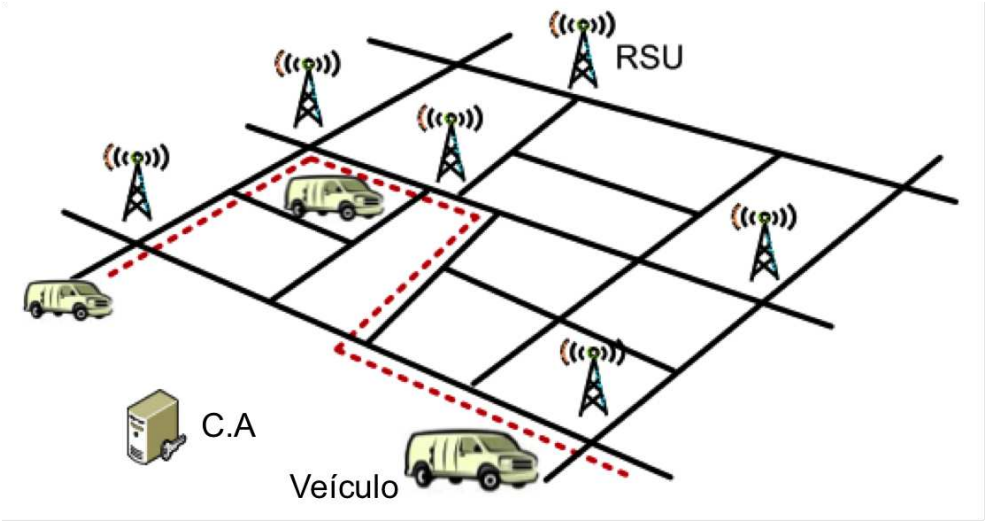


Figura 3.3: As abordagens partem da hipótese que a trajetória de cada veículo pode ser único. RSUs ao longo das vias são responsáveis por autenticar a presença do veículo em uma dada região (Adaptada de [58]).

Séries de Marcas de Tempo

A solução proposta por Park et al [60], denominada *Timestamp Series*, parte da hipótese que dois ou mais veículos não enviarão requisições para uma mesma RSU ao mesmo tempo, considerando que o deslocamento de cada veículo nas rodovias é distinto de qualquer outro veículo. Desta forma, cada veículo gera um par de chaves pública/privada (k_i^+/k_i^-) e solicita a uma RSU_i um certificado digital de marca de tempo ($Cert\_T_i$) para este par de chaves. Como ilustrado na Figura 3.4, a cada nova RSU na qual o veículo virá a transitar no raio de transmissão, uma nova chave pública/privada e uma nova requisição de marcas de tempo devem ser geradas, apresentando-se todos os certificados de marcas de tempo anteriormente obtidos $Cert\_T_{i-1}, Cert\_T_{i-2}, ..., Cert\_T_{i-n}$ como abordagem para autenticação. Mensagens periódicas ou de eventos esporádicos transmitidas na rede devem incluir pelo menos duas marcas de tempos TS_i e TS_{i-1} autenticadas por duas RSUs consecutivas RSU_i e RSU_{i-1}.

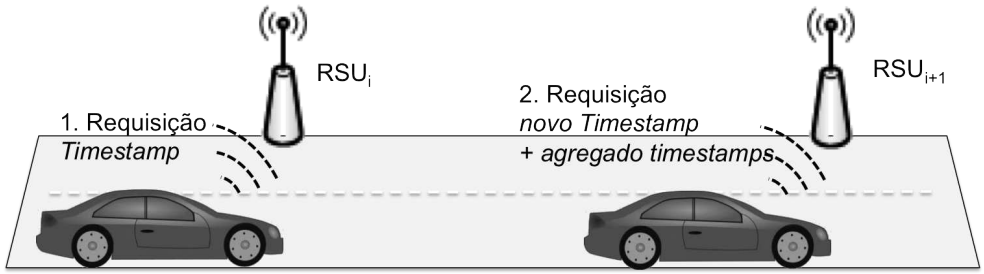


Figura 3.4: Representação da abordagem para inibir ataques *sybil* baseada em marcas de tempo (*timestamp*). (Adaptada de [60])

O protocolo de negociação de marcas de tempo é ilustrado na Figura 3.5. Na Etapa 1, mensagens *broadcasts* transmitidas pela RSU_i informam a autenticidade da RSU_i através do respectivo certificado digital $Cert\_R_i$. Na Etapa 2, o veículo gera um novo par de chaves pública/privada (KV_i^+, KV_i^-). Se a RSU_i atual for a primeira RSU em contato, a requisição para a nova marca de tempo inclui apenas a nova chave pública KV_i^+. Caso contrário, a requisição de renovação de marca de tempo deve incluir a nova chave pública gerada (KV_i^+), o certificado digital das marcas de tempo anteriores ($Cert\_T_{i-1}$), o certificado digital da RSU anterior ($Cert\_R_{i-1}$) - buscando garantir autenticidade de $Cert\_T_{i-1}$ -, e a assinatura digital da requisição da Etapa 2. Por fim, na Etapa 3 é gerado e enviado ao veículo o novo certificado da marca de tempo para a chave pública KV_i^+. Para tal, RSU_i inicialmente extrai os certificados de marcas de tempo gerados em RSUs anteriores a partir de $Cert\_T_{i-1}$ ($TS_{i-1}, TS_{i-2}, TS_{i-3}, ...$) e gera um novo certificado de marcas de tempo (ATS_i) agregando a atual marca de tempo (TS_i) para a nova chave pública KV_i^+. O novo certificado de marcas de tempo é então gerado a partir da assinatura digital da RSU_i corrente (Sig(KR_i^-, Conteúdo)). Mensagens periódicas enviadas à rede

são estruturadas seguindo o formato $\langle Dados, Sig(KV_i^-, Dados), Cert\_T_i, Cert\_R_i \rangle$.

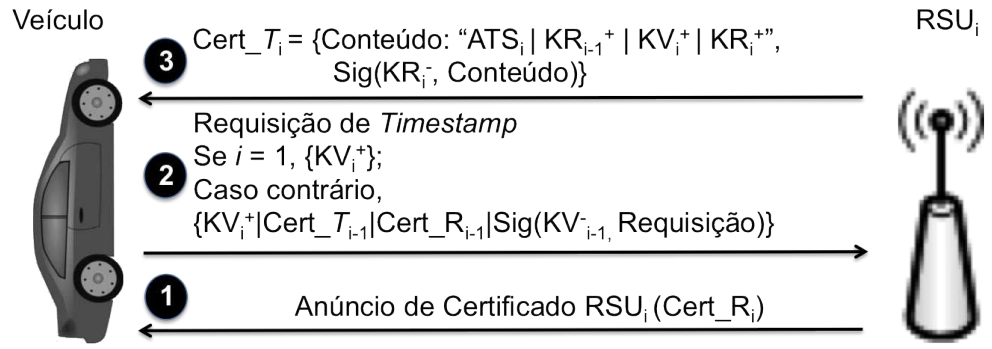


Figura 3.5: Protocolo de renovação de marcas de tempo para novo par de chaves pública/privada. (Adaptada de [60])

Considerando duas mensagens arbitrárias $M_1 = \langle Dados, Cert\_T_i, Cert\_R_i \rangle$ e $M_2 = \langle Dados, Cert\_T_j, Cert\_R_j \rangle$, sendo $Cert\_R_n$ o certificado digital da enésima RSU, um nó avaliador detectará um potencial nó *sybil* avaliando os seguintes parâmetros:

1. Se os certificados digitais $Cert\_R_i$ e $Cert\_R_j$ são os mesmos, isto é, os certificados digitais pertencem às mesmas RSUs;

2. Se os certificados de marcas de tempo mais recentes $Cert\_T_i$ e $Cert\_T_j$ foram emitidos pela mesma RSU;

3. Se os certificados digitais $Cert\_R_{i-1}$ e $Cert\_R_{j-1}$ são idênticos, isto é, a penúltima RSU originou as marcas de tempo;

4. E, por fim, se a diferença entre as duas últimas marcas de tempo é inferior a um determinado limiar: $|TS_i - TS_j| < \epsilon$ e $|TS_{i-1} - TS_{j-1}| < \epsilon$.

A proposta de marcas de tempo se apresenta como uma solução interessante para o controle entre inibir e detectar ataques *sybil* e o anonimato dos veículos. Por outro lado, uma análise rigorosa do protocolo revela um importante problema. Para tal, considere o cenário ilustrado na Figura 3.6. Ao transitar pelas RSUs 1, 2 e 3, o veículo adquiriu três marcas de tempo (TS_1, TS_2, TS_3) para três diferentes chaves (KV). Ao transitar pela RSU_4, o veículo deixa de renovar as marcas de tempo agregadas e passa a receber uma nova marca de tempo (TS_4), e a atualiza ao transitar pela RSU_5. A partir deste momento, duas mensagens $M_1 = \langle Dados, Sig(KV_3^-, Dados), Cert\_T_3, Cert\_R_3 \rangle$ e $M_2 = \langle Dados, Sig(KV_5^-, Dados), Cert\_T_5, Cert\_R_5 \rangle$ podem ser transmitidas à rede. Para as duas mensagens M_1 e M_2, nenhum dos 4 critérios de avaliação de um nó *sybil* detectaria um potencial ataque na área ilustrada na Figura 3.6:

1. $Cert\_R_3 \neq Cert\_R_5$;
2. $Cert\_T_3(TS_1, TS_2, TS_3) \neq Cert\_T_5(TS_4, TS_5)$;
3. $Cert\_R_2 \neq Cert\_R_4$;
4. As diferenças das marcas de tempo $|TS_5 - TS_3|$ e $|TS_4 - TS_2|$ serão potencialmente maiores que o limiar ϵ devido ao tempo de deslocamento do veículo para transitar entre as RSUs 2 e 5.

Este mesmo processo de raciocínio para explorar ataques *sybil* nas abordagens baseadas em espaço/tempo também pode ser aplicado nas abordagens propostas por [58, 59].

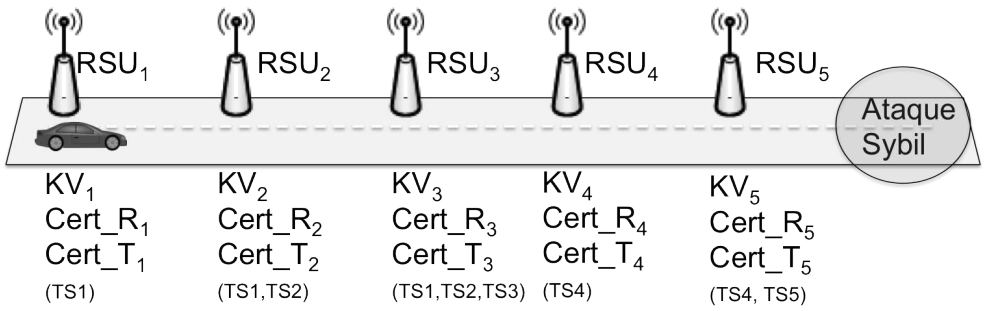


Figura 3.6: Potencial ataque *sybil* na abordagem de marcas de tempo.

A seguir são apresentados os parâmetros de comparação com relação à abordagem em questão:

1. **Detecção de ataques *sybil* na região geográfica e no momento de ocorrência do ataque**: a abordagem é capaz de detectar ataques tanto na região de ocorrência, quanto no momento do ataque;
2. **Independência de uma infraestrutura fixa para detecção de ataques *sybil***: a solução depende exclusivamente da distribuição das RSUs, porém, não depende da presença dessas no momento do ataque;
3. **Independência da característica de fluxo de veículos e/ou da topologia das estradas para detecção de ataques *sybil***: as soluções baseadas nesta categoria possuem limitações quanto ao fluxo de veículos nas rodovias, como discutido na Seção 1.2;
4. **Resiliência a resultados falso-positivo e falso-negativo**: ambos os resultados podem ser evoluídos. Resultados falso-negativo podem ser obtidos em cenários discutidos no item anterior. Por outro lado, resultados falso-positivo podem ser obtidos quando dois ou mais veículos deslocam-se em conjunto e enviam requisições com intervalos próximos;

5. **Detecção de ataques *sybil* oriundos de mensagens periódicas e esporádicas**: a solução é capaz de detectar ataques oriundos em ambos os tipos de mensagens;

6. **Autenticação com suporte à não-repúdio**: não oferece suporte à não-repúdio, uma vez que os certificados obtidos para autenticação não associa identidades de veículos.

Footprint

A abordagem denominada *Footprint* [58] explora a relação espaço/tempo a partir das RSUs ao longo das vias considerando principalmente três hipóteses: primeira, a probabilidade de dois veículos distintos possuírem a mesma rota, no mesmo intervalo de tempo, é baixa; segunda, um veículo não se desloca entre dois pontos (leia-se, duas RSUs) em um intervalo de tempo menor que t unidades de tempo (denominado limite de tempo de travessia, do inglês *traverse time limit*); e, por fim, a terceira hipótese afirma que a quantidade de RSUs numa trajetória para um intervalo de tempo é limitada pela velocidade do veículo (limite de tamanho de trajetória, do inglês *trajectory length limit*).

Está ilustrada na Figura 3.7 a primeira fase do protocolo *Footprint*, a qual tem como objetivo permitir que veículos construam uma trajetória autêntica. Para tal, um veículo v, ao transitar por uma RSU, gera um par de chaves $K^+_{v,i}/K^-_{v,i}$ e requisita para a RSU uma autenticação de mensagem (Etapa 1). Em seguida, a RSU gera uma assinatura digital da mensagem M que inclui a marca de tempo atual (*timestamp*) e a chave pública enviada pelo veículo. Esse processo é repetido para cada nova RSU na trajetória, porém, gerando-se um novo par de chaves $K^+_{v,i+1}/K^-_{v,i+1}$.

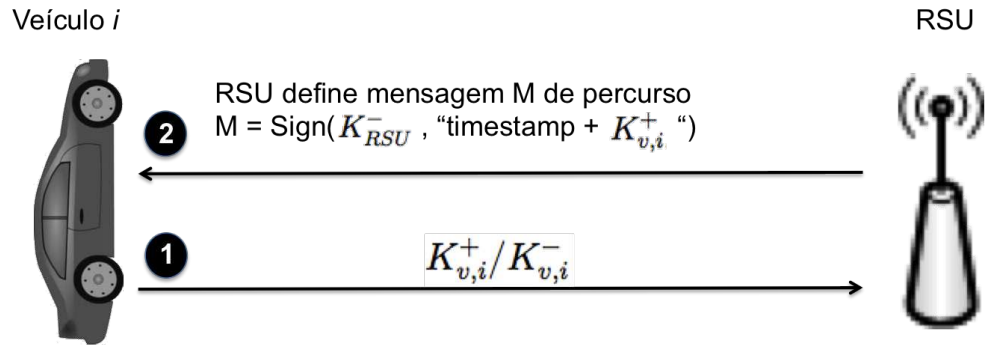


Figura 3.7: Protocolo de aquisição de mensagem para a construção de trajetórias da abordagem *Footprint*.

O processo de detecção de ataques *sybil* ocorre em duas etapas: na primeira etapa, realiza-se um processo de teste de exclusão (*exclusion test*), cujo objetivo é examinar se duas trajetórias distintas pertencem a veículos diferentes. O teste terá resultado positivo (ou seja, serão duas trajetórias pertencentes a dois veículos diferentes) se a partir do

conjunto de RSUs visitadas, duas possíveis condições serão satisfeitas: existem duas RSUs distintas em intervalos de tempo menor que um dado limiar (isto é, o veículo não pode estar em dois lugares diferentes ao mesmo tempo); ou a quantidade de RSUs visitadas, considerando a união de ambas as trajetórias, não é maior que o limite de tamanho de trajetória (isto é, o veículo não se deslocou uma distância maior que o possível). Ilustra-se na Figura 3.8 esta primeira condição, onde uma janela de verificação é estabelecida (linhas pontilhadas) para determinar as semelhanças ou diferenças nas trajetórias (ex.: trajetórias de v_i e v_j são diferentes devido às RSUs R3 e R2, respectivamente).

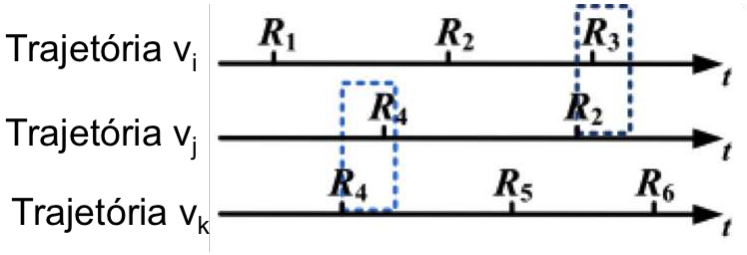


Figura 3.8: Janela de checagem permitem determinar diferenças entre trajetórias. Adaptada de [58].

Para avaliar a segunda condição, determina-se, inicialmente, a sequência cronológica de cada RSU. Considerando a Figura 3.8, tem-se: $\{R_1; R_4; R_2; R_5; R_3; R_6\}$. Ao considerar o tamanho do limite de trajetória igual a 5, conclui-se que as trajetórias pertencem a dois veículos distintos, uma vez que seria impossível, para esse limite de trajetória, um único veículo se deslocar por 6 RSUs diferentes.

Caso não seja possível detectar um ataque *sybil* a partir do teste de exclusão, busca-se determinar a similaridade entre as duas rotas a partir da Equação 3.1, ou seja, quanto maior a quantidade de RSUs diferentes entre v_i e v_j, maior o valor de $Diff$ e menos semelhantes serão as trajetórias.

$$\frac{T_1 \cap T_2}{Min\{|T_1 \cap T_2\}} \tag{3.1}$$

A seguir, são apresentados os parâmetros de discussão sobre o projeto *Footprint*:

1. **Detecção de ataques *sybil* na região geográfica e no momento de ocorrência do ataque**: o processo de detecção pode ser realizado na região de ataque e no momento de ocorrência;

2. **Independência de uma infraestrutura fixa para detecção de ataques *sybil***: apesar de não depender de uma infraestrutura fixa durante o momento do ataque, a abordagem *Footprint* dependerá do modelo de distribuição de RSUs a fim de que se determine o tamanho de travessia e trajetória. Este processo pode tornar o modelo

de distribuição de RSUs complexo, bem como exigir um modelo para adaptar o tamanho dos limites de travessia e trajetória;

3. **Independência da característica de fluxo de veículos e/ou da topologia das estradas para detecção de ataques *sybil***: consequência do item anterior, a abordagem dependerá do modelo de distribuição das RSUs, bem como do fluxo de veículos, apesar de ser menos suscetível a ataques *sybil* quando comparada a abordagem discutida anteriormente (*Timestamp Series*);

4. **Resiliência a resultados falso-positivo e falso-negativo**: a abordagem não é resiliente a resultados falso-positivo e falso-negativo, os quais dependerão dos limites de travessia e trajetória definidos, isto é, como as RSUs estarão distribuídas ao longo das vias. Como consequência, tais resultados ocorrem devido ao teste de exclusão, o qual não é possível detectar ataques *sybil* ou evitar que veículos não-maliciosos sejam tratados como tal;

5. **Detecção de ataques *sybil* oriundos de mensagens periódicas e esporádicas**: apesar de não detalhado pelos autores, é possível detectar ataques *sybil* oriundos em ambos os tipos de mensagens. Entretanto, o tamanho das mensagens pode crescer significativamente dependendo dos limites de travessia e trajetória, o que poderá ultrapassar o tamanho ideal das mensagens periódicas;

6. **Autenticação com suporte à não-repúdio**: não oferece suporte à não-repúdio, uma vez que os certificados obtidos sobre a rota do veículo não associa identidades de veículos.

RobSAD

A abordagem denominada RobSAD (*Robust method of Sybil Attack Detection*) [59] também utiliza as infraestruturas de RSUs para monitorar a trajetória realizada por um veículo. Ao trafegar por cada RSU, um veículo v_i solicita e obtém uma assinatura digital para comprovar sua presença na região da RSU, formando um conjunto de pontos trafegados $R_{v_i} = \{RSU_1, RSU_2, RSU_3, ..., RSU_r\}$.

Para detectar um ataque *sybil*, uma entidade avaliadora inicialmente verifica o grau de similaridade entre duas trajetórias a partir da Equação 3.2, partindo da hipótese que dois veículos v_i e v_j possuirão diferenças entre suas trajetórias R_{v_i} e R_{v_j}. Logo, $Diff(R_{v_i}, R_{v_j}) \geq 0$ se $R_{v_i} \neq R_{v_j}$; será 0, caso contrário. Por fim, para detectar um ataque *sybil*, duas trajetórias serão consideradas como pertencentes a veículos distintos se, e somente se, $Diff(v_i, v_j) \geq threshold$.

$$Diff(R_{v_i}, R_{v_j}) = \frac{1}{r} \cdot \sum_{k=1}^{r} d_k, d_k = \begin{cases} 1 & \text{se} \quad RSU_{Rv_i} \neq RSU_{Rv_j} \\ 0 & \text{se} \quad RSU_{v_i} = RSU_{v_j} \end{cases} \tag{3.2}$$

A seguir, são discutidos os parâmetros de comparação considerando a abordagem RobSAD:

1. **Detecção de ataques *sybil* na região geográfica e no momento de ocorrência do ataque**: o processo de detecção pode ser realizado na região de ataque e no momento de ocorrência;

2. **Independência de uma infraestrutura fixa para detecção de ataques *sybil***: a abordagem não depende da infraestrutura para detectar ataques, porém, depende de uma quantidade relativamente grande para evitar resultados *falso-positivo* e *falso-negativo*;

3. **Independência da característica de fluxo de veículos e/ou da topologia das estradas para detecção de ataques *sybil***: as soluções baseadas nesta categoria possuem limitações quanto ao fluxo de veículos nas rodovias, como discutido na Seção 1.2;

4. **Resiliência a resultados falso-positivo e falso-negativo**: assim como analisado pelos autores da abordagem RobSAD, a taxa de detecção de ataques *sybil* diminui à medida que $Diff(R_{v_i}, R_{v_j})$ aumenta. Como exemplo, para $Diff(R_{v_i}, R_{v_j}) = 5\%$, a taxa de detecções corretas está entre 95% e 98%, ao passo que essa taxa diminui para 85% a 93% quando $Diff(R_{v_i}, R_{v_j}) = 10\%$, e para 65% e 75% quando $Diff(R_{v_i}, R_{v_j}) = 20\%$. Ou seja, resultados falso-positivo e falso-negativo podem ocorrer quando o mínimo de similaridade entre duas rotas aumenta;

5. **Detecção de ataques *sybil* oriundos de mensagens periódicas e esporádicas**: a abordagem é capaz de detectar ataques oriundos de ambos os tipos de mensagens;

6. **Autenticação com suporte à não-repúdio**: não oferece suporte à não-repúdio, uma vez que os certificados obtidos sobre a rota do veículo não associa identidades de veículos.

3.2.3 Abordagens Baseadas no Monitoramento de Nós Vizinhos

Outras abordagens para detecção de ataques *sybil* são através do monitoramento dos veículos vizinhos, e da colaboração entre veículos vizinhos [63, 64]. Nestas abordagens,

parte-se de duas hipóteses, a saber: à medida que os nós se deslocam, identidades oriundas de um nó *sybil* são continuamente apresentadas durante a fase de transmissão de mensagens periódicas para um dado intervalo de tempo; e nós vizinhos a um nó *sybil* receberão mensagens periódicas possuindo as mesmas identidades (oriundas de um potencial nó *sybil* presente na região).

Nesse contexto, Piro et al [61] propõem um modelo para o cálculo de afinidade entre duas identidades observadas, uma abordagem inicialmente proposta para MANETs. Inicialmente, um nó avaliador realiza um conjunto de monitoramentos (M_1, M_2, M_3, ..., M_n) de mensagens periódicas observando-se as identidades dos nós vizinhos. Cada monitoramento M_i possui um conjunto de identidades observadas. O modelo para o cálculo de afinidade é representado pela Equação 3.3, onde T_{ij} é o número de monitoramentos nos quais as identidades i e j foram observadas juntas, $L_{i,j}$ é o número de monitoramentos nos quais as identidades i ou j foram observadas e N é a quantidade total de monitoramentos realizados.

$$A_{ij} = (T_{i,j} - 2L_{i,j})\frac{T_{i,j} + L_{i,j}}{N} \tag{3.3}$$

Monitoramento de Vizinhos em VANETs

Uma abordagem inspirada no trabalho de Piro é proposta por Grover et al [62]. A detecção de um nó *sybil* é realizada através de 4 etapas. Na Etapa 1, cada veículo V_i da região monitora as mensagens periódicas as quais recebe dos nós vizinhos em diferentes intervalos de tempo $(t_1, t_2, t_3, ..., t_n)$. Na Etapa 2, cada veículo V_i constrói um conjunto de identidades observadas N_{i,t_n} para cada intervalo t_n. Na Etapa 3, cada veículo V_i compartilha o conjunto de identidades observadas N_{i,t_n} com os demais veículos da região. Por fim, na Etapa 4, cada veículo determina os veículos vizinhos similares $(N_{i,t_n} \cap N_{j,t_n})$.

Como exemplo, seja um conjunto de 15 identidades representadas por $V_1, V_2, ..., V_{15}$. O veículo V_A é um veículo *sybil* e gerou as identidades V_1, V_5 e V_8. Todos os veículos estão situados numa região na qual deslocam-se a partir de um padrão de mobilidade que os garantem a troca de mensagens periódicas. Está apresentado na Tabela 3.1 o conjunto de identidades vizinhas observadas para cada veículo V_x, considerando 4 intervalos de monitoramentos. Desta forma, pode-se observar que os veículos V_C e V_D podem ambos detectarem que estão recebendo mensagens periódicas de potenciais identidades *sybil* (V_1, V_2, V_5, V_8).

As soluções baseadas em monitoramento dos nós vizinhos apresentam uma deficiência simples. Ora, se um veículo *sybil* é capaz de gerar diferentes identidades e determinar quais identidades serão utilizadas em um determinado momento, então um veículo *sybil*, ao alternar identidades em intervalos de tempo menores que o intervalo de monitoramento

V_x	T_0	T_1	T_2	T_3
V_E	$V_1, V_2, V_8, V_5, V_{10}$	$V_1, V_2, V_3, V_8, V_5, V_{10}$	V_5, V_8	V_8
V_B	$V_1, V_2, V_8, V_5, V_{12}, V_3$	$V_1, V_2, V_8, V_5, V_3, V_{12}$	V_3, V_5, V_8	V_8, V_{12}
V_C	$V_1, V_2, V_5, V_8, V_7, V_6$	V_1, V_2, V_5, V_8, V_7	V_1, V_2, V_5, V_8	V_1, V_2, V_5, V_8, V_6
V_D	$V_1, V_2, V_5, V_8, V_4, V_{11}$	$V_1, V_2, V_5, V_8, V_{11}$	$V_1, V_2, V_5, V_8, V_{11}$	V_1, V_2, V_4, V_5, V_8
...	...	...	...	...

Tabela 3.1: Conjunto de vizinhos monitorados para 4 intervalos de monitoramento.

dos nós (ex.: T_0 para T_1), pode nunca ser detectado. Para tal, considere que o veículo *sybil* V_A, além de ser responsável pela geração das identidades V_1, V_5 e V_8, também gerasse as identidades V_{16}, V_{17}, V_{18}. Para evitar ser detectado, veículo V_A poderia alternar entre todos as identidades *sybil* de tal modo que a interseção entre duas ou mais identidades não seja possível para mais de um intervalo de monitoramento. Além disso, não se pode garantir que veículos vizinhos compartilham conjuntos consistentes de identidades observadas, isto é, um veículo (ou um conluio de veículos) malicioso poderá simplesmente não incluir as identidades de um nó *sybil* nos conjuntos de identidades que compartilha, o que exige mecanismos de confiança e reputação [178, 179] para inicialmente filtrar apenas veículos confiáveis.

A seguir, uma breve análise desta abordagem com relação aos principais pontos considerados:

1. **Detecção de ataques *sybil* na região geográfica e no momento de ocorrência do ataque**: o processo de detecção pode ser realizado na região de ataque e no momento de ocorrência. Entretanto, dependerá do tempo de monitoramento dos nós vizinhos;

2. **Independência de uma infraestrutura fixa para detecção de ataques *sybil***: a abordagem não depende da infraestrutura para detectar ataques *sybil*;

3. **Independência da característica de fluxo de veículos e/ou da topologia das estradas para detecção de ataques *sybil***: depende do fluxo de veículos, uma vez que são monitoradas identidades que se deslocam em conjunto;

4. **Resiliência a resultados falso-positivo e falso-negativo**: este é o fator mais crítico da abordagem de monitoramento de nós vizinhos. Resultados *falso-positivo* poderão ser gerados quando diferentes identidades pertencentes a diferentes veículos deslocam-se em conjunto por um longo período de tempo, ao passo que resultados *falso-negativo* ocorrerão quando um veículo malicioso alternar entre identidades para

diferentes intervalos de tempo. Esta mesma análise também é válida para o trabalho de Piro;

5. **Detecção de ataques *sybil* oriundos de mensagens periódicas e esporádicas**: oferece suporte à detecção de ataques *sybil* apenas quando explorado em mensagens periódicas, uma vez que realiza apenas um monitoramento de mensagens em diferentes intervalos de tempo à medida que os veículos se deslocam na via;

6. **Autenticação com suporte à não-repúdio**: não oferece mecanismos de autenticação. Consequentemente, dependerá do modelo de autenticação utilizado.

Monitoramento baseado em Enfileiramento de Veículos (platton-based)

A abordagem proposta por Al-Mutaz et al [65] explora as características físicas relacionadas à dispersão de enfileiramento de veículos, uma teoria investigada pela engenharia de transportes. De acordo com essa teoria, o enfileiramento entre veículos se altera conforme eles se deslocam ao longo da via (Figura 3.9) devido a diversos fatores, quais sejam: as velocidades dos veículos se alteram, os veículos tendem a alternar entre as faixas, limitações físicas das rodovias não permitem manter o enfileiramento constante, isto é, com o mesmo comportamento. A partir desta teoria, parte-se da hipótese que um veículo malicioso, ao explorar um ataque *sybil*, não apresenta um comportamento de dispersão de enfileiramento.

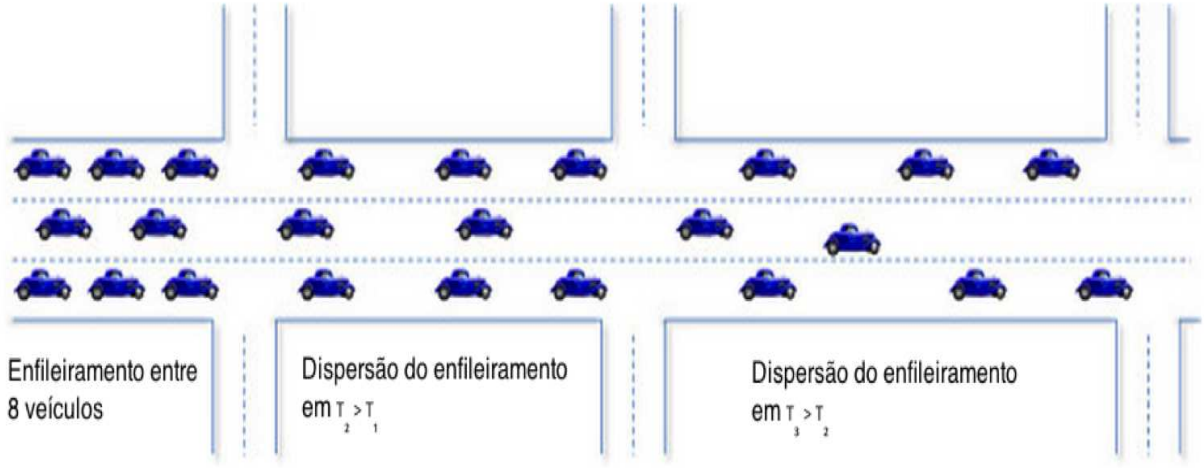


Figura 3.9: Dispersão de enfileiramento de veículos.
Adaptada de [65].

Desta forma, um conjunto de RSUs é alocado ao longo das vias para monitorar o tráfego a fim de identificar enfileiramentos que não seguem um padrão de dispersão esperado. O monitoramento realizado pelas RSUs é baseado em dois modelos amplamente

estudados no contexto de engenharia de transportes, a saber: o modelo de distribuição geométrica de Robertson [180] e o modelo de distribuição de Pacey [181]. Ambos os modelos consideram que os veículos assumem uma distribuição de probabilidade específica. A partir da variação de velocidade entre os veículos e do tempo médio de deslocamento, é computado o grau de dispersão de enfileiramento dos veículos.

A seguir, uma breve análise desta abordagem com relação aos principais pontos considerados:

1. **Detecção de ataques *sybil* na região geográfica e no momento de ocorrência do ataque**: o processo de detecção pode ser atrasado enquanto não alcançar uma quantidade de RSUs necessária para determinar o tempo médio de deslocamento e a velocidade média relativa entre os veículos. Desta forma, o ataque nem sempre será detectado na região em que se iniciou;

2. **Independência de uma infraestrutura fixa para detecção de ataques *sybil***: a abordagem depende exclusivamente da infraestrutura de RSUs para detectar ataques *sybil*, uma vez que os modelos de detecção de dispersão de enfileiramento são executados em cada uma;

3. **Independência da característica de fluxo de veículos e/ou da topologia das estradas para detecção de ataques *sybil***: depende do fluxo de veículos, uma vez que são monitoradas identidades que se deslocam em conjunto;

4. **Resiliência a resultados falso-positivo e falso-negativo**: se uma quantidade relativamente grande de veículos se desloca em diferentes faixas, a velocidade relativa entre os veículos tende a se manter praticamente constante, gerando resultados *falso-positivo*. Resultados *falso-negativo* ocorrerão quando um veículo malicioso implementar um modelo de dispersão de enfileiramento entre as mensagens transmitidas;

5. **Detecção de ataques *sybil* oriundos de mensagens periódicas e esporádicas**: oferece suporte à detecção de ataques *sybil* apenas quando explorado em mensagens periódicas, uma vez que realiza apenas um monitoramento de mensagens em diferentes intervalos de tempo à medida que os veículos se deslocam na via;

6. **Autenticação com suporte à não-repúdio**: não oferece mecanismos de autenticação. Consequentemente, dependerá do modelo de autenticação utilizado.

3.3 Considerações Finais

Neste capítulo, foram descritas as principais abordagens correlatas à proposta deste trabalho de tese. A seguir, está detalhado na Tabela 3.2 um comparativo entre as referidas abordagens e o protocolo *ASAP*-V, ora apresentado no Capítulo 4.

A principal limitação encontrada nas abordagens refere-se a detecções *falso-positivo* e *falso-negativo*, principalmente quando não se há uma infraestrutura centralizada (RSU ou C.A) para detectar um ataque *sybil*. Ademais, as soluções que fazem uso de tais infraestruturas têm como principal desvantagem a sobrecarga imposta às RSUs, bem como a limitação em detectar ataques *sybil* em cenários onde as RSUs não estão disponíveis devido a diversos fatores, a saber: número restrito de RSUs na fase de implantação inicial das redes VANETs; e a indisponibilidade de RSUs devido a fatores físicos, tais como roubos de equipamentos, falhas e ataques contra a disponibilidade de serviços (DoS). O protocolo *ASAP*-V é imune a detecções *falso-positivo* e *falso-negativo*, isto é, um veículo legítimo não é detectado como malicioso e, da mesma forma, um veículo malicioso será sempre detectado.

Tabela 3.2: Comparação com as abordagens discutidas.

Abordagens	Suporte a Falso-negativo ou Falso-positivo	Não-Repúdio	Periódica ou Esporádica	Infraestrutura Centralizada	Infraestrutura e fluxo de veículos
ASAP-V	**Ambos**	**Sim**	**Ambos**	**Não**	**Não**
P^2DAP	Negativo	Sim	Ambos	Sim	Não
Footprint	Não	*	Ambos	Sim	Sim
RobSAD	Não	*	Ambos	Sim	Sim
Timestamp Series	Não	Não	Ambos	Sim	Sim
Monitoramento	Não	*	Periódica	Não	Não
RFID-based	Positivo	Não	Ambos	Sim	Não
Platton-based	Não	*	Periódica	Sim	Não

*Dependerá do modelo de autenticação a ser utilizado.

Um outro fator pouco explorado nas abordagens discutidas refere-se ao controle de anonimato dos veículos envolvidos. Apesar de apresentarem mecanismos para lidar com tal requisito, nenhuma das abordagens analisam e discutem sobre o grau de anonimato efetivamente oferecido pela solução. Nesse contexto, o anonimato dos veículos em abordagens baseadas na relação espaço/tempo pode ser afetado devido às assinaturas digitais

que cada RSU define a um veículo específico. Por outro lado, nas abordagens baseadas em PKI, apenas a solução P^2DAP oferece um nível de controle de anonimato dos veículos, porém, exige a presença de uma RSU para evitar detecções *falso-negativo*. Por outro lado, o anonimato de um veículo na solução RFID-based pode ser comprometido se as zonas forem geograficamente e relativamente grandes, uma vez que um veículo poderá armazenar e utilizar apenas uma única identidade. Por fim, o controle de anonimato nas demais abordagens dependerá do modelo de autenticação a ser utilizado.

Capítulo 4

Autenticação e Detecção de Ataques Sybil em Redes Ad Hoc Veiculares

Neste capítulo, apresenta-se um protocolo para autenticação e detecção de ataques *sybil* em Redes Ad Hoc Veiculares (VANETs) denominado *ASAP*-V (do inglês, *Authentication and Sybil Attack detection Protocol for VANETs*). Tanto para o processo de autenticação, quanto para o processo de detecção de ataques *sybil*, o protocolo provê suporte ao controle de anonimato de veículos[1].

Este capítulo inicia-se delineando o modelo de ameaça contra a segurança pretendida, prosseguindo com as diretrizes e os principais requisitos para lidar com as potenciais ameaças. Posteriormente, é introduzida a arquitetura principal da solução, detalhando o modelo de autenticação de veículos e o mecanismo de detecção de ataques *sybil* com suporte ao controle de anonimato dos usuários. Finalmente, descreve-se a execução da fase de detecção de ataques *sybil* modelada em Máquinas de Estados Finito, finalizando com uma visão geral sobre o capítulo.

4.1 Considerações Preliminares

4.1.1 Modelo de Ameaça

O projeto e a concepção de protocolos de segurança em um sistema distribuído exigem, inicialmente, a compreensão das potenciais ameaças que podem surgir durante a execução dos serviços disponíveis. Tais ameaças são oriundas de potenciais entidades que têm como objetivo central burlar o sistema para obter vantagens ou torná-lo, por exemplo, indisponível.

[1] As expressões "anonimato de veículos" ou "anonimato de usuários" serão utilizadas para referir-se ao anonimato do dono de um veículo.

Nesta perspectiva, há basicamente duas principais ameaças consideradas no protocolo proposto, a saber: ataques *sybil* e violação de anonimato dos usuários participantes (ex.: motoristas). Com base na categorização definida por Raya e apresentada na Seção 2.5, para o primeiro caso, entidades são usuários (atacantes) que podem ser classificados como *interno*, *racional* ou *malicioso*, e *ativo*, os quais modificam internamente um veículo para a execução do ataque. O atacante está normalmente situado na região de ataque e utiliza seu próprio veículo para executar o ataque. As consequências deste ataque também estão restritas a uma região específica (i.e.: normalmente afetando um raio entre 2 a 3 quilômetros).

No segundo caso, o atacante pode ser *interno* ou *intruso*, *racional* e *passivo* e pode estar situado em uma região específica monitorando o canal de comunicação, ou bem como distribuir sensores de monitoramento em diferentes regiões a fim de coletar e enviar os dados para uma infraestrutura centralizada.

4.1.2 Diretrizes e Requisitos da Solução

Nesta seção, são apresentados os principais requisitos que conduziram o desenvolvimento do protocolo. O protocolo oferece mecanismos de autenticação e não-repúdio de veículos, bem como integridade de mensagens transmitidas, ao passo que a detecção de ataques *sybil* e a verificação de autenticidade de mensagens transmitidas na rede são realizadas sem comprometer o anonimato dos usuários. Os requisitos considerados são basicamente seis, a saber:

1. **Autenticação com suporte ao anonimato condicional**: apenas entidades tais como C.As e governos podem relacionar as mensagens enviadas por veículos a uma identidade única (ex.: dono do veículo), promovendo anonimato condicional. Isto é, a associação entre entidade e identidade manifesta-se apenas em casos excepcionais (es.: investigação de acidentes, emissão automática de multas etc.);

2. **Detecção de ataques *sybil* sem afetar o anonimato condicional**: a detecção de um possível ataque *sybil* não afeta o anonimato condicional de veículos legítimos, isto é, a relação entre mensagem e a identidade real de um veículo legítimo não é estabelecida durante o processo de detecção de ataque *sybil*;

3. **Detecção de ataques *sybil* de forma descentralizada**: a detecção de ataques *sybil* ocorre de forma distribuída em cada veículo, sem a necessidade de uma infraestrutura fixa (ex.: RSUs ou C.As);

4. **Detecção de ataques *sybil* sem necessidades de mecanismos de reputação, e resiliente ao conluio entre veículos *sybil***: a fase de detecção de ataques

sybil não exige mecanismos de reputação de veículos, ou seja, não se faz necessário determinar o grau de confiabilidade dos nós envolvidos;

5. **Detecções de ataques *sybil* resilientes a resultados *falso-positivo* e *falso-negativo***: a solução proposta neste trabalho garante que um veículo *sybil* seja detectado como tal (não há resultados *falso-negativo*), e que veículos legítimos não sejam detectados como maliciosos (não há resultados *falso-positivo*);

6. **Exclusão do veículo *sybil* da rede**: uma vez detectado um veículo malicioso, este é (temporariamente) excluído da rede com o objetivo de minimizar o impacto de futuros ataques deste veículo na rede. Este processo ocorre através de um procedimento de acusação, no qual veículos legítimos que detectaram o ataque enviam para a RSU/C.A cópias de mensagens oriundas do veículo malicioso utilizadas durante o ataque.

4.1.3 Arquitetura Geral da Solução

Em um sistema distribuído, há basicamente dois modelos de segurança, a saber: infraestruturado ou descentralizado (*ad hoc*). Evidentemente, o modelo infraestruturado é tradicionalmente considerado em soluções que envolvem autenticação, fazendo-se uso de uma entidade confiável para distribuição de identidades para os nós da rede. Tal entidade é comumente chamada de Autoridade Certificadora e assegura que nós participantes do sistema se comuniquem de forma segura por meio de chaves de criptografia. No segundo caso, a distribuição de identidades e chaves de criptografia é realizada pelos próprios nós. Neste caso, modelos de confiança e reputação [182] são exigidos para assegurar que mensagens oriundas de quaisquer nós sejam consideradas autênticas.

Nesta perspectiva, devido à entrada e saída de (novos) nós na rede, o uso de um modelo puramente *ad hoc* para proporcionar segurança em ambientes veiculares pode tornar a rede menos segura[2] e mais complexa para gerenciar. Isso se deve ao fato de que a funcionalidade para assegurar que veículos sejam autênticos é distribuída entre os veículos. Caso um veículo malicioso não seja detectado, este poderá diminuir o grau de confiança e reputação de veículos legítimos. Desta forma, o protocolo de autenticação proposto neste trabalho de pesquisa faz uso do modelo infraestruturado para a *distribuição de chaves de criptografia*, assim como boa parte dos trabalhos que envolvem segurança encontrados na literatura [8–10, 183–186].

[2]Como exemplo, alguma entidade deve garantir que veículos de emergência, tais como ambulâncias e de segurança pública, sejam, de fato, autênticos. Caso contrário, veículos podem, por exemplo, apresentar-se como tipo de emergência para obter acesso livre nas vias.

Uma característica basilar das redes *ad hoc* é a falta de uma infraestrutura fixa para gerenciar serviços na rede. Em redes VANETs, um dos serviços que as RSUs devem prover é a comunicação entre veículos em ambientes veiculares esparsos. Ademais, as RSUs podem proporcionar serviços de conexões com outras redes, tal como a internet. Entretanto, nem sempre será possível considerar que uma RSU estará disponível numa dada região devido a diversos fatores, a saber: custos; sobrecarga na rede; roubo de equipamentos; ataques com o objetivo de tornar indisponível serviços da RSU (como, por exemplo, negação de serviços - DoS) etc. Como consequência dessa premissa, pode-se encontrar trabalhos na literatura que têm como objetivo a construção de modelos de distribuição de RSUs usando-se, como métrica principal, o potencial de disseminação de informações, bem como o baixo custo [55–57]. Desta forma, a abordagem para detectar ataques *sybil* proposta neste trabalho *não depende da disponibilidade de uma infraestrutura fixa*, tornando a solução tolerante a falhas e desconexões.

4.2 Protocolo *ASAP-V*: autenticação e detecção de ataques *sybil* em redes VANETs com suporte ao controle de anonimato

Nesta seção, são apresentados os detalhes do protocolo proposto. Denominado *ASAP-V*, o protocolo é dividido em quatro fases, a saber: registro e autenticação de veículos (Fase 1); distribuição de identidades temporárias a veículos (Fase 2); detecção de ataques *sybil* (Fase 3); e acusação de veículos *sybil* (Fase 4). Nas subseções a seguir são detalhadas as fases utilizando-se a nomenclatura apresentada na Tabela 4.1.

Tabela 4.1: Nomenclatura para descrição do protocolo *ASAP*-V.

Símbolo	**Descrição**
v_c	Veículo c.
RSU_q	Uma RSU com identidade q disponível na estrada.
$cert_a$	Certificado digital da entidade a.
$cert_{a,n}$	Certificado digital da enésima chave pública da entidade a.
$k^+_{a,n}$	Enésima chave pública da entidade a, cujo certificado digital é $cert_{a,n}$.
$k^-_{a,n}$	Enésima chave privada da entidade a associada a chave pública $k^+_{a,n}$.
TK_a	Conjunto de pares de chaves temporárias (pseudônimos) da entidade a.
gsk_a	Do inglês *Group Signing Key*. Chave secreta da entidade a para assinatura de grupo (esquema de assinatura de grupos).

Continua na próxima página

Tabela 4.1 – *Continuação da página anterior*

Símbolo	**Descrição**
gpk	Do inglês *Group Public Key*. Chave pública de grupo (esquema de assinatura de grupos).
grt_c	Do inglês *group revocation token*. O *Token* do veículo v_c (esquema de assinatura de grupos).
RL	Lista de *tokens grt* revogados (esquema de assinatura de grupos).
tmp	Marca de tempo atual.
tmp_{ctn}	Marca de tempo em que o conteúdo *ctn* foi assinado.
$threshold_X$	Denota o tempo máximo (X = max) ou mínimo (X = min) para definição de um intervalo de tempo t.
$Signed_a^{ctn}$	Denota que a entidade a é responsável pela assinatura digital do conteúdo *ctn*.
m_a	Mensagem definida pela entidade a
$a \Rightarrow b : m_a$	Requisição originada pela entidade a e endereçada para a entidade b com mensagem m_a.
$Sign(\bullet)$	Função para geração de assinaturas digitais com chave e parâmetros específicos (modelo de criptografia assimétrica ou esquema de assinatura de grupos).
$Verify(\bullet)$	Função para verificação de assinaturas digitais.
$E(\bullet)$	Função para criptografia utilizando chaves assimétricas.
$D(\bullet)$	Função para decriptografia utilizando chaves assimétricas.
$sybil_{v_c}$	Um veículo v_c é um nó malicioso que executou um ataque *sybil*.

De uma forma geral, o protocolo $ASAP$-V é apenas uma peça de uma sistema SV a ser executado em uma rede veicular. O sistema SV é definido a partir da tupla a seguir:

$$SV = \langle V, RSU, ca \rangle,$$

em que,

- $V = \{v_0, v_1, ..., v_p\}$ é o conjunto de veículos registrados no sistema, sendo $p \in \mathbb{N}$;
- $RSU = \{RSU_0, RSU_1, RSU_2, ..., RSU_r\}$ é o conjunto de unidades de acostamento que estão registradas no sistema, sendo $r \in \mathbb{N}$. As RSUs compartilham um único par de chaves de criptografia (k^+_{RSU}, k^-_{RSU}), sendo a chave pública k^+_{RSU} representada pelo certificado digital $cert_{RSU}$;

- *ca* representa uma autoridade certificadora C.A[3], a qual é responsável pelo registro de cada veículo v_c $(1 \leq c \leq p)$ e de cada unidade de acostamento RSU_q $(1 \leq q \leq r)$ no sistema SV. Uma C.A é representada pela tupla $\langle gmsk, (k^-_{C.A}, k^+_{C.A}, cert_{C.A})$, K-AS $\rangle$, em que $(k^+_{C.A}, k^-_{C.A})$ representa um par de chaves pública/privada, sendo que a autenticidade da chave pública $k^+_{C.A}$ é garantida pelo certificado digital $cert_{C.A}$. Uma *C.A* pode ser uma entidade física/lógica, como um Departamento Nacional de Trânsito (DNT), e é a única entidade capaz de determinar a real identidade dos veículos a partir das mensagens transmitidas nas estradas. Esse procedimento é possível a partir de uma chave de gerenciamento de grupos *gmsk* (do inglês, *Group Management Singing Key*). Por fim, K-AS representa um conjunto de *conjuntos anonimato* (ver Seção 2.5.2) e é detalhado na próxima seção.

4.2.1 Fase 1: Registro e Autenticação de Veículos

A primeira fase do protocolo refere-se ao registro de um veículo na C.A. Naturalmente, com o processo de registro de veículos, pretende-se garantir a autenticidade de mensagens transmitidas na rede veicular, bem como garantir mecanismos de não-repúdio. Para tal, pressupõe-se que o veículo seja equipado com um conjunto de *hardwares* compatíveis com o padrão WAVE, incluindo um *chip* TPD (do inglês, *Tamper-Proof Device*) [187, 188] - o qual é resiliente a modificações não autorizadas -, um receptor GPS (*Global Positioning System*) e uma antena de rede sem fio compatível com o padrão 802.11p.

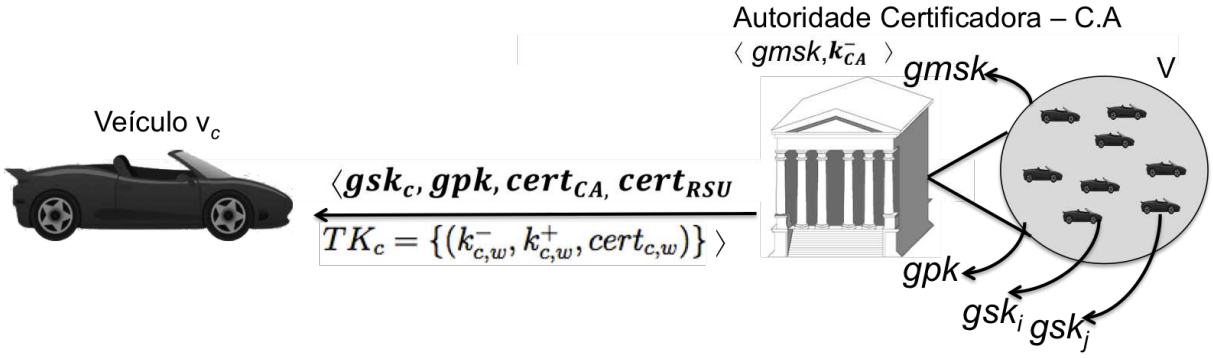


Figura 4.1: Representação do registro de veículos no modelo de autenticação *ASAP*-V.

O modelo de autenticação proposto faz uso da técnica de criptografia de chaves assimétricas (RSA, Curvas Elípticas, entre outros) e do sistema de *criptografia de grupos*. Nesse contexto, está ilustrado, na Figura 4.1, o cenário de registro de um veículo em uma C.A.

O processo de registro divide-se em duas etapas: na primeira etapa, um veículo v_c é registrado na C.A, sendo este veículo representado pela seguinte tupla:

[3]No decorrer do texto, utiliza-se a sigla C.A para representar uma *ca*.

$$v_c = \langle (gsk_c, gpk), TK_c, AS_c, CERT_{AS_c} \rangle,$$

em que,

- (gsk_c, gpk) é um par de chaves do sistema de criptografia de grupos;
- TK_c é um conjunto de pares de chaves pública/privada utilizadas como *pseudônimos* (identidades temporárias). Na fase de registro, a C.A é responsável por gerar w ($w > 1$) pares de chaves pública/privada e os respectivos certificados digitais para o veículo v_c. Um novo conjunto de pares de chaves $TK_c^{'}$ poderá ser solicitado por um veículo v_c a uma $RSU_r \in RSU$, à medida que este trafega nas vias, cujo processo é detalhado na Seção 4.2.2;
- AS_c e $CERT_{AS_c}$ são atributos utilizados para detecção de ataques *sybil* com suporte ao controle de anonimato de um veículo (usuário), e são detalhados a seguir.

Na segunda etapa desta fase de registro de veículos, cada veículo é associado a um *conjunto anonimato de veículos* $AS_{i,j}$ ($i, j \in \mathbb{N}^*; 1 \leq i \leq m, 1 \leq j \leq n$) de tal forma que cada conjunto $AS_{i,j}$ assume as propriedades do modelo formal de conjunto anonimato (ver Seção 2.5.2). No contexto do protocolo *ASAP*-V, são definidos múltiplos conjuntos anonimato $AS_{m,n}$ organizados em m níveis, com n conjuntos anonimato por nível, como ilustrado na Figura 4.2. A estrutura de múltiplos níveis de conjuntos anonimato assume as seguintes propriedades:

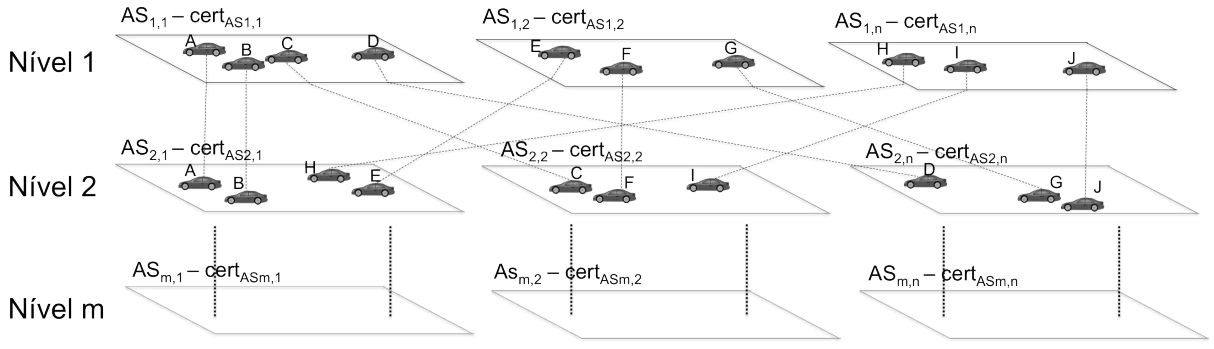


Figura 4.2: Organização em múltiplos conjuntos anonimato no modelo de autenticação e controle de anonimato do protocolo *ASAP*-V.

1. O conjunto K-AS = {$AS_{1,1}$, $AS_{1,2}$, ..., $AS_{1,n}$, ..., $AS_{2,1}$, $AS_{2,2}$, ..., $AS_{2,n}$, ..., $AS_{m,n}$} é o conjunto dos *conjuntos anonimato* divididos em m níveis e n conjuntos por nível;
2. Cada veículo deve pertencer a pelo menos k ($1 < k < n$) conjuntos anonimato por nível. O conjunto AS_c denota o conjunto de todos os *conjuntos anonimato* aos quais

um veículo v_c pertence ($AS_c \subset K\text{-}AS$). Por exemplo, $AS_c = \{AS_{1,1}, AS_{1,3}, AS_{1,12}, AS_{1,22}, AS_{1,35}, AS_{2,5}, AS_{2,9}, ..., AS_{m,n}\}$ se v_c pertence aos conjuntos anonimato $AS_{1,1}$, $AS_{1,3}, ..., AS_{m,n}$, isto é, $v_c \in AS_{1,1} \wedge v_c \in AS_{1,3} \wedge ... \wedge v_c \in AS_{m,n}$;

3. Todo conjunto anonimato $AS_{i,j}$ tem a ele associado um certificado digital $cert_{AS_{i,j}}$ de tal forma que se um veículo v_c está em $AS_{i,j}$, então v_c deve armazenar $cert_{AS_{i,j}}$. Formalmente, tem-se: $v_c \in AS_{i,j} \rightarrow cert_{AS_{i,j}} \in CERT_{AS_c}$ $\{i, j \in \mathbb{N},\ 1 \leq i \leq m$ e $1 \leq j \leq n\}$, onde:

   - $CERT_{AS_c}$ é o conjunto de todos os certificados digitais dos conjuntos anonimato aos quais o veículo v_c pertence; e,
   - Para um dado intervalo de tempo t, um veículo v_c deve selecionar um subconjunto de certificados digitais $CERT^t_{AS_c}$ ($CERT^t_{AS_c} \subset CERT_{AS_c}$), denominado aqui *conjuntos anonimato ativos de* v_c, que inclui apenas um único certificado digital por nível (ex.: para $m = 4$, $CERT^t_{AS_c} = \{cert_{1,3}, cert_{2,7}, cert_{3,1}, cert_{4,10}\}$).

4. Dois veículos arbitrários v_c e $v_{c'}$ pertencentes ao mesmo conjunto anonimato $AS_{1,j}$ (primeiro nível) não poderão pertencer a um mesmo conjunto anonimato de algum nível mais abaixo. Isto é[4], $\forall v_c, v_{c'} \in AS_{1,j},\ \exists\ i\ (\forall\ r\ (v_c \in AS_{i,r} \oplus v_{c'} \in AS_{i,r}))$ $\{i, j, r \in \mathbb{N} : 1 < i \leq m, 1 \leq j \leq n, 1 \leq r \leq n\}$. Consequentemente, pode-se deduzir que $CERT^t_{AS_c} - CERT^t_{AS_{c'}} \neq \emptyset$.

A fase de registro e autenticação é finalizada armazenando-se, no veículo, todas as chaves e certificados digitais definidos. Estes dados devem ser armazenados em um *chip* TPD, como ilustrado na Figura 4.3. Desta forma, o *chip* é responsável por, automaticamente, destruir os dados armazenados caso uma tentativa de acesso ou modificação não autorizadas sejam detectadas.

Ainda de acordo com a Figura 4.3, aplicações embarcadas em um veículo qualquer v_c podem solicitar a assinatura digital de uma mensagem m ao *chip* TPD, o qual retorna a mensagem m assinada digitalmente ($Sign(k^-_{c,i}, m)$, $0 \leq i \leq w$), bem como solicitar a validade da assinatura digital de uma mensagem m ($Verify(k^+_{a,i}, Sign(k^-_{a,i}, m))$ oriunda de um outro veículo v_a.

Ao término desta primeira fase, um veículo v_c está apto a enviar mensagens (periódica ou esporádica) numa rede VANET utilizando um dos pares de chaves TK_c para garantir autenticação e não-repúdio das mensagens. Entretanto, cada par de chaves terá uma validade temporal (ex.: 2 dias) e não poderá ser mais utilizado após este período. Desta forma, um veículo v_c poderá renovar os pares de chaves através de uma RSU disponível na via, cujo processo é realizado na Fase 2, como detalhado a seguir.

[4] O símbolo $\oplus$ representa a operação de "ou exclusivo".

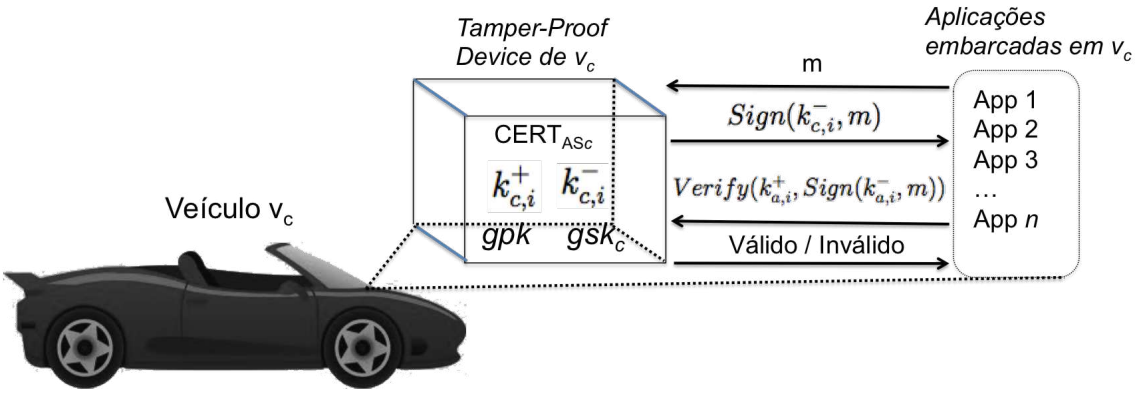


Figura 4.3: Chaves de criptografia e certificados digitais devem ser armazenados de forma segura em um *hardware* resiliente a alterações indevidas.

4.2.2 Fase 2: distribuição de identidades temporárias no protocolo *ASAP*-V.

A fase de registro de um veículo através de uma C.A garante que um veículo possa provar sua autenticidade a outras entidades à medida que se desloca nas vias. Após a fase de registro, a segunda fase do protocolo *ASAP*-V faz uso do modelo de pseudonimato para a distribuição de novas identidades aos veículos, visando prover anonimato a partir do uso de chaves de criptografia assimétrica como identidades temporárias. Para tal, qualquer veículo v_c negocia um novo conjunto de chaves temporárias TK_c através de uma RSU_q disponível ao longo da estrada. Esta fase é executada quando for necessário um veículo v_c renovar o conjunto de identidades TK_c.

Como pressuposto para a execução desta fase, o veículo v_c deve possuir uma identidade temporária $cert_{c,i}$ obtida na Fase 1, ou em alguma execução anterior desta Fase 2, como detalhado a seguir. Além disso, todos os nós da rede devem estar com os respectivos relógios devidamente sincronizados. O protocolo de negociação de chaves temporárias está ilustrado na Listagem 4.1 e é dividido em três etapas:

Listagem 4.1: Protocolo de negociação de identidades temporárias.

1 Etapa (1): Veículo v_c:
2 Etapa (1.1): $payload_c = cert_{c,i}||UUID_c$, $\sigma = Sign(gpk, gsk_c, payload_c)$
3 Etapa (1.2): $m_c = E(k^+_{RSU}, \sigma)$
4 Etapa (1.3): $v_c \Rightarrow RSU_q : m_c$
5 Etapa (2): RSU_q:
6 Etapa (2.1): $\sigma = D(k^-_{RSU}, m_c)$, Verify$(gpk, \sigma, payload_c)$
7 Etapa (2.2): Gera o conjunto TK_c de w pares de chaves temporárias e autentica
8 (assina) digitalmente cada par de chaves
9 Etapa (3): $RSU_q \Rightarrow v_c$: $E(k^+_{c,i}, TK_c||UUID_c)$

- **Etapa 1**: Ao detectar uma RSU_q ao longo da via, o veículo v_c requisita um conjunto de chaves temporárias TK_c. Inicialmente, v_c combina um certificado digital temporário válido $cert_{c,i}$ com um valor aleatório e único baseado no padrão UUID[5], assinando digitalmente com a chave secreta de grupo gsk_c, cujo processo gera a assinatura digital σ (Etapa 1.1). O valor $UUID_c$ é utilizado para evitar ataques de *homem do meio* (ver Seção 2.5.1). Por fim, o veículo gera a mensagem de requisição m_c cifrada com a chave pública da RSU_q (Etapa 1.2) e a transmite para a RSU_q (Etapa 1.3);

- **Etapa 2**: Esta etapa é dividida em duas sub-etapas:

  - **Etapa 2.1**: validação da requisição transmitida na etapa anterior: a RSU_q deve considerar a requisição como *válida* se, e somente se, ambas as condições a seguir forem satisfeitas: *i*) o *token* grt_c relacionado à chave de assinatura de grupo do veículo v_c não pertence à lista de *tokens* revogados (RL). A RL é periodicamente enviada pela C.A para as RSUs e este processo é detalhado na Seção 4.2.4; e *ii*) o intervalo de tempo entre o momento em que a mensagem é recebida nesta etapa (tmp) e o momento em que a requisição da Etapa 1 foi autenticada (tmp_σ), deve ser menor ou igual a um intervalo de tempo máximo pré-determinado ($threshold_{max}$). Para esta último condição, pretende-se detectar ataques de *reprodução* (ver Seção 2.5.1). Esta sub-etapa de validação de requisição, representada pela operação *Verify*, pode ser resumida formalmente como segue, onde σ é a assinatura digital da requisição m_c através do esquema de assinatura de grupo:

$$Verify(gpk, \sigma, payload_c) = valido \leftrightarrow grt_c \notin RL \wedge (tmp - tmp_\sigma \leq threshold_{max}) \tag{4.1}$$

  - **Etapa 2.2**: geração de identidades temporárias para o veículo v_c: caso o processo de verificação seja válido, a Etapa 2 prossegue para a segunda sub-etapa, onde a RSU_q é responsável por gerar um novo conjunto de identidades temporárias TK_c. As identidades são representadas por w pares de chaves temporárias ($k^+_{c,w}/k^-_{c,w}$) e os respectivos certificados digitais ($cert_{c,w}$). Cada certificado digital $cert_{c,i}$ é assinado digitalmente pela RSU_q para assegurar a autenticidade da respectiva chave pública $k^+_{c,i}$. Este processo pode ser resumido na Equação 4.2. Como consequência, tem-se $Signed^{cert_{c,i}}_{RSU}$.

[5]Acrônimo de *Universally Unique IDentifier* - ou identificador único universal -, uma cadeia de caracteres de 128 *bits* estruturada em 5 partes. Ex.: **de305d54-75b4-431b-adb2-eb6b9e546013**.

$$\forall k^{+}_{c,i} \in TK_c (1 \leq i \leq w), Sign(k^{-}_{RSU}, k^{+}_{c,i}) = cert_{c,i}. \quad (4.2)$$

- **Etapa 3**: Por fim, o conjunto de pares de chaves e respectivos certificados digitais $TK_c = \{(k^{+}_{c,1}/k^{-}_{c,1}, cert_{c,1}), (k^{+}_{c,2}/k^{-}_{c,2}, cert_{c,2}), ..., (k^{+}_{c,w}/k^{-}_{c,w}, cert_{c,w})\}$ é, então, enviado ao veículo v_c. Para permitir que apenas o veículo atual v_c tenha acesso às chaves temporárias TK_c geradas para ele, a RSU_n criptografa o conjunto TK_c com uma chave pública temporária ($k^{+}_{c,i}$) do veículo v_c extraído do certificado $cert_{c,i}$ recebido na Etapa 1. Cada certificado digital $cert_{c,i} \in TK_c$ possui um intervalo de tempo de validade representado por $tmp_{cert_{c,i}}$. Após este intervalo, o certificado digital $cert_{c,i}$ perderá sua validade. Ao receber o novo conjunto de pares de chaves TK_c, o veículo v_c aceita a resposta oriunda da RSU_q se, e somente se, $UUID_c$ transmitido na Etapa 1 é o mesmo recebido nesta Etapa 3.

Mensagens transmitidas por qualquer veículo v_c devem incluir os parâmetros de acordo com o formato detalhado na Figura 4.4. O campo *Evn* determina o tipo de mensagem (um evento) a ser transmitido, tais como periódico (*beacon*) ou esporádico; em seguida, o veículo adiciona um ou mais certificados digitais de conjunto anonimato aos quais pertence (mais detalhes na Seção 4.2.3); o próximo campo define a assinatura de grupo (σ) do parâmetro d, o qual pode representar a tupla $\langle vel_c, pos_c, dir_c \rangle$ (velocidade, posição e direção atuais, respectivamente, do veículo v_c) ou dados sobre um evento esporádico (ex.: frenagem brusca); prossegue-se incluindo também o certificado digital $cert_{c,i}$ da chave pública temporária $k^{+}_{c,i}$ cuja equivalente chave privada $k^{-}_{c,i}$ é utilizada para autenticar a mensagem m_c em questão ($Sign(k^{-}_{c,i}, m)$). Ademais, o certificado digital $cert_{c,i}$ representa a identidade atual do veículo v_c; e, por fim, inclui-se a marca de tempo tmp_{m_c} em que a mensagem m_c é gerada.

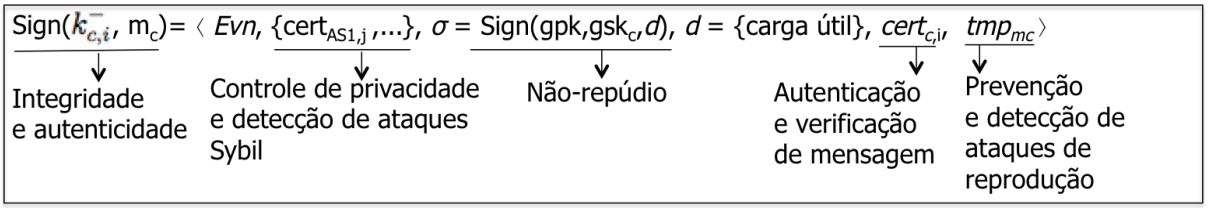


Figura 4.4: Representação do formato de mensagem para transmissão de eventos no protocolo *ASAP*-V.

É importante observar que cada campo da mensagem possui um requisito importante no processo de comunicação segura do protocolo *ASAP*-V. Enquanto a assinatura digital tem como objetivo central garantir a *integridade e a autenticidade* da mensagem m_c, os certificados digitais dos conjuntos anonimato visam garantir *controle de anonimato*

e detecção de ataques sybil (Fase 3), ao passo que a assinatura de grupo σ garante o *não-repúdio* da mensagem m_c e a marca de tempo tmp_{m_c} detecta potenciais *ataques de reprodução*.

Ao receber uma mensagem de um veículo v_c no formato descrito acima, um veículo v_b deve, inicialmente, verificar a autenticidade do certificado digital $cert_{c,i}$, bem como verificar a autenticidade da assinatura digital da mensagem m_c completa. A verificação da autenticidade de $cert_{c,i}$ é realizada a partir da chave pública das RSUs (k^+_{RSU}) disponível no certificado digital $cert_{RSU}$ (obtido na Fase 1). Objetiva-se determinar se o certificado $cert_{c,i}$ foi gerado e assinado digitalmente por uma RSU autêntica, bem como se o certificado ainda é válido no que tange o seu período de validade temporal. Esta verificação está formalizada na Equação 4.3.

$$Verify(k^+_{RSU}, cert_{c,i}) = valida \leftrightarrow Signed^{cert_{c,i}}_{RSU} \wedge (tmp - tmp_{cert_{c,i}} \leq threshold_{max}) \quad (4.3)$$

Uma vez válida, o veículo v_b verifica, então, a autenticidade da mensagem m_c a partir da chave pública $k^+_{c,i}$ disponível no certificado autêntico $cert_{c,i}$. Ademais, examina-se se a mensagem m_c foi gerada recentemente, ou seja, se m_c não é oriunda de um ataque de reprodução. Este processo de verificação está formalizado na Equação 4.4, como segue:

$$Verify(k^+_{c,i}, m_c) = valida \leftrightarrow Signed^{m_c}_{v_c} \wedge (tmp - tmp_{m_c} \leq threshold_{max}) \quad (4.4)$$

Convém destacar que se ao menos uma das verificações não seja satisfeita, a mensagem é descartada pelos nós receptores (ex.: pelo veículo v_b).

Com efeito, o uso de pseudônimos permite que um veículo v_c alterne entre os certificados digitais $cert_{c,i} \in TK_c$ a fim de evitar rastreamento e, consequentemente, uma quebra de anonimato. No protocolo *ASAP*-V, um veículo v_c pode alternar entre $cert_{c,i}$ e $cert_{c,i+1}$, e deve, quando possível, alterar o conjunto de certificados digitais atual de conjuntos anonimato ativos $CERT^t_{AS_c}$ para $CERT^{t+1}_{AS_c}$. Entretanto, tal mudança ocorre apenas δ_{CERT} segundos após a última alteração. O valor de δ_{CERT} dependerá de alguns fatores, tais como a velocidade e o deslocamento médio do veículo.

4.2.3 Fase 3: Detecção de ataques *sybil*

A terceira fase do protocolo *ASAP*-V forma o cerne da proposta deste trabalho e é concernente à detecção de ataques *sybil*, onde um veículo deliberadamente envia múltiplas mensagens com diferentes identidades para anunciar um mesmo *evento*.

Como pressuposto para a execução desta fase, parte-se de que um nó malicioso v_u, isto é, aquele que realiza um ataque *sybil* ($sybil_{v_u}$), é um veículo autêntico, ou seja, a

Fase 1 foi executada por ele e, consequentemente, possui um conjunto de identidades temporárias TK_u. Ademais, cada mensagem transmitida por v_u são logicamente válidas por nós receptores considerando as Equações 4.3 e 4.4 detalhadas na seção anterior.

Partindo da definição 4, um evento é aqui formalmente representado pela seguinte tupla:

$$Evn_e = \langle tmp_e, loc_e, evt_e \rangle,$$

em que:

- tmp_e é a marca de tempo em que o evento ocorreu;
- loc_e é o local de ocorrência do evento;
- $evt_e \in Evt$ é o tipo de evento ocorrido, onde Evt é o conjunto de todos os possíveis eventos que podem ocorrer numa rede VANET.

Detectar um ataque *sybil* apenas a partir dos atributos tmp_e, loc_e e evt_e pode ser relativo e depender das especificidades de cada tipo de evento. Como exemplo, considere o cenário onde dois veículos v_a e v_b transmitem os eventos Env_{e1} e Env_{e2}, respectivamente, e ambos os eventos apresentando frenagem brusca ($evt_{e1} = evt_{e2} = EEBL$). Ambos os veículos podem, naturalmente, transmitir os eventos com intervalos de tempo relativamente curtos ($|tmp_{e1} - tmp_{e2}| \leq 50\ ms$) e com localizações relativamente próximas ($2m \leq |loc_{e1} - loc_{e2}| \leq 5m$) ou distantes ($50m \leq |loc_{e1} - loc_{e2}| \leq 200\ m$). Entretanto, também é possível que os mesmos eventos sejam transmitidos por vários nós *sybil* gerados por um único veículo malicioso v_u.

Seguindo o mesmo raciocínio, se os eventos representam alerta de pista escorregadia ($evt_{e1} = evt_{e2} = RHCN$), o intervalo de tempo entre o anúncio dos dois eventos pode ser curto ($1ms \leq |tmp_{e1} - tmp_{e2}| \leq 50ms$) ou longo ($5s \leq |tmp_{e1} - tmp_{e2}| \leq 10s$), e possuir localizações iguais para informar o local exato do evento ($loc_{e1} = loc_{e2}$). Da mesma forma, ambas as mensagens podem ser transmitidas por dois diferentes veículos v_a e v_b, ou por um único veículo malicioso v_u.

Em uma outra vertente, considere um cenário onde n mensagens periódicas são recebidas com diferentes marcas de tempo ($tmp_{e1} \neq tmp_{e2}, ... \neq tmp_{en}$), com diferentes localizações ($loc_{e1} \neq loc_{e2}, ...loc_{en}$) e sob o tipo de evento *beacon* ($evt_{e1} = evt_{e2} = evt_{en} =$ *beacon*). De forma análoga, tais mensagens podem ser recebidas com marcas de tempo $tmp_{e1} \neq tmp_{e2}, ... \neq tmp_{en}$ relativamente próximas (ex.: $|tmp_i - tmp_j| \leq 10ms$), porém, com localizações relativamente distantes ($50m \leq |loc_{ei} - loc_{ej}| \leq 200m$). Em ambos os casos, é possível que tais mensagens sejam oriundas de dois ou mais veículos distintos, ou de um único veículo malicioso v_u. Como consequência, pode-se observar que apenas

a partir dos atributos tmp_e, loc_e e evn_e não é possível determinar um potencial ataque *sybil*.

Nas seções a seguir, é detalhado o mecanismo de detecção de ataques *sybil* do protocolo *ASAP*-V. A abordagem utilizada é capaz de detectar ataques tanto através de mensagens com eventos esporádicos, tanto quanto através de mensagens periódicas, visando oferecer também o suporte ao controle de anonimato dos usuários.

Detecção de Ataques *sybil* em mensagens periódicas

A detecção de ataques *sybil* no protocolo *ASAP*-V faz uso da arquitetura de conjuntos anonimato em múltiplos níveis introduzida na Seção 4.2.1 (Fase 1). A abordagem para detectar ataques *sybil* em mensagens periódicas é um processo executado de forma dinâmica e distribuído entre os veículos de uma região específica, não fazendo-se necessária a participação direta de uma infraestrutura fixa, tais como C.A ou RSUs.

Em geral, o processo de detecção de ataques *sybil* visa garantir que mensagens que descrevem o mesmo evento, e são oriundas de diferentes identidades, não apresentem o mesmo conjunto de certificados digitais de *conjunto anonimato ativos*. Formalmente, do ponto de vista de um veículo v_x este processo deve satisfazer a Equação 4.5.

$$\forall(v_c, v_{c'}) \in E_x(\, |CERT^t_{AS_c}| = |CERT^t_{AS_{c'}}| \wedge CERT^t_{AS_c} - CERT^t_{AS_{c'}} \neq \emptyset) \tag{4.5}$$

O processo de detecção de ataques *sybil* explorados em mensagens periódicas é descrito a partir do cenário ilustrado na Figura 1.7, o qual está representado um ataque *sybil* baseado em mensagens periódicas pelo veículo v_e, criando dois novos nós *sybil* v_{e_1} e v_{e_2}.

Como exemplo, considere os veículos v_c, v_e e v_f ilustrados na figura. Suponha também que v_e é um veículo malicioso e faz uso de três identidades para executar um ataque *sybil* no intervalo de tempo tmp_1, ao passo que os veículos v_c e v_f são legítimos e fazem uso de uma única identidade para transmissão de mensagens periódicas.

Considere também que os veículos utilizam os seguintes certificados digitais de *conjuntos anonimato ativos* para 5 níveis ($m = 5$): $CERT^t_{AS_e} = \{cert_{AS_{1,2}}, cert_{AS_{2,4}}, cert_{AS_{3,2}}, cert_{AS_{4,6}}, cert_{AS_{5,1}}\}$, $CERT^t_{AS_c} = \{cert_{AS_{1,2}}, cert_{AS_{2,4}}, cert_{AS_{3,2}}, cert_{AS_{4,4}}, cert_{AS_{5,2}}\}$, $CERT^t_{AS_f} = \{cert_{AS_{1,4}}, cert_{AS_{2,7}}, cert_{AS_{3,2}}, cert_{AS_{4,7}}, cert_{AS_{5,8}}\}$. Evidentemente, como detalhado nas Definições 1 e 2, os veículos v_e, v_c e v_f formam uma rede VANET tal que:

- $E_e = \{(v_e, v_a), (v_e, v_b), (v_e, v_c), (v_e, v_d), (v_e, v_f), (v_e, v_g)\}$;
- $E_c = \{(v_c, v_a), (v_c, v_b), (v_c, v_d), (v_c, v_e), (v_c, v_f), (v_c, v_g), \boldsymbol{(v_c, v_{e_1})}, \boldsymbol{(v_c, v_{e_2})}\}$;
- $E_f = \{(v_f, v_a), (v_f, v_b), (v_f, v_c), (v_f, v_d), (v_f, v_e), (v_c, v_g), \boldsymbol{(v_f, v_{e_1})}, \boldsymbol{(v_f, v_{e_2})}\}$.

Desta forma, pode-se observar que para os veículos v_c e v_f, há dois veículos (possivelmente) legítimos com identidades v_{e_1} e v_{e_2}. Para detectar os nós *sybil* v_{e_1} e v_{e_2}, faz-se necessário analisar os certificados digitais dos conjuntos anonimato incluídos nas mensagens. Este processo é detalhado no diagrama de sequência ilustrado na Figura 4.5.

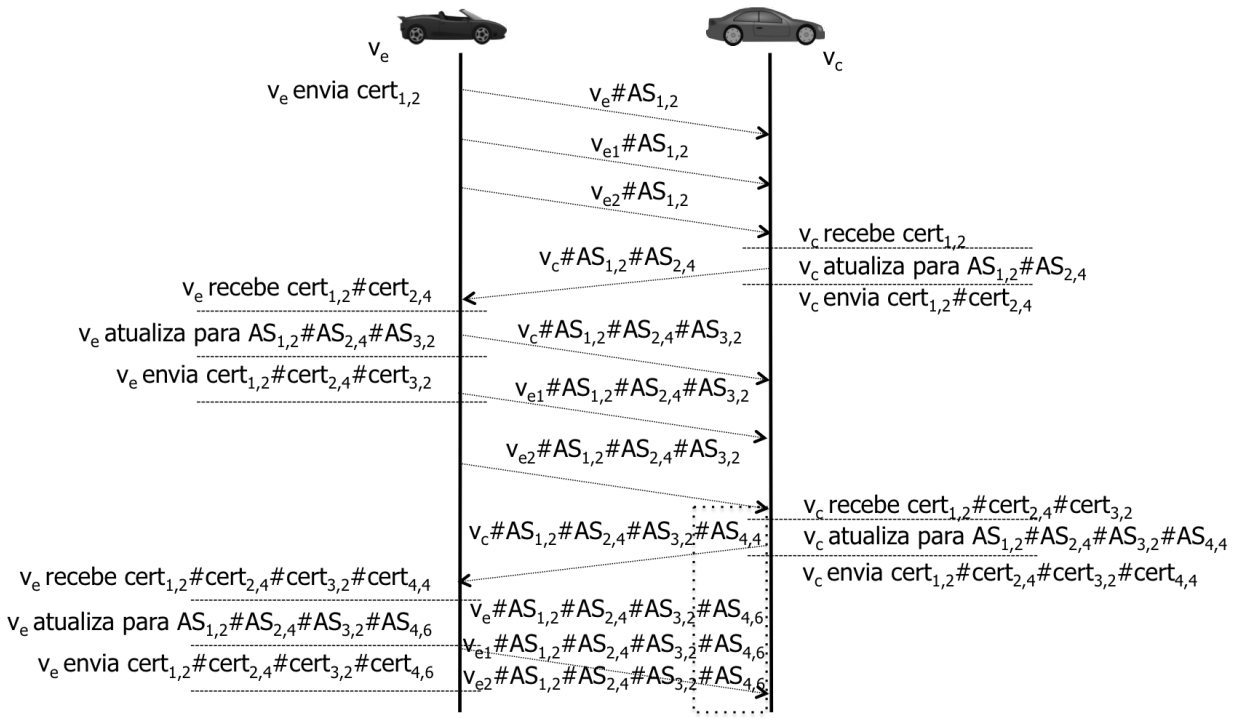


Figura 4.5: Representação da detecção de ataque *sybil* oriundo de mensagens periódicas.

O veículo malicioso v_e, ao transmitir mensagens periódicas com diferentes identidades (v_e, v_{e_1} e v_{e_2}), inclui também o certificado digital do conjunto anonimato ativo de primeiro nível, neste caso, $AS_{1,2}$. Ao receber tais mensagens, um veículo que também estiver transmitindo mensagens periódicas com o mesmo certificado digital do conjunto anonimato de primeiro nível, neste caso, v_c, deve atualizar e incluir o certificado digital do conjunto anonimato de segundo nível. Logo, o veículo v_c inclui o certificado digital do conjunto anonimato $AS_{2,4}$ e o transmite à rede.

Da mesma forma, para que o ataque *sybil* continue ativo, o veículo malicioso deve adicionar um certificado do nível logo abaixo que o diferencie de qualquer outro veículo na rede. Assim, o veículo malicioso v_e adiciona os certificados digitais dos conjuntos de segundo e terceiro níveis, $AS_{2,4}$ e $AS_{3,2}$, respectivamente. Igualmente, ao receber uma mensagem a qual inclui os mesmos certificados digitais ativos, o veículo v_c atualiza e adiciona os certificados digitais dos conjuntos anonimato $AS_{3,2}$ e $AS_{4,4}$. Finalmente, ao receber a mensagem oriunda de v_c, o veículo malicioso deve incluir o certificado digital do conjunto anonimato $AS_{4,6}$.

Neste momento, a partir do certificado digital de quarto nível, a última mensagem

periódica do veículo v_c satisfaz a Equação 4.5 para qualquer par de nós comunicantes em E_c, ao passo que mensagens oriundas de um nó malicioso, ao executar um ataque *sybil* contêm os mesmos certificados digitais de conjuntos anonimato ativos.

Em linhas gerais, se dois ou mais veículos pertencentes ao mesmo conjunto anonimato também estiverem no mesmo conjunto anonimato do nível logo abaixo, inclui-se um novo certificado digital de conjuntos anonimato ativos. Entretanto, é importante observar que este procedimento ocorre apenas se diferentes veículos v_i e v_j, no mesmo raio de transmissão, isto é $(v_i, v_j) \in E$, estão necessariamente no mesmo conjunto anonimato do primeiro nível, ou seja, $cert_{AS_{1,k}} \in CERT^t_{AS_i} = cert_{AS_{1,k}} \in CERT^t_{AS_j} (1 \leq k \leq n)$. Como exemplo, é possível deduzir que mensagens oriundas dos veículos v_c e v_f pertencem a nós legítimos, uma vez que tais mensagens contêm certificados digitais de diferentes conjuntos anonimato de primeiro nível ($AS_{1,2}$ e $AS_{1,4}$).

Retornando ao exemplo em questão, para detectar que o veículo v_e é um veículo malicioso, faz-se necessário que os demais veículos no raio de transmissão aguardem um intervalo de tempo máximo $\delta_{AS_{1,j}}$ para que um próximo certificado digital do conjunto anonimato ativo seja incluído pelo veículo v_e nas mensagens suspeitas (mensagens com identidades v_e, v_{e_1} e v_{e_2}). Tais mensagens ainda possuem certificados de conjuntos anonimato iguais e não satisfazem a Equação 4.5.

Esse procedimento se faz necessário pois, do ponto de vista dos demais veículos no raio de transmissão, é impossível inferir se tais mensagens são oriundas de um único veículo (v_e), ou originadas de diferentes veículos, porém pertencentes aos mesmos conjuntos anonimato $AS_{1,2}$, $AS_{2,4}$, $AS_{3,2}$, $AS_{4,6}$. Caso um próximo certificado digital do próximo nível não seja incluído por v_e em até $\delta_{AS_{1,2}}$ *ms*, então todos os nós vizinhos podem inferir que as mensagens com identidades v_e, v_{e_1} e v_{e_2} são provenientes de um potencial veículo malicioso (v_e). Esse tempo de espera é calculado por um veículo avaliador presente no raio de transmissão (ex.: v_f) para um dado conjunto anonimato de primeiro nível $AS_{1,j}$, como proposto através da Equação 4.6:

$$\delta_{AS_{1,j}} = t_{beacon} + (m - pm) * \frac{N_{v_x,l}}{m} \tag{4.6}$$

em que:

- $N_{v_a,l}$ é o número de veículos vizinhos em que um veículo arbitrário v_a detectou numa região l (raio de transmissão), ou seja, $N_{v_a,l} = |E_{v_a}| - 1$;
- t_{beacon} é o período com que veículos na região l transmitem mensagens periódicas na rede;
- m é a quantidade máxima de níveis de conjuntos anonimato registrados na C.A;

- pm é a quantidade de certificados digitais de conjuntos anonimato ativos já transmitidos em l em mensagens consideradas suspeitas como oriundas de um nó *sybil*; e,

- $\delta_{AS_{1,j}}$ é o intervalo de tempo máximo em que um veículo v_a deverá aguardar até receber novas mensagens periódicas com novos certificados digitais de conjuntos anonimato ativos tal que o certificado digital do conjunto anonimato $AS_{1,j}$ já esteja presente.

Está definido na Equação 4.6 um comportamento no qual o tempo de espera $\delta_{AS_{1,j}}$ deve aumentar quanto maior for o número de veículos no raio de transmissão (N_{v_i}), e deve diminuir paulatinamente à medida que novos certificados digitais de conjuntos anonimato (pm) são apresentados nas mensagens periódicas. Desta forma, é possível lidar com eventuais atrasos ocasionados por disputas de acesso ao meio, e minimizar a duração de um possível ataque *sybil*.

O tempo de espera $\delta_{AS_{1,j}}$ é reinicializado a cada novo certificado digital de conjunto anonimato enviado pelos veículos v_e e v_c. Entretanto, após o veículo malicioso apresentar seus certificados digitais de todos os níveis, o tempo $\delta_{AS_{1,j}}$ do nó avaliador é atingido e este pode deduzir que as mensagens com os mesmos certificados digitais de conjuntos anonimato são oriundas de um nó malicioso.

Em cenários onde ocorre desvanecimento da força dos sinais transmitidos entre os nós comunicantes, o protocolo $ASAP$-V pode concluir falsos ataques *sybil* (detecções falso-positivos), como ilustrado no cenário da Figura 4.6. As localizações dos veículos v_a e v_c são tais que as potências de seus sinais de transmissão não são suficientes para que eles detectem as transmissões de um e de outro, mas, mesmo assim, são suficientemente fortes para alcançar v_b.

Como consequência, se v_a e v_c transmitem mensagens periódicas utilizando certificado digital do mesmo conjunto anonimato de primeiro nível em um instante t, isto é, $AS_{1,j} \in CERT^t_{AS_a}$ e $AS_{1,j} \in CERT^t_{AS_c}$, então a Equação 4.5 não será satisfeita do ponto de vista do veículo v_b, uma vez que v_a e v_c não deverão incluir os certificados digitais dos conjuntos anonimato dos níveis abaixo aos quais cada um pertence.

Desta forma, para evitar o cenário descrito anteriormente, um veículo v_b deve inicialmente determinar se a potência dos sinais de transmissão dos veículos v_a e v_c não são fortes o suficiente para alcançarem um ao outro. Para tal, considere P_{a,pos_b} e P_{c,pos_b} as potências dos sinais de transmissão dos veículos v_a e v_c, respectivamente, detectadas na posição do veículo v_b. Para que o veículo v_b possa estimar se o veículo v_c recebe mensagem do veículo v_a, e igualmente, se v_a recebe mensagem de v_c, faz-se necessário estimar as potências de ambos os sinais transmitidos após se propagarem para ambos os lados, isto

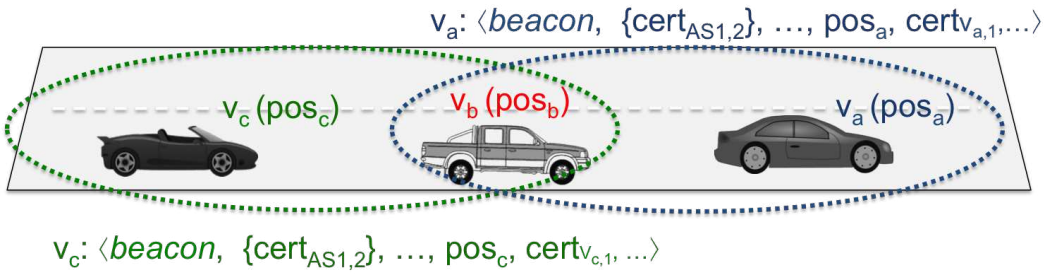


Figura 4.6: Veículos v_a e v_c transmitem mensagens periódicas incluindo o mesmo certificado digital de conjunto anonimato de primeiro nível ($cert_{AS_{1,2}}$). Devido ao desvanecimento da força dos sinais transmitidos pelos veículos v_a e v_c, o protocolo *ASAP*-V pode detectar falsos ataques *sybil* (detecção *falso-positivo*).

é, a potência do sinal transmitido por v_a na posição do veículo v_c (P_{a,pos_c}) e a potência do sinal transmitido por v_c na posição do veículo v_a (P_{c,pos_a}). Assim, deve-se determinar se $P_{a,pos_c} < P_{min}$ e $P_{c,pos_a} < P_{min}$, em que P_{min} é a potência mínima para que uma mensagem periódica seja recebida. Na Seção 4.3.1, é detalhada uma abordagem simples para estimar as potências P_{a,pos_c} e P_{c,pos_a}.

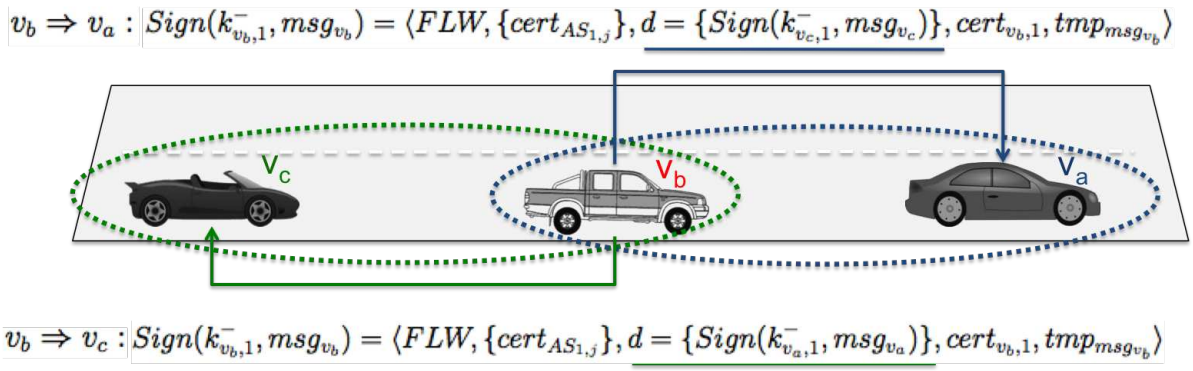


Figura 4.7: Veículo v_b transmite mensagem de *sinalização de primeiro nível* aos veículos v_a e v_c.

Com efeito, se um veículo v_b detectar que v_a e v_c não recebem mensagens entre si, então o veículo v_b deve enviar uma mensagem *broadcast* denominada *sinalização de primeiro nível*, representada por FLW (do inglês *First Level Warning*), aos veículos v_a e v_c, como ilustrado no cenário da Figura 4.7. Mensagens FLW são endereçadas aos veículos que têm transmitido mensagens contendo os mesmos certificados digitais de conjunto anonimato. Cada mensagem inclui uma cópia da mensagem periódica pertencente ao outro veículo, isto é, o veículo v_a recebe uma cópia da mensagem de v_c, e o veículo v_c recebe uma cópia da mensagem pertencente ao veículo v_a, representadas pelo campo de dados d. É ilustrado na Figura 4.8, o processo de execução relacionado ao cenário da Figura 4.7, na qual v_b detecta dois veículos legítimos v_a e v_c após receber mensagens periódicas com certificados

digitais de conjuntos anonimato de quarto nível distintos entre si.

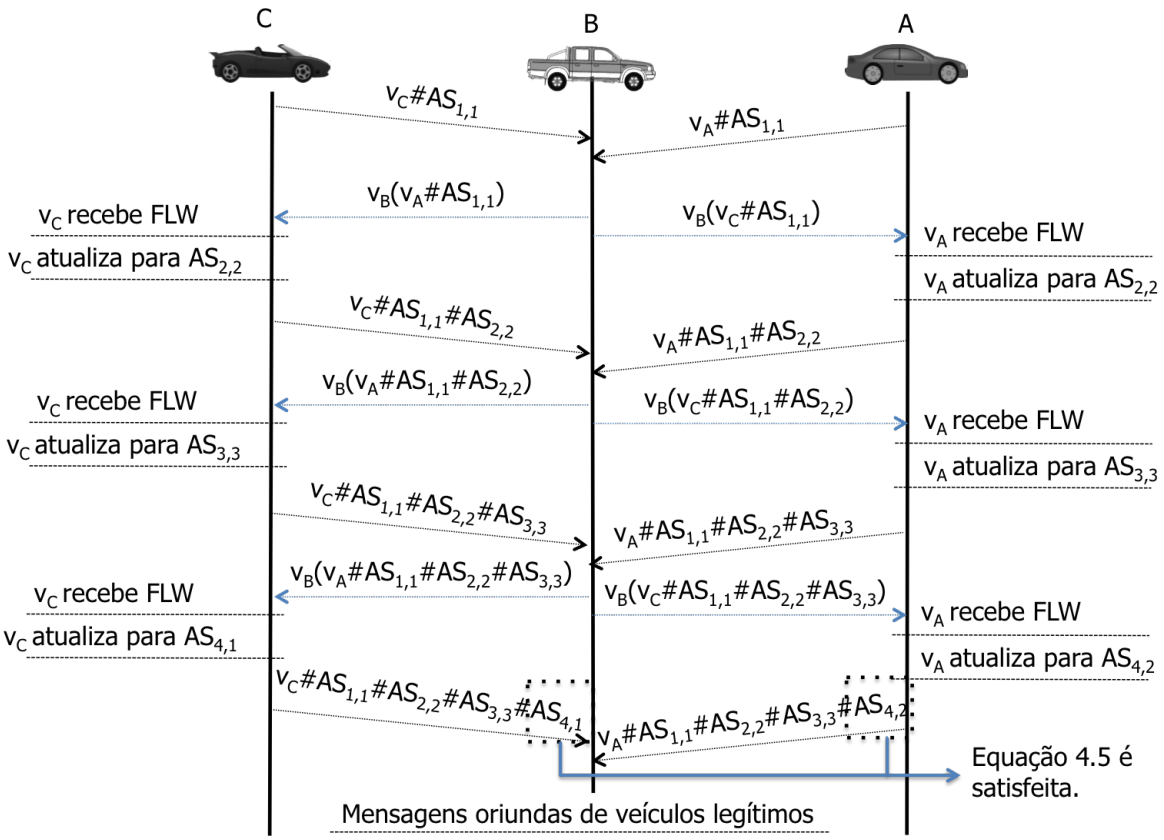


Figura 4.8: Veículo v_b transmite mensagens de *sinalização de primeiro nível* aos veículos v_a e v_c. Após receber mensagens com certificado digital de conjunto anonimato do quarto nível ($m = 4$), v_b detecta que mensagens são oriundas de dois veículos legítimos.

Entretanto, a quantidade de mensagens FLW pode dobrar à medida que se tem um número maior de veículos na região. Como exemplo, se outros dez veículos estiverem posicionados próximos ao veículo v_b, de tal forma que caracterize o cenário de desvanecimento da força de sinal entre os veículos v_a e v_c, a quantidade de mensagens FLW transmitidas na região deverá chegar a vinte.

Assim, para minimizar a quantidade de mensagens transmitidas na rede e, ao mesmo tempo, visando manter a confiabilidade do protocolo na fase de detecção de ataques *sybil*, propõe-se que apenas um subconjunto mínimo de veículos selecionados aleatoriamente transmitam mensagens FLW.

Para tal, cada veículo decide, localmente, se deve ou não enviar mensagens FLW a partir da Equação 4.7, a qual leva em consideração três informações de contexto sobre a rede VANET, sobre o sistema, e sobre o ambiente em que o veículo está inserido, a saber: a quantidade de veículos vizinhos na região (N_{v_b}); a quantidade de vezes em que mensagens periódicas recebidas pelo veículo v_b possuem o mesmo conjunto de certificados ativos de conjuntos anonimato ($m_{cert_{AS}}$); e a quantidade de níveis de conjuntos anonimato

definidos no sistema SV (m).

$$threshold_{min} = [1 - \frac{1}{N_{v_b}}] - [m_{cert_{AS}} * (\frac{m}{100})] \tag{4.7}$$

A partir desses dados, define-se uma janela de transmissão, ou intervalo de transmissão, $\zeta = [threshold_{min}, 1]$ em que, escolhendo-se um valor real aleatório $x_{v_b,r}$ $(0 \leq x_{v_b,r} \leq 1)$, um veículo v_b será um candidato ao envio de mensagens FLW se $threshold_{min} \leq x_{v_b,r} \leq 1$. Se escolhido como candidato para envio de mensagens FLW, um veículo v_b deve ainda aguardar um intervalo de tempo aleatório de espera t_{wait} antes de enviar a mensagem FLW. Este intervalo é definido tomando-se como base a diferença entre o intervalo t_{beacon} e a maior marca de tempo tmp_{m_X} $(x = v_a \oplus x = v_c)$ das duas últimas mensagens *beacon* entre v_c e v_a, ou seja, $t_{wait} = t_{beacon} - \max(tmp_{m_{v_a}}, tmp_{m_{v_c}})$. Justifica-se esta abordagem pois, caso v_b observe que outro veículo tenha transmitido a mensagem FLW, v_b poderá abortar a transmissão de sua mensagem FLW em questão e, consequentemente, evitar o envio demasiado de mensagens FLW na rede.

A janela de transmissão ζ deve aumentar à medida que os certificados digitais ativos recebidos nas mensagens periódicas de v_a e v_c permanecem os mesmos. Como exemplo, considere novamente o cenário da Figura 4.6. Considere também que há 10 veículos v_x $(1 \leq x \leq 10)$, vizinhos ao veículo v_b, de tal forma que todos estejam em conjuntos anonimato diferentes de v_a, v_c. Ainda para este cenário, considere que há 6 níveis de conjuntos anonimato definidos no sistema SV $(m = 6)$.

Ao receber, pela primeira vez, uma mensagem periódica oriunda de cada veículo v_a e v_c, os veículos v_b e v_x deverão definir $threshold_{min} = 0.84$ (para $m_{cert_{AS}} = 1$) e, consequentemente, tem-se janela de transmissão FLW $\zeta = [0.84, 1]$. Tais veículos serão candidatos ao envio de mensagens FLW se, e somente se, $0.84 \leq x_{v_x,r} \leq 1$. Supondo que ao menos 1 par de mensagem FLW seja enviada com sucesso - ou seja, algum veículo v_x transmitiu aos veículos v_a e v_c uma mensagem FLW -, então os veículos v_a e v_c deverão incluir o certificado digital do conjunto anonimato de segundo nível. Se v_a e v_c enviarem mensagens periódicas com certificado digital de segundo nível também iguais, então os veículos v_b e v_x devem manter $threshold_{min} = 0.84$ (para $m_{cert_{AS}} = 1$) e o processo é repetido. Por outro lado, caso nenhuma mensagem FLW seja enviada, então v_b e v_x deverão considerar $m_{cert_{AS}}$ e, consequentemente, $threshold_{min} = 0.78$ e $\zeta = [0.78, 1]$. Este processo deve se repetir à medida que novos certificados digitais de conjuntos anonimato permanecem iguais entre os veículos v_a e v_c.

Detecção de ataques *sybil* em mensagens esporádicas

As mensagens esporádicas são normalmente transmitidas para anunciar eventos tais como pistas interditadas, escorregadias, frenagens bruscas, aproximação de veículos de

emergência etc., e tendem a ser propagadas na rede apenas uma única vez por veículo. Nessa perspectiva, a abordagem do protocolo *ASAP*-V para detectar ataques *sybil* reside basicamente na propriedade 4 da arquitetura de conjuntos anonimato em múltiplos níveis. Nesse contexto, é impossível dois ou mais veículos pertencerem exatamente aos mesmos conjuntos anonimato $AS_{1,j}$ à $AS_{m,n}$ para quaisquer quantidades de veículos e conjuntos anonimato por nível. Consequentemente, sabe-se que não há ataque *sybil* oriundo de mensagens esporádicas se a Equação 4.5 for satisfeita.

Desta forma, duas ou mais mensagens esporádicas com diferentes identidades não poderão incluir exatamente os mesmos m certificados digitais de conjuntos anonimato $cert_{AS_{1,j}} \wedge cert_{AS_{2,q}} \wedge ... \wedge cert_{AS_{m,n}}$. Ou seja, um veículo v_c, ao anunciar uma mensagem sobre algum evento esporádico em um tempo t, inclui na mensagem esporádica todos os certificados digitais ativos $CERT^t_{AS_c}$ de cada conjunto anonimato ao qual pertence.

Como exemplo, considere o cenário ilustrado na Figura 1.6. O processo de detecção de ataques *sybil* oriundos de eventos esporádicos é ilustrado na Figura 4.9. Mensagens RHCN são detectadas como oriundas de um mesmo veículo pois contêm certificados digitais idênticos para o mesmo evento.

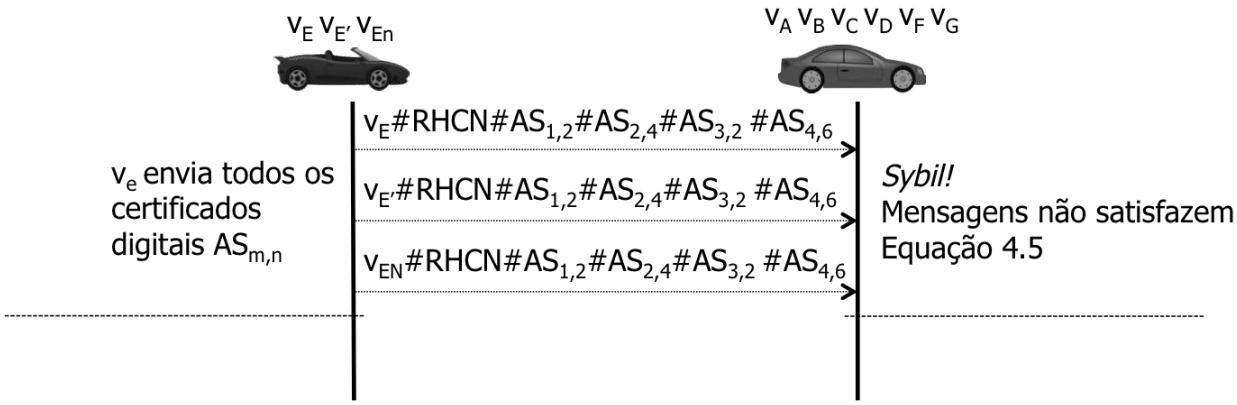


Figura 4.9: Representação de detecção de ataque *sybil* oriundo de mensagens esporádicas.

4.2.4 Fase 4: Acusação de detecção de ataques *sybil*

Finalmente, a última fase do protocolo *ASAP*-V permite que os veículos que detectaram um potencial ataque *sybil* possam denunciar um veículo malicioso a uma C.A. Nesta perspectiva, objetiva-se excluir (talvez temporariamente) o veículo *sybil* da rede para impedir que este continue realizando ataques maliciosos.

Para a execução desta fase, tem-se como pressuposto que um veículo v_i detectou um potencial ataque *sybil* e possui, armazenado localmente, um conjunto de n mensagens suspeitas $M_{c,n}$ de um potencial veículo malicioso v_c.

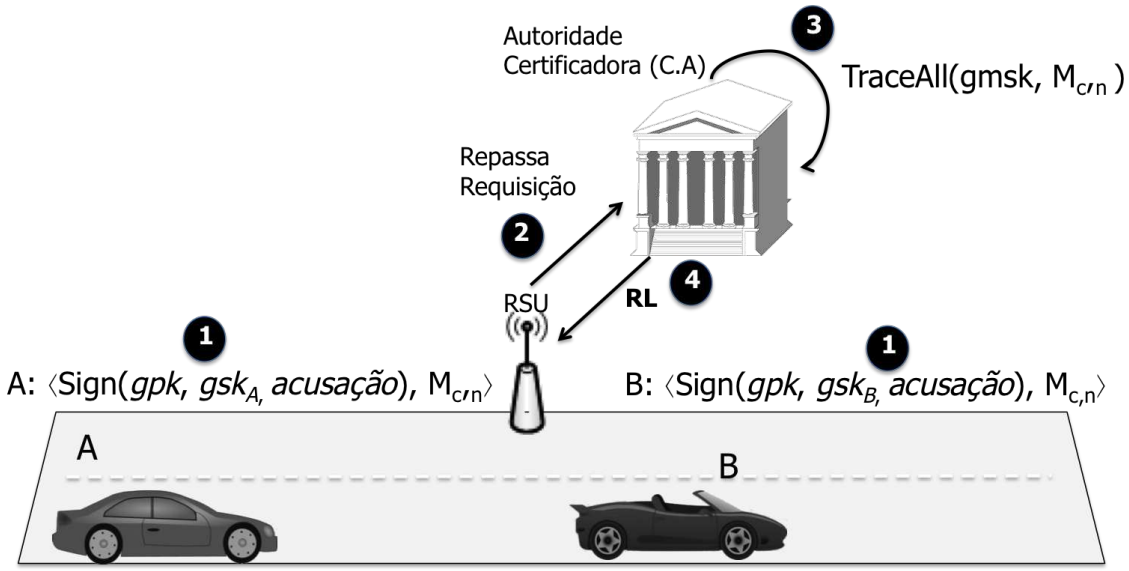


Figura 4.10: Representação de notificação de ataques *sybil* no protocolo *ASAP*-V.

A fase de acusação pode ser resumida através do cenário ilustrado na Figura 4.10. Ao detectar mensagens oriundas de um potencial veículo *sybil* v_c, cada veículo poderá gerar uma requisição de acusação para uma RSU informando as n mensagens recebidas durante o ataque (Passo 1). Neste passo, um veículo autentica uma requisição de acusação através do esquema de assinatura de grupo e inclui cópias das n mensagens suspeitas detectadas. Em seguida, a RSU apenas repassa a requisição para a C.A (Passo 2), a qual determina se as mensagens são oriundas de um ataque *sybil* a partir da verificação das assinaturas de grupo σ_n de cada mensagem m_c presente em $M_{c,n}$ (Passo 3, *TraceAll*).

Esta verificação ocorre a partir da chave de gerenciamento de grupos *gmsk*. Ou seja, a partir de quaisquer assinaturas de grupo σ, é possível determinar a real identidade da entidade que originou σ. Nesse contexto, um veículo v_c é considerado *sybil* se, e somente se, para cada mensagem $m_{c,i}$ presente em $M_{c,n}$ $(1 \leq i \leq n)$, todas as mensagens $m_{c,i}$ descrevem um mesmo evento *evt* e o veículo v_c $(sybil_{v_c})$ é responsável pela geração da assinatura de grupo σ_n presente em cada mensagem $m_{c,i}$. Formalmente, esta verificação é representada como segue:

$$\begin{aligned} TraceAll(gmsk, M_{v_c,n}) = \forall m_i, m_j \in M_{v_c,n}, (evt_i \in m_i = evt_j \in m_j) \wedge \\ (Signed_{v_c}^{\sigma_i} \wedge Signed_{v_c}^{\sigma_j}) \leftrightarrow sybil_{v_c}\{i, j, n \in \mathbb{N} : 1 \leq i \leq n, 1 \leq j \leq n, i \neq j\} \end{aligned} \tag{4.8}$$

Em caso de confirmação de que o veículo v_c executou um ataque *sybil*, o *token* grt_c do esquema de assinatura de grupo do veículo v_c é adicionado à lista de *tokens* revogados RL e, em seguida, distribuída para as RSUs (Passo 4). A partir deste momento, o veículo *sybil* v_c não poderá obter novos conjuntos de identidades temporárias (Fase 2, Etapa 2 do protocolo), impedindo-o de enviar futuras mensagens autênticas na rede.

O *token* grt_c, de um veículo v_c é derivado a partir de uma segunda chave de rastreamento que está armazenada em cada RSU. Este modelo é proposto por Boneh et. al. [189] e permite checar se uma mensagem é oriunda de uma entidade e cujo *token* grt_e está incluído na lista RL. Caso o *token* grt_e não esteja incluído em RL, então é impossível determinar a identidade de e. Desta forma, garante-se o anonimato de mensagens transmitidas para as RSUs.

4.3 Execução do Protocolo *ASAP*-V

Nesta seção, são detalhados os procedimentos realizados pelo protocolo *ASAP*-V durante o processo de detecção de ataques *sybil* (Fase 3). A execução do protocolo é modelada através de Máquinas de Estados Finito (FSM, do inglês *finite-state machine*), destacando-se também os procedimentos executados através de pseudo-algoritmos.

4.3.1 Modelagem Fomal de Execução do Protocolo *ASAP*-V

As FSM descritas nesta seção seguem um padrão adotado por Kurose et al. [190] e proposto inicialmente por Bochmann et al. [191], como exemplificado na Figura 4.11. A seta na descrição da FSM indica a transição do protocolo de um estado para outro. O evento causador da transição é mostrado acima da linha horizontal que a rotula, ao passo que as ações realizadas quando ocorre tal evento são apresentadas abaixo dessa linha. Por fim, o estado inicial é indicado pela seta tracejada.

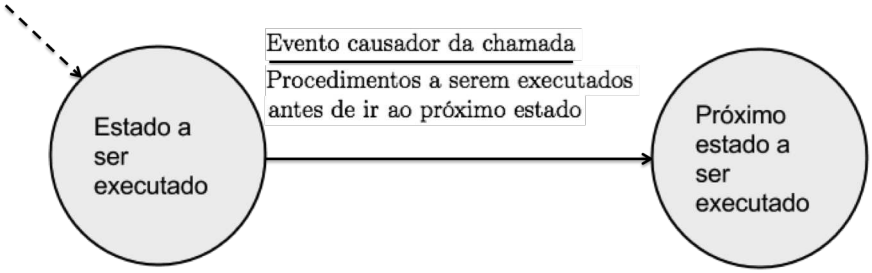
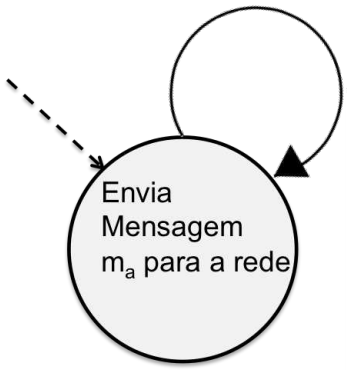


Figura 4.11: Modelo da máquina de estados finito utilizado para descrição de cenários de execução do protocolo *ASAP*-V.

As definições da FSM para um veículo transmissor e para um veículo receptor são ilustradas nas Figuras 4.12 e 4.13, respectivamente. A FSM do transmissor tem apenas um único estado principal, embora possa executar um estado concorrente a ele. Por outro lado, a FSM do receptor tem quatro estados principais e dois concorrentes. Estados concorrentes do transmissor e do receptor são detalhados à medida que é descrito o funcionamento do protocolo *ASAP*-V.

Considere a FSM ilustrada na Figura 4.12. Um veículo transmissor v_a, ao observar o canal de transmissão ocioso - isto é, nenhum outro nó está transmitindo no canal de controle - poderá transmitir dois tipos de mensagens: periódica ou esporádica. No primeiro caso, após o intervalo da última mensagem transmitida, v_a obtém os dados geográficos atuais d (Linha 2) - incluindo velocidade, direção e posição; assina digitalmente tais dados com o esquema de assinaturas de grupo (Linha 3); gera a mensagem periódica m_a a ser transmitida (Linha 4); assina a mensagem m_a com uma chave privada temporária $k^-_{a,i}$ (Linha 9) e a envia à rede através do canal de controle (Linha 10). Este processo é repetido à medida que o intervalo para transmissão de mensagens periódicas seja alcançado e nenhum outro veículo esteja transmitindo.



beacon *timeout* ou novo evento, e canal ocioso

1 **if** *beacon* **then**
2 $\quad d \leftarrow get\_gps\_data()$;
3 $\quad \sigma_a \leftarrow Sign(gpk, gsk_a, d)$;
4 $\quad m_a \leftarrow evt.beacon||cert_{AS_{i,j}} \in CERT^t_{AS_a}||\sigma_a||d||cert_{a,i}||tmp_{m_a}$;
5 **else**
6 $\quad Evn \leftarrow get\_sensed\_event\_data()$;
7 $\quad \sigma_a \leftarrow Sign(gpk, gsk_a, Evn.d)$;
8 $\quad m_a \leftarrow Evn.evt||CERT^t_{AS_a}||\sigma_a||Evn.d||cert_{a,i}||tmp_{m_a}$;
9 $m_a \leftarrow Sign(k^-_{a,i}, m_a)$;
10 $send(m_a)$;

Figura 4.12: Procedimentos realizados por um veículo remetente v_a ao transmitir mensagens periódicas.

Uma mensagem periódica m_a é construída como detalhada na Linha 4. Inicialmente inclui-se uma *flag beacon* para caracterizar uma mensagem periódica; em seguida, um ou mais certificados digitais $cert_{AS_{i,j}} \in CERT^t_{AS_a}$ de conjuntos anonimato são adicionados, conforme detalhado na Seção 4.2.3; prossegue-se adicionando uma assinatura digital (σ_a) dos respectivos dados geográficos (d), bem como o i-ésimo certificado digital temporário $cert_{a,i} \in K_a$, cuja principal função é permitir que veículos receptores verifiquem a autenticidade da mensagem, como discutido na Seção 4.2.2; e, por fim, adiciona-se a marca de tempo tmp_{m_a} da mensagem gerada. É importante destacar que os procedimentos descritos nas Linhas 3, 4 e 9 são realizados pelo módulo TPD presente em cada veículo, garantindo, assim, a segurança das chaves de criptografia.

Um veículo v_a pode transmitir uma mensagem de evento esporádico conforme detalhado entre as Linhas 6 e 8. Inicialmente, v_a obtém os dados capturados sobre o evento e assina digitalmente com uma chave de grupo (Linhas 6 e 7). Em seguida constrói a mensagem m_a adicionando-se todos os certificados digitais de conjuntos anonimato, a assinatura

digital sobre o evento e os dados sobre o evento, bem como o enésimo certificado digital $cert_{a,i} \in K_a$ e a marca de tempo tmp_{m_a} (Linha 8). Da mesma forma, os procedimentos de assinatura digital sobre o evento esporádico (Linha 7) e da construção e assinatura digital da mensagem m_a (Linha 8) são realizados pelo TPD.

A FSM principal de um veículo receptor v_a é ilustrada na Figura 4.13. No estado inicial, ao receber uma mensagem m_b de um veículo v_b, o veículo v_a determina inicialmente o tipo da mensagem e direciona a execução para um dos três principais estados, a saber: processamento de mensagens periódicas; processamento de mensagens de eventos esporádicos; e processamento de mensagens FLW.

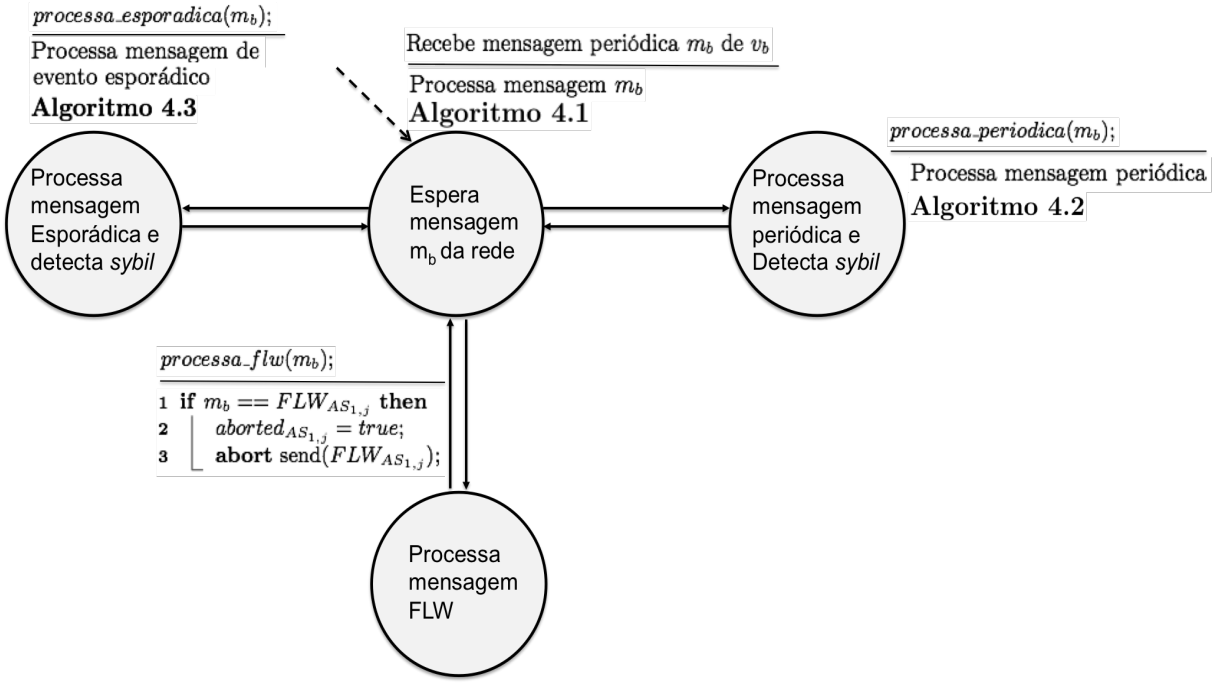


Figura 4.13: FSM de veículo receptor v_a. O estado inicial recebe uma mensagem m_b e determina um dos três outros estados a ser processado.

Estão descritos no Algoritmo 4.1 os procedimentos que são executados nesse estado, dividido em três principais blocos:

1. registrar veículos vizinhos (Linhas 2 a 8): a cada nova mensagem m_b recebida, um veículo receptor v_a verifica-se se já recebeu anteriormente mensagens do veículo transmissor v_b. Caso negativo, verifica a autenticidade da mensagem m_b (como detalhado na Seção 4.2.2) e registra o certificado digital $cert_{b,i}$ recebido, além de associá-lo ao conjunto anonimato de primeiro nível $AS_{1,j}$ (Linhas 4 a 8). Mensagens subsequentes deste mesmo veículo (i.e.: deste mesmo certificado digital $cert_{b,i}$) não são verificadas, reduzindo o tempo de processamento relacionado a assinaturas digitais (como discutido na Seção 5.4);

2. verificar o tipo de mensagem e selecionar o módulo de processamento relacionado à mensagem (Linhas 9 a 15): no contexto de redes VANETs, e em especial do protocolo *ASAP*-V, há três tipos de mensagens que podem ser enviadas/recebidas. Neste estado, um veículo v_a receptor determina o tipo da mensagem recebida e a repassa ao módulo responsável pelo processamento da mensagem específica;

3. verificar os certificados digitais de conjuntos anonimato $cert_{AS_{i,j}} \in CERT^t_{AS_b}$ contidos na mensagem m_b (Linhas 16 a 18): neste caso, um veículo receptor v_a verifica se a mensagem recebida m_b possui o mesmo subconjunto de certificados digitais de conjuntos anonimato do veículo transmissor v_b. Desta forma, v_a deve incluir i $(1 \leq i \leq m)$ certificados digitais $cert_{AS_{i,j}}$ enquanto $cert_{AS_{i,j}} \in CERT^t_{AS_a} = cert_{AS_{i,j}} \in CERT^t_{AS_b}$.

Algoritmo 4.1: Processa mensagem m_b.

```
1  updated ← false;
2  if (v_a, v_b) ∉ E_a then
3      if Verify(k+_RSU, cert_{b,i}) and Verify(k+_{b,i}, m_b) then
4          v_b ← new Vehicle(cert_{b,i}, CERT^t_{AS_b});
5          v_in_AS_{1,j}.append(v_b);
6          hashtable.add(cert_{AS_{1,j}}, ids_in_AS_{1,j}.append(cert_{b,i}));
7  else
8      updated ← update_if_needed(v_b, CERT^t_{AS_b});
9  switch m_b do
10     case periodica
11         processa_periodica(m_b);
12     case FLW
13         processa_flw(m_b);
14     case esporadica
15         processa_esporadica(m_b);
16 for cert_{AS_{i,j}} ← CERT^t_{AS_b} do
17     if cert_{AS_{i,j}} == this.CERT^t_{AS_a}.next() then
18         CERT^t_{AS_a} ← update_current_active_AS(i++);
```

Após registrar localmente um veículo v_b e verificar a autenticidade da mensagem m_b, um veículo receptor v_a repassa a mensagem m_b para um dos três módulos citados acima através de chamadas às funções $processa\_periodica(m_b)$; (Linha 11), $processa\_esporadica(m_b)$; (Linha 13) e $processa\_flw(m_b)$;.

Se uma mensagem recebida m_b caracterizar uma mensagem periódica, a função *processa_periodica*(m_b); é invocada e são executados os procedimentos detalhados no Algoritmo 4.2. Desta forma, verifica-se inicialmente se veículos vizinhos v_x ($(v_a, v_x) \in E_a$) têm transmitido mensagens periódicas com o mesmo certificado digital de conjunto anonimato de primeiro nível (Linha 1), isto é, $cert_{AS_{1,j}} \in CERT^t_{AS_x}$. Caso afirmativo, verifica-se se mensagens oriundas de diferentes pares de veículos v_b/v_x - $(v_a, v_b) \in E_a$ e $(v_a, v_x) \in E_a$ - possuem os mesmos certificados digitais de conjunto anonimato (Linhas 2 e 3), cujo processo reflete a principal condição para detecção de ataques *sybil* no protocolo $ASAP$-V, como detalhado na Seção 4.2.3.

Algoritmo 4.2: Processa mensagem periódica.

```
1  if v_in_AS_{1,j}.size() > 1 and hashtable.get(cert_{AS_{1,j}}).size() > 0 then
2      condition_s ← |CERT^t_{AS_b}| == |CERT^t_{AS_x}| ∧ CERT^t_{AS_b} − CERT^t_{AS_x} ≠ ∅;
3      if ∃ CERT^t_{AS_x} in v_in_AS_{1,j} that do not satisfy condition_s then
4          if P_{b,pos_x} < P_min or P_{x,pos_b} < P_min then
5              flw_message(m_b, m_x).start();
6          else
7              pm ← max(|CERT^t_{AS_b}|, |CERT^t_{AS_x}|);
8              if updated and started_{AS_{1,j}} then
9                  restart(δ_{AS_{1,j}}, pm);
10                 updated ← false;
11             else
12                 start_time(δ_{AS_{1,j}}, pm);
13                 started_{AS_{1,j}} ← true;
14     else
15         if started_{AS_{1,j}} then
16             stop(δ_{AS_{1,j}});
17             started_{AS_{1,j}} ← false;
18             hashtable.get(cert_{b,i}).removeAll();
```

Supondo que, neste momento, v_b transmitiu uma mensagem periódica com o mesmo subconjunto de conjuntos anonimato de um veículo v_x, verifica-se, então, a distância entre ambos os veículos e determina-se se ambos os veículos recebem mensagens entre si, isto é, $(v_b, v_x) \in E_b$ e $(v_x, v_b) \in E_x$. Assim, objetiva-se avaliar cenários relacionados ao desvanecimento da força dos sinais transmitidos, como discutido através do cenário da Figura 4.6.

A seguir, apresenta-se uma abordagem[6] simplificada baseada no modelo de William et al. [192, p. 306] para determinar se $P_{b,pos_x} < P_{min}$ ou se $P_{x,pos_b} < P_{min}$, em que P_{b,pos_x} e P_{x,pos_b} são as potências dos sinais transmitidos por v_b na posição do veículo v_x, e por v_x na posição do veículo v_b, respectivamente. Ou seja, pretende-se determinar se um dos veículos vizinhos v_b ou v_x não recebem mensagens periódicas entre si. Assim, v_b não está no raio de transmissão de v_x e v_x não está no raio de transmissão de v_b. Logo, tem-se que $(v_b, v_x) \notin E_b$ ou $(v_x, v_b) \notin E_x$. O valor de P_{min} dependerá principalmente de três fatores, a saber: da taxa de transmissão, do esquema de modulação e da taxa de codificação utilizados, como detalhado na Tabela 2.1.

Seja $d(v_p, v_q)$ a distância euclidiana entre os veículos v_q e v_p, e α uma constante associada ao decaimento exponencial da potência da onda eletromagnética com a distância percorrida entre os nós v_p e v_q. As Equações 4.9 e 4.10 relacionam as potências média das ondas eletromagnéticas em um dielétrico dissipativo (com perdas) com a distância percorrida pelas ondas dos sinais transmitidos por v_b e v_x, respectivamente. Desta forma, se o veículo receptor v_a detectar que ambos os veículos v_b e v_x não recebem mensagens entre si, então mensagens FLW devem ser enviadas, inicializando-se uma nova *thread* (Linha 5, Algoritmo 4.2) e ativando um novo estado, como ilustrado na Figura 4.14.

$$P_{b,pos_a} = P_{b,pos_b} \cdot e^{-\alpha \cdot d(v_b, v_a)} \quad \text{(Potência de } v_b \text{ detectada por } v_a\text{)}$$
$$P_{b,pos_b} = P_{b,pos_a} \cdot e^{\alpha \cdot d(v_b, v_a)} \quad \text{((1) Potência inicial do sinal transmitido por } v_b\text{)}$$

$$P_{x,pos_a} = P_{x,pos_x} \cdot e^{-\alpha \cdot d(v_x, v_a)} \quad \text{(Potência de } v_x \text{ detectada por } v_a\text{)}$$
$$P_{x,pos_x} = P_{x,pos_a} \cdot e^{\alpha \cdot d(v_x, v_a)} \quad \text{((2) Potência inicial do sinal transmitido por } v_x\text{)}$$

$$P_{b,pos_x} = P_{b,pos_b} \cdot e^{-\alpha \cdot d(v_b, v_x)} \quad \text{((3) Potência do sinal de } v_b \text{ na posição de } v_x\text{)}$$
$$P_{b,pos_x} = P_{b,pos_a} \cdot e^{\alpha \cdot d(v_b, v_a)} \cdot e^{-\alpha \cdot d(v_b, v_x)} \quad \text{((4) Aplicando (1) em (3))}$$

$$P_{b,pos_x} = P_{b,pos_a} \cdot e^{\alpha \cdot \sqrt{(x_b - x_a)^2 + (y_b - y_a)^2} - \sqrt{(x_b - x_x)^2 + (y_b - y_x)^2}} \tag{4.9}$$

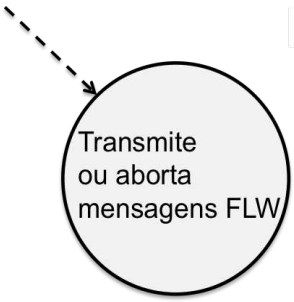
[6]Não são considerados erros associados a fatores tais como mudança de posição dos veículos, reflexão do sinal em árvores, ruído eletromagnético, e precisão do GPS para a estimativa da posição dos veículos.

$$P_{x,pos_b} = P_{x,pos_x} \cdot e^{-\alpha \cdot d(v_x, v_b)} \quad \text{((5) Potência do sinal de } v_x \text{ na posição de } v_b\text{)}$$

$$P_{x,pos_b} = P_{x,pos_a} \cdot e^{\alpha \cdot d(v_x, v_a)} \cdot e^{-\alpha \cdot d(v_x, v_b)} \quad \text{((6) Aplicando (2) em (5))}$$

$$P_{x,pos_b} = P_{x,pos_a} \cdot e^{\alpha \cdot \sqrt{(x_x - x_a)^2 + (y_x - y_a)^2} - \sqrt{(x_x - x_b)^2 + (y_x - y_b)^2}} \tag{4.10}$$

Os procedimentos executados nesta *thread* seguem a abordagem detalhada na Seção 4.2.3. Inicialmente, determina-se o intervalo ζ para que v_a seja um candidato ao envio de mensagens FLW, sendo $|E_a|$ o número de veículos detectados no raio de transmissão, $m_{cert_{AS}}$ a quantidade total de vezes em que mensagens oriundas de v_b (m_b) e de v_x (m_x) possuem os mesmos certificados digitais de conjuntos anonimato, e m o número total de níveis registrados no sistema SV (Linha 1).



Thread inicializada para transmissão de mensagens FLW

1 $thr\_min \leftarrow 1 - (1/|E_a|) - (m_a * (m/100))$;
2 $x_{v_a,r} \leftarrow random(0,1)$;
3 **if** $x_{v_a,r} \in \zeta$ **then**
4 $\quad T_{wait} \leftarrow random(T_{beacon} - max(tmp_{m_b}, tmp_{m_x})$;
5 $\quad$ **sleep**(T_{wait});
6 $\quad$ **if** $not\ aborted_{AS_{1,j}}$ **then**
7 $\quad\quad send(FLW_{AS_{1,j}}, v_b, v_x)$;

Figura 4.14: Procedimentos executados por um veículo receptor v_a para transmitir ou abortar mensagens FLW.

Se v_a escolher um valor aleatório $x_{v_a,r} \in \zeta$ (Linhas 2 e 3), então se tornará um candidato ao envio de mensagens FLW e aguardará um intervalo aleatório T_{wait} (Linhas 4 e 5) milissegundos baseado no intervalo de mensagens periódicas oriundas de v_b e v_x. Neste momento, duas situações podem ocorrer: (1) se v_a receber uma mensagem FLW oriunda de outro veículo v_y $(v_a, v_y) \in E_a$, v_a executará a função $processa\_flw(m_b)$ (Algoritmo 4.1, Linhas 12 e 13) e irá para o estado "Processa mensagem FLW", ilustrado na Figura 4.13. Neste momento, v_a poderá abortar o envio da mensagem FLW. Caso contrário, (2) o tempo T_{wait} excederá e v_a envia mensagens FLW para v_b e v_x (Linhas 6 e 7, Figura 4.14). Este processo é repetido enquanto v_a receber mensagens periódicas oriundas de v_b e v_x, situados numa distância que impossibilita o recebimento de mensagens periódicas entre ambos, e possuem o mesmo conjunto de certificados digitais de conjuntos anonimato.

Retornando ao Algoritmo 4.2, caso ambos os veículos v_b e v_x estejam no raio de transmissão um do outro, executa-se o processo básico de detecção de ataques *sybil* exemplificado na Seção 4.2.3 e ilustrado na Figura 4.5. Para tal, inicializa-se o intervalo de tempo $\delta_{AS_{1,j}}$ baseado na Equação 4.6 (Linhas 12 e 13) e o reinicia sempre que v_b e v_x adicionar um novo e mesmo certificado digital de conjunto anonimato às respectivas mensagens periódicas m_b e m_x (Linhas 8 a 10). Caso m_b e m_x passem a ser distinguíveis entre si, isto é, não possuem mais os mesmos certificados de conjuntos anonimato, v_a poderá interromper a contagem do intervalo $\delta_{AS_{1,j}}$ (Linhas 15 a 18).

Em um ataque *sybil* explorado por meio de mensagens periódicas, um veículo malicioso v_b transmite mensagens com os mesmos certificados digitais. Desta forma, inevitavelmente o intervalo $\delta_{AS_{1,j}}$ excederá (*timeout*) e mensagens oriundas de v_b serão consideradas como suspeitas de um ataque *sybil*. Um evento de *timeout* para o intervalo $\delta_{AS_{1,j}}$ dispara um novo estado, como ilustrado na FSM da Figura 4.15.

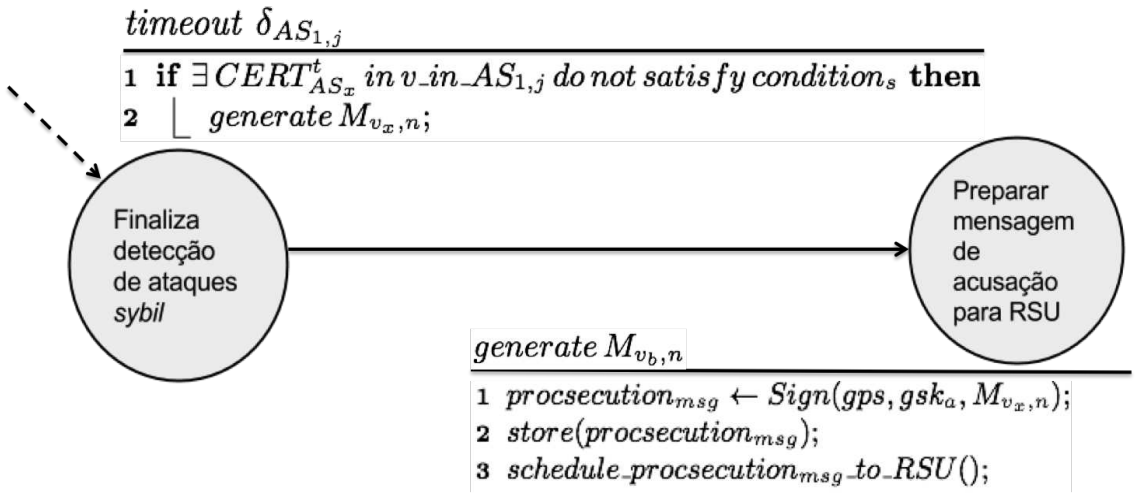


Figura 4.15: Procedimentos executados por um veículo receptor v_a ao exceder o tempo necessário em que mensagens periódicas possuirão diferentes certificados digitais de conjuntos anonimato. Veículo v_a define e armazena mensagem de acusação (Fase 4) a ser enviada a próxima RSU disponível ao longo da via.

Ao exceder o intervalo $\delta_{AS_{1,j}}$, v_a obtém o conjunto de n mensagens que possuem os mesmos certificados digitais de conjuntos anonimato e define uma mensagem de acusação $M_{v_x,n}$. Este processo dispara a transição ao estado "Preparar mensagem de acusação para RSU", no qual v_a assina digitalmente a mensagem de acusação $M_{v_x,n}$ com sua chave privada de grupo gsk_a, e a armazena para ser enviada a próxima RSU disponível na via (Linhas 1 a 3), finalizando, assim, o processamento de detecções de ataques *sybil* oriundos de mensagens periódicas.

Finalmente, o terceiro e último tipo de mensagem que um veículo receptor v_a poderá receber é concernente a eventos esporádicos, e a execução é detalhada através do Algo-

ritmo 4.3. Neste cenário, uma mensagem m_b oriunda de um veículo v_b deve apresentar todos os m certificados digitais de conjuntos anonimato. Desta forma, ao receber uma mensagem m_b, um veículo v_a deve inicialmente obter as mensagens de eventos esporádicos recentemente recebidas (Linha 2). Em seguida, verifica-se se, para este evento, todas as mensagens recebidas não possuem os mesmos certificados digitais de conjuntos anonimato para diferentes pseudônimos (Linhas 3 e 4). Finalmente, caso exista ao menos um par de mensagens com os mesmos m certificados de conjuntos anonimato, deduz-se, então, que a mensagem m_b é oriunda de um mesmo veículo v_b. Assim, o veículo receptor v_a pode apenas descartar a mensagem m_b (Linhas 5 a 7). Caso contrário, registra-se a nova mensagem para o evento específico (Linhas 8 e 9).

Algoritmo 4.3: Processa mensagem m_b de um evento esporádico.

```
1 drop ← False;
2 event_messages ← hashtable_events.get(m_b.evn);
3 for m_x ← event_messages do
4     if m_x.CERT^t_{AS_x} == m_b.CERT^t_{AS_b} then
5         drop(m_b);
6         drop ← False;
7         break;
8 if not drop then
9     hashtable_events.add(m_b.evn, m_b);
```

Com efeito, o processo descrito até aqui permite um veículo receptor v_a analisar dinamicamente o conjunto de certificados digitais $cert_{AS_{i,j}} \in CERT^t_{AS_b}$ de conjuntos anonimato incluídos nas mensagens recebidas m_b, garantindo que tais mensagens são oriundas de diferentes veículos. Entretanto, se um veículo v_a receber mensagens com os mesmos certificados digitais de conjuntos anonimato que ele, v_a deve incluir dinamicamente novos certificados $cert_{AS_{i,j}} \in CERT^t_{AS_a}$ em suas mensagens, permitindo, assim, que outros veículos também possam distinguí-los. Este processo forma o terceiro e último bloco principal de execução de um veículo receptor v_a, detalhado no Algoritmo 4.1.

Nesse contexto, ao receber uma mensagem m_b de um veículo transmissor v_b, um veículo receptor v_a compara cada certificado digital de conjuntos anonimato ativos $cert_{AS_{i,j}} \in CERT^t_{AS_b}$ com seus respectivos certificados digitais de conjuntos anonimato ativos $cert_{AS_{i,j}} \in CERT^t_{AS_a}$ (Linhas 16 e 17). Caso sejam iguais, v_a atualiza e adiciona um novo certificado digital do conjunto anonimato do nível logo abaixo (Linha 18). É importante destacar que a atualização do conjunto de certificados digitais de conjuntos anonimato ativos $CERT^t_{AS_a}$ é refletido no processo executado para transmissão de mensagens m_a do veículo v_a, como detalhado nos procedimentos da FSM de transmissão ilustrada na Figura 4.12 (Linha 4).

4.4 Controle de Anonimato no Protocolo *ASAP*-V

A solução de negociação de identidades (Fase 2) do protocolo *ASAP*-V torna complexo o monitoramento de um veículo e a consequência violação do anonimato de um usuário. Isso deve-se ao fato de que uma requisição a uma RSU não permite determinar qual a identidade real do veículo requisitante, mas apenas determinar a sua autenticidade através do esquema de assinatura de grupos.

Naturalmente, um veículo tem a ele associado um usuário proprietário, bem como outros usuários que, eventualmente, podem fazer uso desse veículo. Daí, torna-se crucial dificultar o monitoramento de um veículo específico a longo prazo, evitando assim que o anonimato de um usuário seja violado.

O primeiro ponto de controle de anonimato reside no uso do esquema de pseudonimato, ou seja, cada veículo possui um conjunto de identidades temporárias, periodicamente alternadas enquanto válidas em um intervalo de tempo. Em contrapartida, o efetivo controle de anonimato nesse contexto dependerá diretamente do modelo de troca de identidades a ser adotada, tais como zonas mistas ou períodos de silêncio, como discutido na Seção 2.5.2.

O segundo ponto chave no controle de anonimato está no uso do esquema de assinatura de grupo. Nesta perspectiva, o monitoramento de mensagens periódicas ou esporádicas não pode ser diretamente associado a um único veículo uma vez que um atacante não poderá extrair informações identificáveis em assinaturas de grupo, salvo a autoridade certificadora que, através da chave de gerenciamento de grupos *gsmk*, deve proporcionar a propriedade de não-repúdio.

Como discutido na Seção 4.1, para detectar ataques *sybil* faz-se necessário determinar se diferentes mensagens, com diferentes identidades, anunciam um mesmo evento e são originadas de um mesmo nó. Evidentemente, para um nó não malicioso, tal procedimento permitiria associar suas diferentes identidades e, consequentemente, construir um perfil de rotas desse veículo. Desta forma, o agrupamento de veículos em conjuntos anonimato, bem como a organização hierárquica de tais conjuntos permitem, respectivamente, manter um grau de incerteza sobre a identidade real de um nó, visto que, uma mensagem transmitida na rede pode ter sido originada de quaisquer veículos pertencentes ao conjunto. Na Seção 5.3, é apresentada uma análise do grau de anonimato no protocolo *ASAP*-V à medida que um veículo v_c expõe os certificados digitais de conjuntos anonimato aos quais v_c pertence.

Por outro lado, para detectar ataques *sybil* em mensagens esporádicas, faz-se necessário incluir todos os certificados digitais dos conjuntos anonimato aos quais o veículo remetente pertence. Entretanto, tal abordagem potencialmente poderá expor o anonimato de um veículo, uma vez que seria possível correlacionar diferentes mensagens esporádicas transmitidas em diferentes regiões. Portanto, cada veículo periodicamente deve solicitar,

por meio de uma RSU, a atualização dos certificados digitais dos conjuntos anonimato aos quais pertence, após todas as possíveis combinações de certificados digitais de conjuntos anonimato serem utilizadas. A segurança dessa abordagem é garantida por intermédio do *hardware* resiliente a modificações não autorizadas, o qual deve validar a requisição e a atualização dos certificados digitais.

4.5 Considerações Finais

Neste capítulo, foi apresentado o protocolo *ASAP*-V, cujo objetivo principal é permitir a autenticação e a detecção de ataques *sybil* em redes *ad hoc* veiculares visando também prover o controle de anonimato dos usuários envolvidos. Em linhas gerais, o protocolo divide-se em 4 fases, incluindo registro e autenticação de veículos, negociação de identidades temporárias, detecção de ataques *sybil* e, por fim, notificação de veículos maliciosos ao sistema.

Ao contrário das soluções investigadas na literatura, o protocolo *ASAP*-V proporciona requisitos tanto para autenticar veículos e detectar ataques *sybil*, quanto para permitir que veículos possam contribuir na identificação de veículos maliciosos e, consequentemente, que esses veículos maliciosos sejam excluídos da rede. Ademais, a solução proposta é flexível tanto para detectar ataques em mensagens periódicas, quanto para mensagens esporádicas.

Capítulo 5

Experimentos e Resultados Alcançados

Neste capítulo, são apresentados os resultados alcançados da presente pesquisa. Inicia-se com uma breve discussão sobre a relevância do processo de avaliação de protocolos de segurança. Em seguida, na Seção 5.2, são apresentadas a metodologia e a validação do protocolo de autenticação e negociação de identidades temporárias introduzido na Seção 4.2.2. Prossegue-se, na Seção 5.3, com uma análise do grau de anonimato oferecido pela abordagem de múltiplos níveis de conjuntos anonimato. Em seguida, na Seção 5.4, é apresentada uma análise da sobrecarga do protocolo *ASAP*-V relacionada ao gerenciamento, ao processamento, ao armazenamento e à comunicação do modelo de criptografia e troca de mensagens propostos. Contempla-se ainda, na Seção 5.5, com a metodologia, os cenários e as métricas utilizadas durante o processo de avaliação do protocolo de detecção de ataques *sybil*. Logo após são apresentados os principais resultados obtidos. Por fim, é apresentado um comparativo entre os resultados obtidos e algumas soluções encontradas na literatura e introduzidas no Capítulo 3.

5.1 Considerações Preliminares

O presente trabalho de pesquisa envolve três grandes áreas da segurança da informação: autenticação, controle de anonimato e ataques *sybil*. No primeiro caso, é de real valia garantir que um processo de autenticação não apresente falhas ou pontos de vulnerabilidade. A detecção tardia de potenciais falhas pode tornar o protocolo não confiável, elevar custos e, consequentemente, não ser utilizado em futuras soluções. No segundo caso, é fundamental analisar o grau de anonimato oferecido pelo sistema, a fim de avaliar a quantidade de informação sobre os usuários que pode ser exposta. Por fim, no terceiro caso, faz-se necessário avaliar o comportamento de execução do protocolo, o qual pretende-se observar se a existência de nós maliciosos é detectada para diferentes cenários.

Em uma outra vertente, há 3 fatores que podem impactar diretamente na escolha de

um protocolo de segurança, a saber: a sobrecarga para gerenciar as chaves de criptografia, a quantidade de dados que precisam ser armazenados e processados, e o tamanho das mensagens que precisam ser transmitidas para se estabelecer a segurança pretendida. Tais fatores também são essenciais que sejam avaliados.

5.2 Validação do Protocolo de Negociação de Identidades Temporárias

No contexto de análise e validação de protocolos de autenticação, torna-se fundamental empregar métodos formais para garantir que os objetivos propostos pelo protocolo foram alcançados, bem como para detectar falhas e provar a consistência na troca de mensagens entre entidades. Nessa perspectiva, há basicamente quatro categorias de métodos formais para verificação de protocolos de autenticação, a saber: linguagem de verificação, sistemas especialistas, sistemas algébricos e lógicas modais.

O modelo formal utilizado neste trabalho para validação do protocolo de autenticação (Fase 2) é chamado de Lógica BAN (*Burrows*, *Abadi* e *Needham*) [193] e foi escolhido devido a sua ampla adoção e expressividade de linguagem. Tal modelo foi capaz de encontrar falhas em protocolos de autenticação e distribuição de chaves utilizados em larga escala, tais como *Needham-Schroeder* [194], CCITT X.509 [195] e Kerberos [196]. De acordo com a proposta inicial da Lógica BAN, o objetivo é descrever a crença das partes envolvidas na autenticação e a evolução desta crença enquanto os participantes se comunicam. A evolução se dá a partir de postulados, ou seja, regras de inferência pré-definidas pela Lógica BAN.

A execução da Lógica BAN divide-se em 3 etapas. A primeira etapa consiste em idealizar o protocolo (*Protocol Idealization*). A segunda etapa é concernente ao levantamento das suposições de crença (*assertions*) e os objetivos com afirmações numa notação simbólica. A existência de crenças duvidosas torna o protocolo inseguro e indica a vulnerabilidade do protocolo. Por fim, na terceira etapa, denominada análise do protocolo (*Protocol Analysis*), transforma-se os passos do protocolo numa notação simbólica e aplica-se as regras de postulados (*inference rules*) para atingir os objetivos do protocolo. Ao atingir os objetivos sem a existência de crenças duvidosas, garante-se então que não há falhas na execução do protocolo.

Está apresentada na Tabela 5.1 parte da nomenclatura utilizada pela Lógica BAN e uma breve descrição de cada símbolo, sendo P e Q entidades comunicantes, e X o conteúdo transmitido entre ambos.

Tabela 5.1: Nomenclatura Lógica BAN.

Representação	**Descrição**
$P \vDash X$	P *acredita em* X: para P, X é verdadeiro ou P pode agir como se X fosse verdadeiro.
$P \triangleleft X$	P *recebe* X: P recebeu uma mensagem contendo X, e por isso, P pode obter X da mensagem. P pode ler e repetir X.
$P \mid\sim X$	P *disse* X: P enviou uma mensagem contendo X em algum momento.
$P \Rightarrow X$	P *tem jurisdição sobre* X: P é responsável por X, ou seja, P tem uma autoridade sobre X e deve ser confiado nesta importância.
$\#(X)$	*Novo* X: X é novo e não foi utilizado antes. Os identificadores e as marcas de tempo (*timestamps*) são comumente gerados com a finalidade de serem novos.
$P \overset{X}{\rightleftharpoons} Q$	A fórmula X *é um segredo de* P e Q: Somente P e Q podem utilizá-lo.
$\{X\}_k$	Fórmula X *cifrada com* a chave k.
$< X > Y$	Combinação entre a fórmula X e a Y.

A seguir, são detalhados os postulados existentes em Lógica BAN, restringindo-se apenas aos necessários para validação do protocolo *ASAP*-V. Outros postulados podem ser encontrados em Burrows et. al [193].

A. $\dfrac{P \vDash Q \overset{Y}{\rightleftharpoons} P, P \triangleleft < X > Y}{P \vDash Q \mid\sim X}$: Se P acredita que Q e P compartilham uma fórmula Y, e P recebe Y combinado com X, então P acredita que Q disse X em algum momento;

B. $\dfrac{P \vDash \#(X), P \vDash Q \mid\sim X}{P \vDash Q \vDash X}$: Se P acredita que X é novo, e P acredita que Q disse X em algum momento, então P acredita que Q acredita em X;

C. $\dfrac{P \vDash Q \Rightarrow X, P \vDash Q \vDash X}{P \vDash X}$: Se P acredita que Q tem jurisdição sobre X, e P acredita que Q acredita em X, então P acredita em X;

D. $\dfrac{P \vDash \#(X)}{P \vDash \#(Y,X)}$: Se P acredita que X é novo, então P acredita que a combinação de X e Y são novos;

E. $\dfrac{P \vDash \xrightarrow{K^+} P, P \triangleleft \{X\}_{K^+}}{P \triangleleft X}$: Se P possui a chave pública k^+ e P recebe uma mensagem X cifrada com a chave pública k^+, então P recebe X.

O primeiro passo da validação consiste em transcrever o protocolo para a notação da Lógica BAN. A seguir, apresenta-se a formulação da requisição de um veículo v_c (Etapa 1) e a respectiva resposta de uma RSU_q (Etapa 3).

$$\text{(Etapa 1):} \quad v_c \rightarrow RSU_q : \{< UUID, cert_{c,i} > m_c\}_{k^+_{RSU_q}}$$
$$\text{(Etapa 3):} \quad RSU_q \rightarrow v_c : \{< TK_c > UUID\}_{k^+_{c,i}}$$

Uma vez definidos os postulados a serem utilizados, e transcrito o protocolo para a notação da Lógica BAN, descreve-se a seguir o conjunto de crenças em que acredita-se ter um fundo de verdade durante a troca de mensagens do protocolo de autenticação proposto. Assim, será possível, conjuntamente com os postulados, verificar se o protocolo há falhas ou pontos de vulnerabilidades.

1. $RSU_q \vDash v_c \overset{cert_{c,i}}{\rightleftharpoons} RSU_q$: RSU_q acredita que compartilha o i-ésimo certificado digital $cert_{c,i}$ com o veículo v_c. Essa suposição é possível pois $Signed^{cert_{c,i}}_{RSU_q}$ para qualquer RSU_q;

2. $RSU_q \vDash \#(m_c)$; RSU_q acredita que a mensagem oriunda do veículo v_c é nova. Essa suposição é possível através da marca de tempo presente na mensagem;

3. $RSU_q \vDash v_c \Rightarrow m_c$: RSU_q acredita que o veículo v_c é responsável pela mensagem m_c. Essa suposição é possível pois v_c armazena $cert_{c,i}$ no *hardware* TPD;

4. $RSU_q \triangleleft \{< UUID, cert_{c,i} > m_c\}_{k^+_{RSU_q}}$: RSU_q recebe a mensagem de requisição m_c com um valor $UUID_c$ do veículo v_c e o i-ésimo certificado digital $cert_{c,i}$ cifrado com a chave pública da RSU;

5. $v_c \triangleleft \{< TK_c > UUID_c\}_{K^+_{c,i}}$: veículo v_c recebe o novo conjunto de pseudônimos e o valor $UUID_c$ enviado à RSU (Etapa 1) cifrado com sua iésima chave pública $k^+_{c,i}$;

6. $v_c \vDash RSU_q \overset{k^+_{c,i}}{\rightleftharpoons} v_c$: veículo v_c acredita que compartilha sua iésima chave pública $k^+_{c,i}$ com a RSU;

7. $v_c \vDash RSU_q \Rightarrow TK_c$: veículo v_c acredita que a RSU é responsável pelo novo conjunto de pseudônimos TK_c;

8. $v_c \vDash \#(TK_c)$: veículo v_c acredita que o conjunto de pseudônimos recebido é novo;

9. $RSU_n \vDash \overset{k^+_{RSU}}{\longrightarrow} RSU_n$: RSU acredita que possui uma chave pública k^+_{RSU};

10. $RSU_n \vDash v_c \overset{k^+_{RSU}}{\rightleftharpoons} RSU_n$: RSU acredita que compartilha sua chave pública k^+_{RSU} com o veículo v_c;

11. $v_c \vDash \overset{k^+_{c,i}}{\longrightarrow} v_c$: veículo v_c acredita que possui uma chave pública $k^+_{c,i}$.

A partir do conjunto de crenças definido acima e com base nos postulados da lógica BAN, a verificação correta do protocolo de negociação de identidades temporárias está sujeita à conclusão dos objetivos descritos na Tabela 5.2:

Tabela 5.2: Objetivos da verificação de corretude do protocolo *ASAP*-V.

Objetivos	**Sintaxe BAN**	**Descrição**
1	$RSU_n \vDash m_c$	A RSU confia na mensagem m_c.
2	$RSU_n \vDash \#(UUID_c, cert_{c,i})$	A RSU confia que a mensagem m_c, o certificado digital do veículo v_c e o valor aleatório $UUID_c$ são recentes.
3	$v_c \vDash TK_c$	O veículo v_c confia no novo conjunto de identidades temporárias TK_c.
4	$v_c \vDash \#(TK_c, UUID_c)$	O veículo v_c confia que a resposta da RSU é recente e relacionada à requisição m_c.

Para provar que o protocolo de autenticação não apresenta falhas ou vulnerabilidades, aplicam-se os postulados A a E da Lógica BAN às crenças 1 a 11 consideradas, como detalhado a seguir:

I. Postulado E aplicado às crenças 4 e 9:
$\frac{RSU_n \vDash \xrightarrow{K^+_{RSU}} RSU_n, RSU_n \triangleleft \{< UUID_c, cert_{c,i} > m_c\}_{k^+_{RSU}}}{RSU \triangleleft < UUID_c, cert_{c,i} > m_c}$: se a RSU possui a chave pública K^+_{RSU} e recebe a mensagem $< UUID_c, cert_{c,i} > m_c$ cifrada com a chave pública K^+_{RSU}, então RSU recebe $< UUID_c, cert_{c,i} > m_c$;

II. Postulado A aplicado à crença 1 e ao resultado I:
$\frac{RSU_n \vDash v_c \overset{cert_{c,i}}{\rightleftharpoons} RSU_n, RSU_n \triangleleft < UUID_c, cert_{c,i} > m_c}{RSU_n \vDash v_c \mid\sim m_c}$: se a RSU acredita que compartilha o i-ésimo certificado digital $cert_{c,i}$ com o veículo v_c, e recebe uma requisição m_c combinada com o certificado $cert_{c,i}$, então a RSU acredita que o veículo v_c enviou a requisição m_c;

III. Postulado B aplicado à crença 2 e ao resultado II:
$\frac{RSU_n \vDash \#(m_c), RSU_n \vDash v_c \mid\sim m_c}{RSU_n \vDash v_c \vDash m_c}$: se a RSU acredita que a mensagem m_c é nova (através da marca de tempo), e a RSU acredita que o veículo v_c enviou m_c em algum momento, então a RSU acredita que o veículo v_c acredita na mensagem m_c;

IV. Postulado C aplicado à crença 3 e ao resultado III:
$\frac{RSU_n \vDash v_c \Rightarrow m_c, RSU_n \vDash v_c \vDash m_c}{RSU_n \vDash m_c}$: se a RSU acredita que o veículo v_c é responsável pela mensagem m_c (devido ao i-ésimo certificado digital $cert_{c,i}$), e a RSU acredita que o veículo v_c acredita na mensagem m_c, então a RSU acredita na mensagem m_c. Desta forma, *o objetivo 1 é alcançado*;

V. Postulado D aplicado à crença 2:
$\frac{RSU \vDash \#(m_c)}{RSU \vDash \#(UUID_c, cert_{c,i})}$: se a RSU acredita que a mensagem de requisição m_c é nova, então a RSU acredita que a mensagem inteira, isto é $UUID_c$ e o certificado $cert_{c,i}$, é nova. Desta forma, *o objetivo 2 é alcançado*;

VI. Postulado E aplicado às crenças 5 e 11:
$\frac{v_c \vDash \xrightarrow{K^+_{c,i}} v_c, v_c \triangleleft \{< TK_c > UUID_c\}_{K^+_{c,i}}}{v_c \triangleleft < TK_c > UUID_c}$: se o veículo v_c acredita que possui a iésima chave pública $k^+_{c,i}$ e v_c recebe uma mensagem de resposta com o conjunto de novos pseudônimos e o $UUID_c$ combinados e cifrados com sua chave pública $k^+_{c,i}$, então o veículo v_c recebeu o conjunto de novos pseudônimos e o $UUID_c$ combinados;

VII. Postulado A aplicado à crença 6 e ao resultado VI:
$\frac{v_c \vDash RSU_n \overset{k^+_{c,i}}{\rightleftharpoons} v_c, v_c \triangleleft < TK_c > UUID_c}{v_c \vDash RSU \mid\sim TK_c}$: se o veículo v_c acredita que compartilha sua chave pública $k^+_{c,i}$ com a RSU, e recebe o conjunto de pseudônimos TK_c da RSU combinado com o $UUID_c$, então o veículo v_c acredita que a RSU enviou TK_c em algum momento;

VIII. Postulado B aplicado à crença 8 e ao resultado VII:
$\frac{v_c \vDash \#(TK_c), v_c \vDash RSU_n \mid\sim TK_c}{v_c \vDash RSU_n \vDash TK_c}$: se o veículo v_c acredita que o novo conjunto de pseudônimos TK_c é recente (novo), e v_c acredita que a RSU transmitiu TK_c em algum momento, então o veículo v_c acredita que a RSU acredita no conjunto de pseudônimos TK_c;

IX. Postulado C aplicado à crença 7 e ao resultado VIII:
$\frac{v_c \vDash RSU_n \Rightarrow TK_c, v_c \vDash RSU_n \vDash TK_c}{v_c \vDash TK_c}$: se o veículo v_c acredita que a RSU é responsável pelo novo conjunto de pseudônimos TK_c (uma vez que RSU assinou digitalmente cada par de chaves), e o veículo v_c acredita que a RSU é responsável por TK_c, então o veículo v_c acredita no novo conjunto de pseudônimos TK_c. Desta forma, *o objetivo 3 é alcançado*;

X. Postulado D aplicado à crença 8:
$\frac{v_c \vDash \#(TK_c)}{v_c \vDash \#(TK_c, UUID_c)}$: se o veículo v_c acredita que o conjunto de pseudônimos TK_c é novo (uma vez que os certificados digitais possuem marcas de tempo), então toda mensagem é nova. Ou seja, a resposta da RSU é nova. Desta forma, *o objetivo 4 é alcançado.*

Como não há a existência de crenças duvidosas para obter os resultados III, IV, VII e VIII, observa-se que o protocolo de autenticação garante que tanto o veículo quanto a RSU confiam nas mensagens que recebem. Por outro lado, é evidente que a Lógica BAN não tem como objetivo garantir a segurança dos algoritmos criptográficos a serem utilizados, mas apenas a consistência de execução do protocolo. Sob esta perspectiva, prova-se que o protocolo de autenticação proposto é confiável e cabe ao projeto de implementação do protocolo o uso de um esquema de criptografia seguro.

Um outro fator importante a ser discutido é concernente a ataques de Homem do Meio (Seção 2.5.1). No contexto do protocolo *ASAP*-V (Fase 2), um ataque MITM resultaria em dois diferentes veículos v_c e v_M (malicioso) armazenando os mesmos pares de chaves TK_c. Isso seria possível se um veículo malicioso v_M interceptasse a mensagem de requisição m_c do veículo v_c, alterasse o certificado digital $cert_{c,i}$ para $cert_{M,i}$ e enviasse à RSU. Ao retornar um novo conjunto de pseudônimos TK_M, v_M obteria e armazenaria TK_M, ao mesmo tempo que retornaria para v_c o mesmo conjunto de pseudônimos TK_M (como TK_c). Consequentemente, v_c armazenaria TK_c e, desta forma, tanto v_c quanto v_M teriam os mesmos pseudônimos. Este ataque permitiria, por exemplo, que o veículo v_M explorasse ataques de rede (ex.: *sybil*) com identidades do veículo v_c.

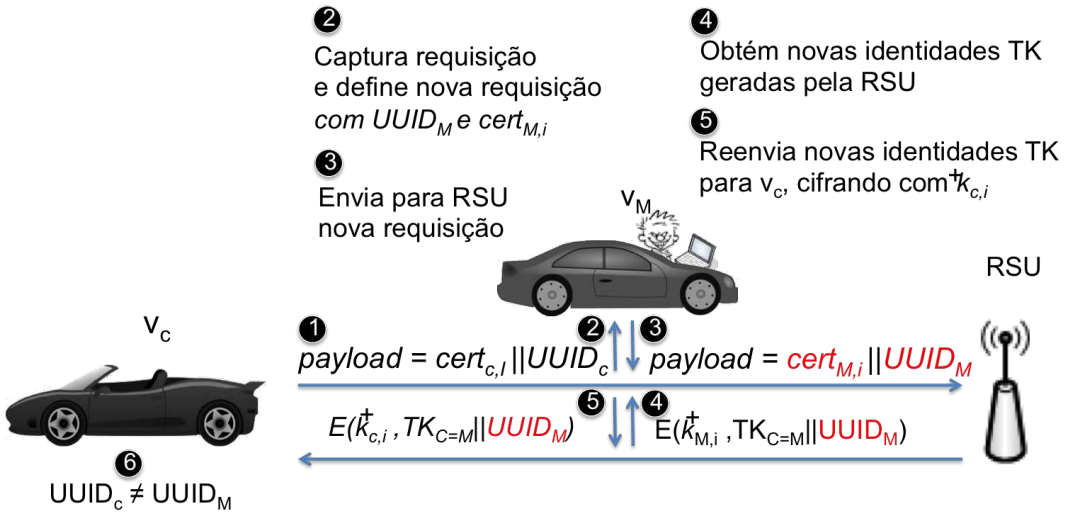


Figura 5.1: Representação da detecção de ataques MITM no protocolo *ASAP*-V.

Para detectar ataques MITM, um veículo v_c deve comparar o valor aleatório $UUID_c$ enviado, com o valor $UUID_c$ recebido em conjunto com os novos pseudônimos. Para tal, estão ilustradas na Figura 5.1 as etapas realizadas em um ataque MITM e como um veículo v_c o detecta. Ao transmitir a requisição de renovação de pseudônimos (Etapa 1), um veículo malicioso v_M intercepta a requisição e adiciona dados de v_M, tais como $UUID_M$ e $cert_{M,i}$ (Etapa 2). Em seguida, transmite a mensagem de requisição para RSU_q (Etapa 3). Ao receber o novo conjunto de pseudônimos TK, o veículo malicioso

v_M armazena-o (Etapa 4) e reenvia TK ao veículo v_c, cifrando-se o conjunto TK com o $UUID_M$ (Etapa 5). Finalmente, ao receber o novo conjunto TK, um veículo v_c detectará o ataque uma vez que $UUID_c \neq UUID_M$ (Etapa 6). Um veículo malicioso v_M não poderá obter $UUID_c$ original pois a requisição (Etapa 1) é transmitida cifrando-se o conteúdo *payload* com a chave pública da RSU_q.

5.3 Verificação e Análise do Controle de Anonimato no Protocolo *ASAP*-V

Nesta seção, apresenta-se uma análise do controle de anonimato proporcionado ao utilizar o protocolo *ASAP*-V.

A partir dos conceitos de conjunto anonimato introduzidos na Seção 2.5.2, considera-se, na presente pesquisa de tese, que o grau de anonimato será total quando um usuário intruso - aquele interessado em monitorar mensagens na rede - associar uma mensagem m_v transmitida na rede como sendo oriunda de qualquer veículo do sistema com igual probabilidade. Desta forma, para verificar o grau de anonimato de um veículo no protocolo *ASAP*-V, aplica-se, então, um método normalizado baseado na Entropia de Shannon [197] para quantificar a incerteza da informação e, assim, ser possível evoluir o grau de anonimato de um veículo em uma determina região.

Em linhas gerais, a abordagem utilizada para determinar o grau de anonimato de um veículo v_c compara a entropia de um conjunto anonimato $AS_{i,j}$ com a entropia máxima do conjunto anonimato de primeiro nível $AS_{1,j}$. Ou seja, a abordagem avalia a quantidade de informação exposta pelo sistema após o envio de uma mensagem m_c por um veículo v_c que contém os certificados digitais $cert_{AS_{i,j}} \in CERT^t_{AS_c}$ dos conjuntos anonimato $AS_{i,j}$ $(1 < i \leq m)$. Desta forma, é possível mensurar o quão distinguível é o veículo v_c dentro de um conjunto de veículos.

Seja $AS_{1,j}$ o conjunto anonimato de primeiro nível ao qual um veículo v_c pertence, e $N_{AS_{1,j}}$ o número total de veículos nesse conjunto. Desta forma, está definida na Equação 5.1 a entropia máxima $H^M_{AS_{1,j}}$ do conjunto $AS_{1,j}$.

$$H^M_{AS_{1,j}} = log_2(N_{AS_{1,j}}) \tag{5.1}$$

A entropia $H^X_{AS_{i,j}}$ de um conjunto anonimato $AS_{i,j}$ $(1 < i \leq m)$ após um veículo v_c expor o i-ésimo certificado digital $cert_{AS_{i,j}}$ desse conjunto anonimato está definida na Equação 5.2. Um usuário intruso atribui uma probabilidade p_{v_c} para cada veículo v_q $(1 \leq q \leq N_{AS_{i,j}})$ no conjunto $AS_{i,j}$ como sendo o transmissor da mensagem m_c.

$$H^X_{AS_{i,j}} = -\sum_{k=1}^{N} log_2(p_{v_c}) \tag{5.2}$$

A informação adquirida por um intruso após monitorar o canal de comunicação e observar o i-ésimo certificado digital do conjunto anonimato $AS_{i,j}$ é $H^M_{AS_{1,j}} - H^X_{AS_{i,j}}$. Divide-se o valor por $H^M_{AS_{1,j}}$ para normalização. Assim, está definido na Equação 5.3 o grau de anonimato $d_{AS_{i,j}}$ de um conjunto anonimato de veículos $AS_{i,j}$:

$$d_{AS_{i,j}} = 1 - \frac{H^M_{AS_{1,j}} - H^X_{AS_{i,j}}}{H^M_{AS_{1,j}}} = \frac{H^X_{AS_{i,j}}}{H^M_{AS_{1,j}}} \tag{5.3}$$

O grau de anonimato $d_{AS_{i,j}}$ $(1 \leq i \leq m)$ varia entre 0 - quando um veículo v_c aparece como sendo o transmissor da mensagem m_c com probabilidade 1 - e 1, quando todos os veículos no conjunto $AS_{i,j}$ têm igual probabilidade de ser o transmissor da mensagem m_c.

Está apresentada na Tabela 5.3 uma análise do grau de anonimato considerando o seguinte cenário: sistema SV possui 80 milhões de veículos registrados[1], $j = 420$ grupos por nível e cada veículo presente em $k = 20$ conjuntos anonimato por nível. A coluna *N° de veículos juntos/nível* descreve a quantidade de veículos pertencentes ao conjunto $AS_{1,j}$ que ainda compartilham os mesmos certificados digitais no conjunto $AS_{i,j}$. Consequentemente, para o último nível $i = 6$, todos os veículos distribuídos pelos conjuntos anonimato satisfazem a propriedade 4 da arquitetura de conjuntos anonimato proposta na Seção 4.2.1.

Tabela 5.3: Grau de anonimato ($d_{AS_{i,j}}$) para um dado conjunto anonimato $AS_{i,j}$.

Níveis	N° de veículos juntos/nível	$H^X_{AS_{i,j}}$	$d_{AS_{i,j}}$
$i = 1$	3.809.524	21.87	1.00
$i = 2$	181.405	17.47	0.79
$i = 3$	8.638	13.08	0.59
$i = 4$	412	8.7	0.39
$i = 5$	19	4.4	0.20
$i = 6$	≈ 1	-0.10	0.00

Quando um veículo v_c transmite mensagens com um único certificado digital do conjunto anonimato $AS_{1,j}$, o grau de anonimato $d_{AS_{i,j}}$ é igual a 1 e, consequentemente, pode-se afirmar que todos os veículos no conjunto $AS_{1,j}$ possui a mesma probabilidade de ter sido o transmissor das mensagens. Ao adicionar o i-ésimo certificado digital do conjunto anonimato $AS_{i,j}$ nas mensagens que são transmitidas na rede, um veículo v_c expõe

[1]De acordo com o DNIT - Departamento Nacional de Trânsito Brasileiro - este número inclui carros, motos e ônibus no final do ano de 2014.

informações que podem identificá-lo exclusivamente, diminuindo gradativamente o valor do anonimato $d_{AS_{i,j}}$. Quando o veículo v_c expõe todos os certificados digitais $CERT^t_{AS_c}$ em um momento t, o grau de anonimato $d_{AS_{i,j}}$ é igual a zero e v_c aparece como sendo o transmissor das mensagens com probabilidade igual a 1.

É importante notar que apesar da possibilidade do anonimato de um veículo v_c diminuir totalmente, v_c expõe apenas uma "parte" do anonimato no momento t, uma vez que o conjunto de certificados digitais de conjuntos anonimato ativos $CERT^t_{AS_c}$ é temporário. Veículo v_c poderá, então, selecionar um novo subconjunto de certificados digitais ativos $CERT^{t_2}_{AS_c}$ para o instante t_2. Ou seja, para o cenário em questão, v_c possui 20^6 possíveis combinações de certificados digitais de conjuntos anonimato ativos. Desta forma, decorre-se que a probabilidade de que dois diferentes veículos v_c e $v_{c'}$, no mesmo conjunto anonimato $AS_{1,j}$, selecionem os mesmos $m-1$ certificados digitais de conjuntos anonimato ativos $CERT^t_{AS_c}$ e $CERT^{t+1}_{AS_c}$ é $\prod_{i=1}^{m-1} \frac{1}{20}$, ou seja, uma chance relativamente pequena. Consequentemente, a probabilidade de que o anonimato de v_c seja totalmente exposto ao transmitir mensagens periódicas também é pequena. Desta forma, quanto maior os valores para k e j, menor serão as changes de um veículo expor o anonimato.

5.4 Análise de Gerenciamento, Armazenamento, Processamento e Comunicação do protocolo *ASAP*-V

Nesta seção, é apresentada uma análise sobre o custo computacional relacionado ao gerenciamento, ao armazenamento, ao processamento e à comunicação do protocolo *ASAP*-V.

- **Custo de Gerenciamento**:
  - *Na Autoridade Certificadora*: a C.A é a única entidade responsável pelo gerenciamento dos certificados digitais de conjuntos anonimato, bem como das chaves de assinaturas de grupo, os quais, uma vez definidos, não mudarão;
  - *Nos Veículos*: os veículos precisam apenas gerenciar o processo de renovação de identidades temporárias, o qual ocorre a depender de dois fatores, a saber: da quantidade w de identidades armazenadas no último procedimento de aquisição de identidades temporárias (Fase 2); e da taxa de troca de identidades - a qual dependerá também de outros dois fatores: (1) do período de validade de cada certificado digital $cert_{c,i}$ $(1 \leq i \leq w)$ - o qual exigirá a troca de uma identidade - e (2), da quantidade de vezes em que o veículo participou de algum procedimento de detecção de ataques *sybil*;

  - *Nas Unidades de Acostamento (RSUs)*: as RSUs são responsáveis apenas pela geração de w identidades temporárias (Fase 2), a qual não se faz necessário gerenciar cada identidade posteriormente. Neste momento, há sobrecarga maior apenas no contexto de processamento, como é discutido a seguir.

- **Custo de Processamento**: o custo de processamento durante comunicação V2V (entre veículos) e V2I (entre veículos e RSUs) foi avaliado numa plataforma com processador 2.9 GHz (Intel Core i7) e 8 GB de memória (RAM). Optou-se pelos algoritmos *Elliptic Curve Digital Signature Algorithm* (ECDSA) [69] e *Group Signatures with Almost-for-free Revocation* (GSAR) [198] para o processo de assinaturas digitais em arquitetura de chaves pública/privada, e assinaturas de grupo, respectivamente. Justifica-se a escolha destes algoritmos por terem menor custo de processamento[2] para assinaturas, verificação de assinaturas e verificação de revogação de chaves.

  - *Em comunicação V2V*: para permitir o envio de mensagens[3] V2V de forma autenticada e com suporte à integridade, um veículo v_a inicialmente assina os dados d (sobre mobilidade ou sobre eventos esporádicos) através da sua chave de assinaturas de grupo gsk_a, cujo processo possui tempo médio de 11 *ms* com o algoritmo GSAR; logo em seguida, a mensagem inteira é assinada com a *i-ésima* chave privada $k^-_{a,i}$ do veículo v_a, cujo tempo médio é de 0,1 *ms* utilizando ECDSA. Desta forma, o tempo médio para assinar uma mensagem é de 11,1 *ms*.

    Por outro lado, para determinar a autenticidade e a integridade das mensagens recebidas, um veículo v_b realiza duas etapas, a saber: verifica a autenticidade da chave pública $k^+_{a,i}$ do remetente (v_a) da mensagem, a qual está disponível no certificado digital $cert_{a,i}$; e, na segunda etapa, verifica a autenticidade da mensagem completa, a qual foi assinada digitalmente com essa chave pública $k^+_{a,i}$. Na primeira etapa, leva-se um tempo médio de 0,4 *ms*, ao passo que leva-se um tempo médio de 0,4 *ms* para a segunda etapa, totalizando 0,8 *ms* para verificar a autenticidade e a integridade da mensagem completa.

    É importante destacar que a primeira etapa é realizada apenas uma única vez por cada identidade temporária (certificado digital) $cert_{a,i}$. Ademais, o veículo receptor não precisa verificar a autenticidade da assinatura de grupo, uma vez que esta autenticação é utilizada apenas para garantir a propriedade de não-repúdio. Finalmente, como resultado da sobrecarga de processamento, um

[2]Porém, ambos os algoritmos exigem maior espaço para armazenamento de chaves quando comparado a alguns outros trabalhos.

[3]Mensagens com o formato detalhado na Figura 4.4.

veículo é capaz de assinar 90 mensagens por segundo, ao passo pode verificar 1250 mensagens por segundo.

- *Em comunicação V2I*: durante o processo de renovação de identidades temporárias (Fase 2 do protocolo *ASAP*-V), um veículo v_a assina a mensagem de requisição m (gerando σ, Etapa 1) através de sua chave secreta de grupo gsk_a, o que pode ser realizado em um tempo médio de processamento de 11 *ms* utilizando GSAR; em seguida, a mensagem de requisição é criptografada com chave pública da RSU através de ECDSA, com tempo de 0,1 *ms*; ao receber a requisição m, a RSU inicialmente decripta a mensagem com sua chave privada, com um tempo de 0,4 *ms*; verifica se o *token* grt_a está na lista de *tokens* revogados, cujo custo de processamento é *O(n)* - onde n é a quantidade de *tokens* revogados -, bem como verifica a autenticidade da assinatura digital de grupo, cujo processo totaliza um tempo médio de 132 *ms*; em seguida, a RSU gera w par de chaves, cujo tempo médio de processamento é de w*83 *ms*, e assina cada par de chaves com um tempo de processamento de w*0,1 *ms*.

  Se a quantidade w de pares de chaves for alta (ex.: w = 1000), um veículo poderia não receber o novo conjunto de chaves devido à velocidade de deslocamento ao transitar pela RSU em questão. Para contornar esta limitação, uma RSU poderia manter armazenado um conjunto de chaves pré-assinadas (ex.: w' = 10.000), cuja abordagem teria impacto menor no processamento durante a requisição de renovação de chaves e, inclusive, menor impacto na sobrecarga de armazenamento, como detalhado a seguir.

- **Custo de Armazenamento**: o custo de armazenamento refere-se à quantidade de dados que devem ser armazenados em cada entidade.

  - *Na Autoridade Certificadora*: a C.A deve armazenar um conjunto de certificados digitais, incluindo: os certificados digitais dos conjuntos anonimato, os quais exigem $m*n*56$ bytes, utilizando o modelo ECDAS de 224 *bits*; a chave privada de grupo de cada veículo (gsk_p), bem como a chave pública de grupo *gpk*, os quais exigem $N*64$ bytes e *O (log N)*-bytes de armazenamento, respectivamente, para N veículos registrados na C.A. Ao utilizar GSAR, o tamanho dos certificados digitais de cada veículo se mantém constante (*O(1)*).

    É importante destacar que a C.A não precisa armazenar os conjuntos de certificados temporários de cada veículo que os obtêm na fase de renovação de identidades (Fase 2), reduzindo o custo de armazenamento na C.A, um problema que ocorre em outros trabalhos encontrados na literatura [53, 54].

- *Em cada veículo*: um veículo v_a deve armazenar sua chave secreta de grupo gsk_a (64 bytes), cujo tamanho não dependerá da quantidade de veículos N (*O (1)*), bem como uma única chave pública de grupo *gpk*, cujo tamanho é *O (log N)*-bytes; além das chaves de assinaturas de grupo, cada veículo deve armazenar w pares de chaves pública/privada, totalizando w*56 bytes, bem como cada certificado digital do conjunto anonimato ao qual pertence, totalizando $k*m*56$ bytes. Neste último caso, para o cenário detalhado na Seção 5.3, um veículo deve armazenar apenas 6,72 Kbytes ($k = 20$, $m = 6$).
- *Em cada Unidade de Acostamento*: uma RSU deve armazenar a lista RL de *tokens* revogados, onde RL consome *O(r)*-bytes, onde r é a quantidade de *tokens* revogados. Além disso, para lidar com a limitação citada na sobrecarga de processamento no contexto de comunicação V2I, uma RSU pode armazenar um conjunto de tamanho w' pré-definido de pares de chaves pública/privada, consumindo $w' * 28$ bytes.

- **Custo de Comunicação**: o custo de comunicação está relacionado à quantidade de dados que deve ser transmitida em uma única mensagem. Dentro do contexto deste trabalho, pode-se avaliar o custo de comunicação em dois cenários:

  - *Em comunicação V2V*: veículos comunicam-se através de mensagens periódicas (*beacon*) ou esporádicas. No primeiro caso, uma mensagem periódica transmitida por um veículo v_a inclui um certificado digital de um conjunto anonimato de primeiro nível ($AS_{1,j}$), o qual possui 56 bytes (utilizando ECDSA com chave de 224 *bits*); em seguida, adiciona-se a assinatura digital dos dados d (σ), cujo tamanho é constante em 225 bytes (*O(1)*) utilizando GSAR; por fim, adiciona-se o *i-ésimo* certificado digital $cert_{i,a}$, o qual consome 56 bytes; a assinatura da mensagem completa tem tamanho de 56 bytes, totalizando 393 bytes a serem transmitidos numa única mensagem periódica.

    A cada novo certificado digital de conjunto anonimato a ser adicionado (fase de detecção de ataques *sybil*), adiciona-se 56 bytes ao tamanho total da mensagem a ser transmitida. Na Seção 5.3, foi feita uma avaliação do tamanho mínimo ou ideal de níveis m para assegurar anonimato, sem comprometer a eficiência do protocolo *ASAP*-V na fase de detecção de ataques *sybil*;
  - Em comunicação V2I: veículos comunicam-se com RSUs nas Fases 2 e 4 do protocolo *ASAP*-V. Na Fase 2, um veículo v_a envia uma requisição de renovação de identidades temporárias (Etapa 1) à RSU incluindo os seguintes dados: assinatura digital de grupo, a qual consome 225 bytes, bem como a criptografia

da requisição, a qual possui tamanho de 56 bytes. Desta forma, o tamanho total desta requisição é 281 bytes.

A resposta desta requisição transmitida pela RSU inclui o conjunto TK_a possuindo w pares de chaves temporárias e os respectivos certificados digitais, totalizando $w * 56$ bytes; adiciona-se também a assinatura digital do conjunto TK_a, a qual consome 56 bytes. Desta forma, o tamanho total da mensagem de resposta à requisição da Etapa 1 totaliza $w * 56 + 56$ bytes.

A partir da análise delineada anteriormente, é possível observar que mesmo com a utilização de dois diferentes esquemas de assinaturas digitais - arquitetura de chaves públicas e assinaturas de grupo -, o protocolo *ASAP*-V possui uma sobrecarga computacional viável, isto é, é um protocolo que pode ser aplicado dentro do contexto de redes VANETs. Justifica-se tal afirmação pois, como pontuado por [199], em uma VANET, energia e poder computacional não são requisitos que devem restringir a aplicação de algoritmos que exigem maior consumo de energia ou processamento, uma vez que os nós participantes deverão contemplar recursos de hardware compatíveis.

5.5 Avaliação da Detecção de Ataques Sybil

Nesta seção, são apresentados os resultados da avaliação do protocolo de detecção de ataques *sybil*. Inicialmente são introduzidos o cenário, os parâmetros e as métricas que foram consideradas durante os experimentos e, em seguida, os principais resultados alcançados, comparando conjuntamente com duas abordagens encontradas na literatura.

5.5.1 Cenário, Métricas e Parâmetros dos Experimentos

Os experimentos foram realizados através do simulador de redes Veins (baseado no *framework* Omnet++) [200] em conjunto com o simulador de mobilidade SUMO (*Simulator of Urban MObility*) [201]. Foram considerados diferentes topologias de rede, isto é, quantidade de nós na rede, formas de mobilidade dos nós e infraestruturas das vias.

Através dos experimentos, objetivou-se responder aos seguintes questionamentos:

Q1: Se dois veículos v_c e $v_{c'}$ pertencentes ao mesmo conjunto anonimato de primeiro nível ($AS_{1,j}$) forem detectados por um nó avaliador v_a - ou seja, $(v_a, v_c) \in E_a$ e $(v_a, v_{c'}) \in E_a$ e, consequentemente, mensagens periódicas transmitidas por v_c e $v_{c'}$ possuem certificados iguais $cert_{AS_{1,j}}$ -, então qual é o tempo médio para que v_a conclua que são mensagens originadas de dois veículos diferentes? A resposta a esse primeiro ponto é apresentada na Seção 5.5.2.

Q2: Qual é o tempo médio para detectar um ataque *sybil* considerando mensagens periódicas oriundas de um único veículo malicioso v_e? A resposta a esse segundo ponto é apresentada na Seção 5.5.2.

Q3: Qual é o tempo médio para detectar dois veículos legítimos v_c e $v_{c'}$ ao transmitir mensagens FLW? Ou seja, os sinais transmitidos por v_c e $v_{c'}$ não são recebidos por ambos, respectivamente, caracterizando um cenário de desvanecimento da força dos sinais. A resposta a esse terceiro ponto é apresentada na Seção 5.5.2.

Para responder aos questionamentos definidos, foram considerados durante os experimentos diferentes números de veículos, diferentes níveis de conjuntos anonimato e diferentes taxas de transmissão de pacotes *beacon* (mensagem periódica). Na Tabela 5.4, são listados os parâmetros de rede utilizados, bem como as variáveis do protocolo de detecção de ataques *sybil*. Tais parâmetros também foram selecionados em outras abordagens encontradas na literatura, permitindo, assim, compará-las com o protocolo *ASAP*-V.

- Níveis de conjuntos anonimato: mensagens periódicas oriundas de dois veículos diferenciam uma das outras nos certificados digitais dos níveis 4, 5 ou 6. O mesmo raciocínio também foi utilizado para detectar veículos *sybil*, isto é, atacantes transmitem diferentes mensagens até o nível limite de conjuntos anonimato;

- Taxa de transmissão de mensagens periódicas: para cada cenário avaliado, foram consideradas as taxas de transferência 3, 5 e 10 mensagens periódicas por segundo. Isto é, cada veículo transmite mensagens periódicas na rede com intervalos de 100, 200 ou 300 milissegundos. Tais intervalos são especificados pelo padrão WAVE (Seção 2.3.1) devido a altas velocidades de deslocamento dos veículos.

Tabela 5.4: Parâmetros dos Experimentos.

Representação	**Descrição**
Número médio de execuções/cenário	30
Tempo total de simulação por execução[4]	10s, 20s, 30, 50s, 74s, 80s, 100s, 140s, 160s
Protocolo de rede sem fio	802.11p
Potência max. transmissão (PHY 802.11p)	10 mW (ou 10 dBm)
Sensibilidade do Receptor (PHY 802.11p)	-73 dBm
Modelo de Propagação do Sinal	*Obstacle Shadowing*
Taxa de transmissão	18Mbps

Continua na próxima página

[4]Tempo varia de acordo com a quantidade de veículos na região.

Tabela 5.4 – *Continuação da página anterior*

Símbolo	**Descrição**
Taxa de mensagens periódicas (*beacon*)	3, 5 e 10 mensagens por segundo
Número de veículos na região	3, 5, 7, 12, 17, 22, 25, 30, 40, ..., 100
Velocidade média de deslocamento	40 - 120 km/h
Modelo de mobilidade	Krauss[5]
Níveis de conjuntos anonimato (m)	4, 5 e 6
Número de identidades *sybil*	3
Tamanho dos certificados digitais	56 bytes (ECDSA 224 bits)[6]

O cenário considerado nos experimentos está ilustrado na Figura 5.2, no qual os veículos se deslocam em direções contrárias para diferentes faixas, com velocidades aleatórias e seguindo o modelo de mobilidade *Krauss*.

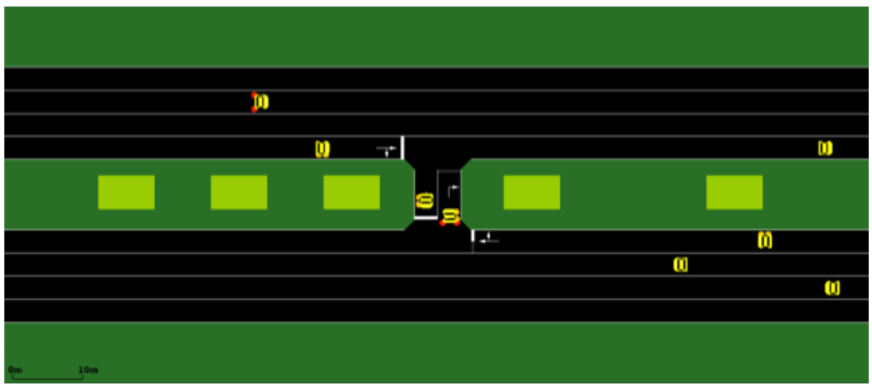


Figura 5.2: Cenário de execução dos experimentos.

5.5.2 Resultados Alcançados

Detecção de Veículos Legítimos

Detalha-se na Figura 5.3, a execução do protocolo *ASAP*-V no simulador Veins. Para o cenário descrito em questão, considerou-se uma taxa de transmissão de 10 mensagens periódica por segundo, 7 veículos no raio de transmissão (identidades de 0 a 6 atribuídas aos veículos pelo simulador Veins), e um número máximo de 4 níveis de conjuntos anonimato ($m = 4$). Considerou-se também a presença de 2 veículos que estão incluídos em

[5]Modelo de mobilidade implementado no simulador SUMO. Permite representar variações de velocidade, e objetiva-se evitar colisões entre os veículos a partir de uma distância mínima entre eles.

[6]Assinaturas de Curvas Elípticas (Elliptic Curve Digital Signature Algorithm - ECDSA)

três conjuntos anonimato iguais ($AS_{1,j}$, $AS_{2,j}$ e $AS_{3,j}$) e diferem apenas no conjunto anonimato do quarto nível ($AS_{4,k}$ e $AS_{4,q}$). Como resultado, o tempo para um nó avaliador concluir que as mensagens oriundas dos dois veículos e não de um veículo malicioso (com duas identidades *sybil*) foi de aproximadamente 185 *ms*.

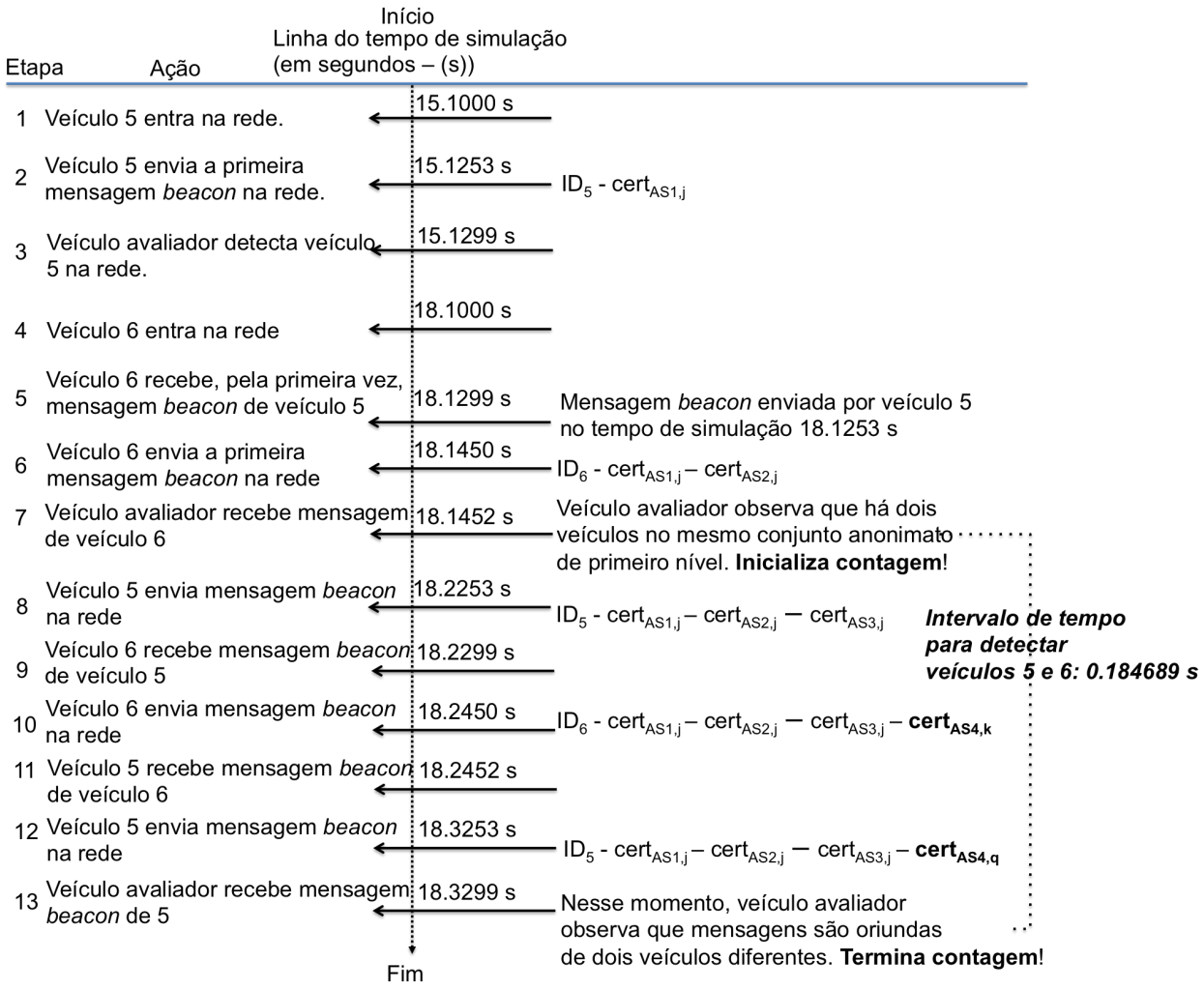


Figura 5.3: Cenário de execução para detectar dois veículos legítimos. Na rede, há 7 veículos na região e ambos os veículos transmitem mensagens periódicas com os mesmos certificados digitais dos conjuntos anonimato de níveis 1, 2, e 3.

Inicialmente, um veículo com identificador 5 (ID_5) entra na rede na Etapa 1 e envia a primeira mensagem periódica à rede na Etapa 2. Neste momento, o veículo 5 apresenta apenas o certificado digital do conjunto anonimato de primeiro nível ao qual pertence ($cert_{AS_{1,j}}$). Em seguida, na Etapa 3, um veículo avaliador recebe a primeira mensagem originada do veículo 5 e registra-o localmente associando-o ao conjunto anonimato $AS_{1,j}$. Um outro veículo, com identificador 6 (ID_6), entra na rede na Etapa 4 e, antes mesmo de observar o meio livre para envio de suas mensagens periódicas, na Etapa 5 o veículo 6 recebe do veículo 5 uma mensagem periódica contendo o certificado digital do conjunto

anonimato $cert_{AS_{1,j}}$. A execução prossegue com o veículo 6 observando o canal livre e enviando a primeira mensagem periódica na Etapa 6. Como este possui conhecimento que existe outro veículo na região que pertence ao mesmo conjunto anonimato de primeiro nível, então, objetivando não se tornar um suspeito de um ataque *sybil* do ponto de vista do nó avaliador, veículo 6 inclui nas mensagens periódicas o certificado digital do próximo nível, a saber, $cert_{AS_{2,j}}$. Na Etapa 7 o nó avaliador observa que há mensagens com diferentes identidades mas que possuem o mesmo certificado digital do primeiro nível de conjunto anonimato.

Neste momento, para o nó avaliador há duas possibilidades: ou as mensagens são originadas de um ataque *sybil*, onde um veículo malicioso envia mensagens com diferentes identidades, ou existem dois veículos diferentes mas que estão no mesmo conjunto anonimato de primeiro nível. Desta forma, ainda na Etapa 7, o nó avaliador inicia uma contagem de tempo baseada na Equação 4.6 e aguarda até δ *ms* para que mensagens com identificadores 5 ou 6 apresentem um novo certificado digital do próximo conjunto anonimato. Na Etapa 8, ao observar que existem mensagens na rede cujos certificados digitais de conjuntos anonimato são iguais nos níveis 1 e 2 ($cert_{AS_{1,j}}$ e $cert_{AS_{2,j}}$), o veículo 5 envia a próxima mensagem periódica incluindo os certificados digitais dos níveis 1, 2 e 3 ($cert_{AS_{1,j}}$, $cert_{AS_{2,j}}$ e $cert_{AS_{3,j}}$, respectivamente). Por sua vez, na Etapa 9, o veículo 6 observa que há outro veículo na rede pertencente aos mesmos conjuntos anonimato em três níveis consecutivos e passa a incluir o último certificado digital, a saber, $cert_{AS_{4,k}}$, na Etapa 10. Em seguida, na Etapa 11, ao receber mensagem do veículo 6 e observar que suas mensagens continuam sendo suspeitas sob a perspectiva de um nó avaliador, o veículo 5 também inclui o certificado digital do quarto e último nível, $cert_{AS_{4,q}}$, na Etapa 12. Finalmente, na Etapa 13, o nó avaliador detecta que as mensagens com diferentes identidades agora apresentam certificados digitais distintos e pode concluir que não há um veículo *sybil* na rede. É importante observar que os veículos 5 e 6 diferem apenas no certificado digital do quarto nível ($cert_{AS_{4,k}}, cert_{AS_{4,q}}$), ou seja, o pior caso em cenários com $m = 4$ níveis de conjuntos anonimato.

Estão ilustrados nos gráficos da Figura 5.4 o tempo médio e os respectivos intervalos de confiança para 95% em torno da média para detectar dois veículos legítimos. Para cada cenário, as médias finais foram obtidas a partir de 30 médias amostrais originadas de um total de 900 execuções. Em linhas gerais, foi possível detectar ambos os veículos em menos de 1 segundo. Pode-se observar que à medida que o número de veículos aumenta no raio de transmissão, o tempo médio para detectar dois veículos cresce aproximadamente de forma linear. Este comportamento se deve pelo fato de que quanto maior o número de veículos no raio de transmissão, maior será o atraso relacionado à contenção de acesso meio. Ademais, um veículo avaliador tende a processar uma quantidade maior de certificados digitais de

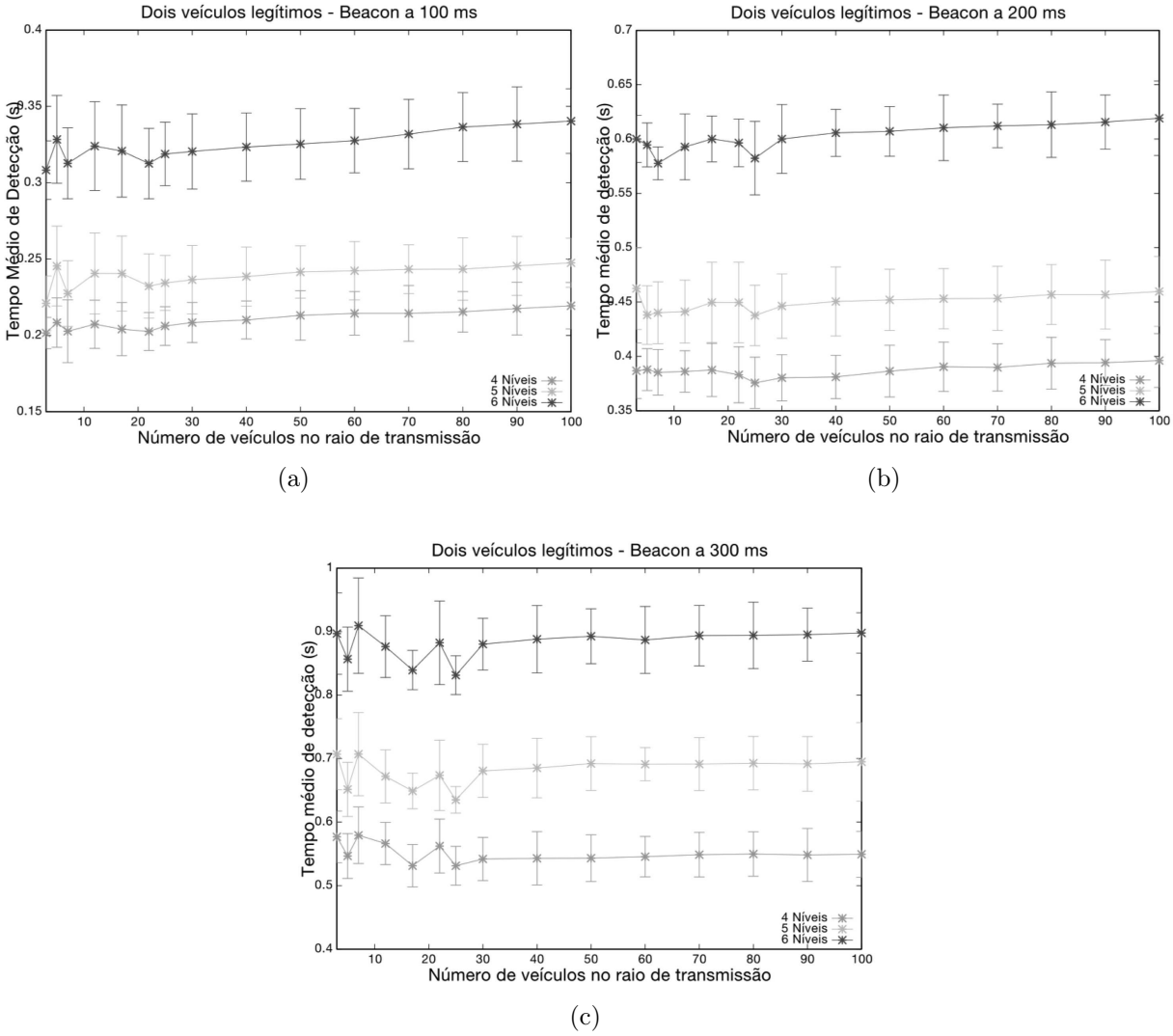


Figura 5.4: Tempo médio para detectar dois veículos legítimos que transmitem mensagens periódicas com os certificados digitais dos $m-1$ conjuntos anonimato ativos.

conjuntos anonimato, uma vez que se faz necessário determinar as potências dos sinais transmitidos, bem como a presença de outros veículos no mesmo conjunto anonimato de primeiro nível.

O processo de detecção de veículos legítimos será predominante em redes veiculares, uma vez que deverá ocorrer um número proporcionalmente pequeno de ataques *sybil* em cenários reais. Desta forma, analisa-se, a seguir, um cenário onde a quantidade de veículos no mesmo conjunto anonimato $AS_{1,j}$ é maior que dois. É ilustrado na Figura 5.5 o processo para detectar todos os veículos legítimos seguindo uma linha do tempo de execução.

Quando a quantidade de veículos legítimos no mesmo raio de transmissão se aproxima do número de conjuntos anonimato iguais que tais veículos selecionam como ativos, o tempo médio para detectar cada veículo estará em torno do intervalo de tempo de transmissão de mensagens periódicas. Como exemplo, no cenário da Figura 5.5, onde 5 veículos

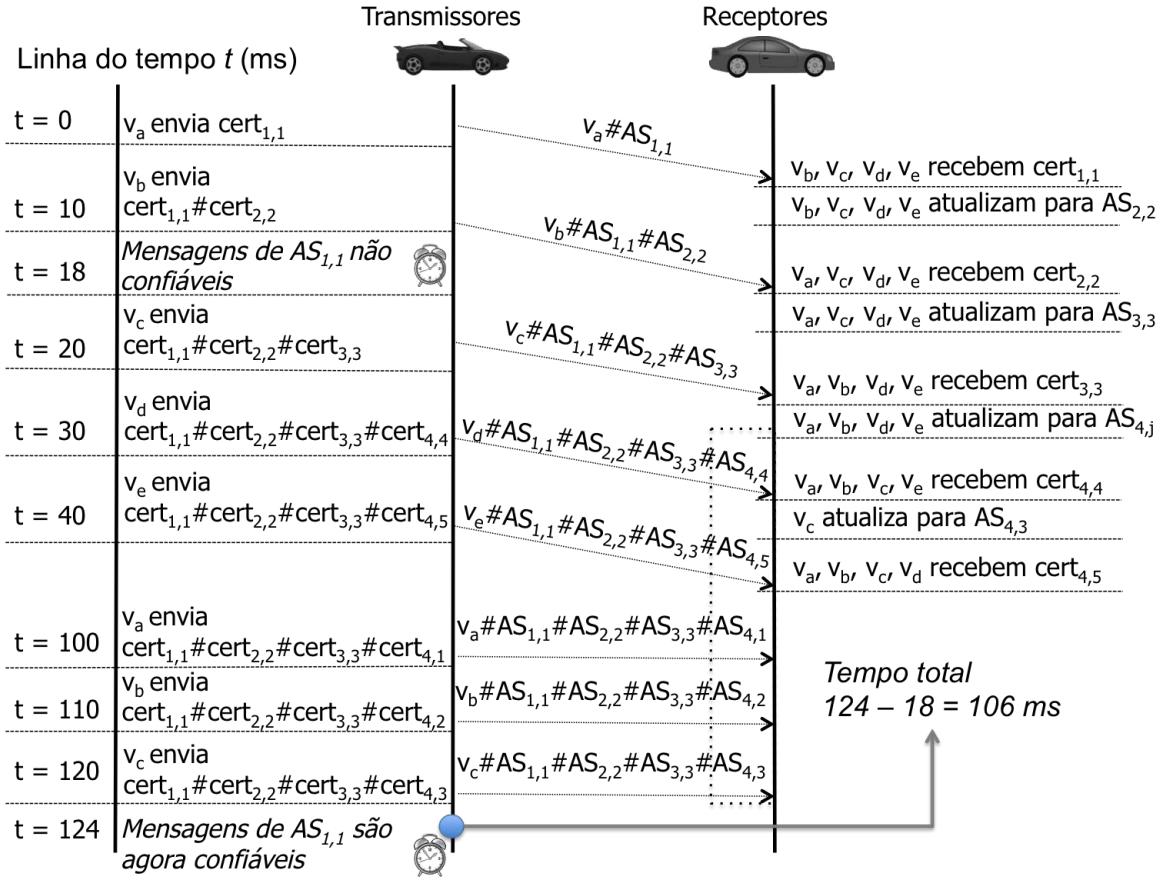


Figura 5.5: Quando o número de veículos é igual ou maior que o número de conjuntos anonimato aos quais esses veículos permanecem juntos, o tempo para detectá-los na rede como veículos legítimos está em torno do intervalo de mensagens periódicas.

legítimos, transmitindo mensagens periódicas a cada 100 *ms*, compartilham os certificados digitais de conjuntos anonimato ativos dos três primeiros níveis, e diferem apenas no certificado digital do quarto nível, o tempo total para detectar todos os veículos legítimos foi de apenas 106 *ms*.

Para tal, considere que os veículos v_a, v_b, v_c, v_d e v_e estão no mesmo raio de transmissão (ex.: $(v_a, v_c) \in E_a$ e $(v_c, v_a) \in E_c$). Ademais, suponha também que todos os veículos selecionem os mesmos certificados de conjuntos anonimato ativos para os três primeiros níveis (ex.: $cert_{AS_{1,1}}, cert_{AS_{2,2}}, cert_{AS_{3,3}}$), mas escolham um certificado digital de conjunto anonimato diferente no quarto nível (ex.: $cert_{AS_{4,1}}, cert_{AS_{4,2}}, cert_{AS_{4,3}}, cert_{AS_{4,4}}$ e $cert_{AS_{4,5}}$, respectivamente). A pergunta é: qual é o tempo médio para que outros veículos no raio de transmissão detectem cada veículo legítimo $v_a, ...v_e$? Ou seja, elimine a possibilidade de um ataque *sybil*?

Neste cenário, cada veículo transmite mensagens periódicas a cada 100 ms. Suponha também que cada veículo transmita mensagens periódicas com os pseudônimos $cert_{a,1}$, $cert_{b,1}$, $cert_{c,1}$, $cert_{d,1}$ and $cert_{e,1}$, respectivamente. No instante $t = 0$, veículo v_a trans-

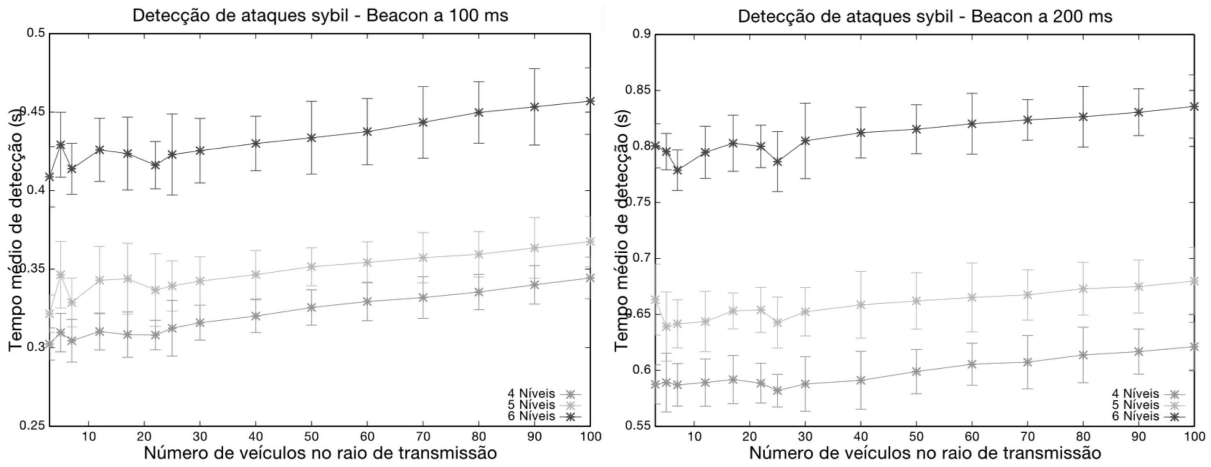
mite mensagem periódica com o certificado digital do conjunto anonimato de primeiro nível $AS_{1,1}$ ($cert_{1,1}$). Em seguida, cada veículo v_b, v_c, v_d e v_e gasta $8ms$ para verificar a autenticidade da mensagem oriunda de v_a e, uma vez que esses também selecionaram o conjunto de primeiro nível $AS_{1,1}$, todos atualizam para o conjunto $AS_{2,2}$. Desta forma, para o momento $t = 10$, o veículo v_b envia a próxima mensagem periódica com os certificados digitais $cert_{1,1}$ e $cert_{2,2}$. Igualmente, os demais veículos atualizam para $AS_{3,3}$. No instante $t = 18$, os demais veículos armazenam as mensagens oriundas de v_a e v_b como mensagens suspeitas, inicializando o tempo $\delta_{AS_{1,1}}$. No instante $t = 20$, veículo v_c envia a próxima mensagem periódica com os certificados $cert_{1,1}$, $cert_{2,2}$ e $cert_{3,3}$. Ao receberem tal mensagem, os demais veículos atualizam para $AS_{4,j}$. Neste momento, no instante $t = 30$, veículo v_d envia a próxima mensagem periódica com os certificados digitais $cert_{1,1}$, $cert_{2,2}$, $cert_{3,3}$, $cert_{4,4}$ e, após receber mensagem de v_d, veículo v_c atualiza para o quarto nível ($AS_{4,3}$). No instante $t = 40$, veículo v_e envia mensagem periódica com o certificado digital do quarto nível. A cada 100 ms depois de enviarem suas mensagens periódicas, os veículos v_a, v_b e v_c enviam novas mensagens periódicas com o certificado digital de quarto nível, respectivamente, nos instantes $t = 100$, $t = 110$ e $t = 120$. Após receber a última mensagem oriunda do veículo v_c, os demais veículos consomem 4 ms para verificar a autenticidade da mensagem de v_c e, finalmente, concluem que as mensagens com pseudônimos $cert_{a,1}$, $cert_{b,1}$, $cert_{c,1}$, $cert_{d,1}$ e $cert_{e,1}$ são confiáveis, uma vez que satisfazem a restrição da Equação 4.5, e são oriundas de veiculos legítimos. Neste momento, o tempo $\delta_{AS_{1,1}}$ é interrompido.

Com efeito, para o cenário em questão, o processo completo para detectar 5 veículos legítimos totalizou 106 ms, tempo que está próximo do intervalo de transmissão de mensagens periódicas. Consequentemente, com o mecanismo de detecção de ataques *sybil* utilizado pelo protocolo $ASAP$-V, observa-se um baixo impacto na comunicação padrão V2V principalmente por dois principais fatores, a saber: primeiro, veículos nos mesmos conjuntos anonimato atualizam os certificados digitais em blocos de pelo menos dois certificados digitais por nova mensagem a ser transmitida (ex.: v_e atualiza de $cert_{AS_{1,1}}$ para $cert_{AS_{4,5}}$); e, segundo, a probabilidade de que muitos veículos selecionarão os mesmos $m - 1$ certificados digitais de conjuntos anonimato ativos ($CERT^t_{AS_v}$) é muito pequena, como discutido na Seção 5.3.

Detecção de Ataques *Sybil*

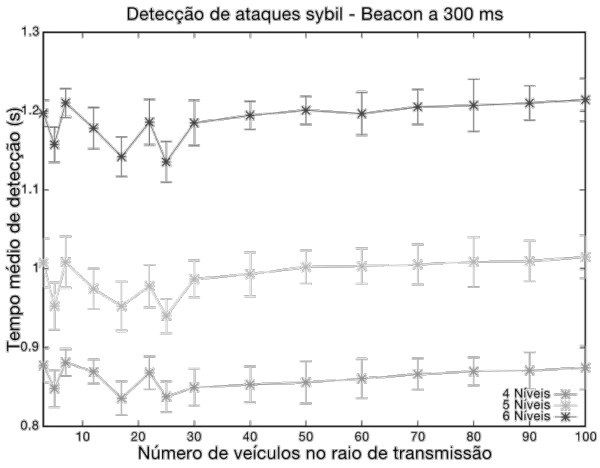
O segundo ciclo de experimentos teve como objetivo determinar o tempo médio para um veículo avaliador v_a detectar um ataque *sybil* em mensagens periódicas. Da mesma forma que apresentada na Figura 5.3, a execução do protocolo também é válida para esse cenário, porém, um veículo malicioso não poderá permitir que o tempo de espera $\delta_{AS_{1,j}}$

seja expirado. Caso isso ocorra, o efeito do ataque é eliminado antes mesmo de atingir o último nível de conjuntos anonimato. Desta forma, pode-se observar que a abordagem proposta baseada em níveis de conjuntos anonimato deve também minimizar o tempo em que um veículo malicioso mantém um ataque *sybil* em execução.



(a)

(b)



(c)

Figura 5.6: Tempo médio para detectar um veículo malicioso que explora um ataque *sybil* e transmite mensagens periódicas com os certificados digitais dos $m - 1$ conjuntos anonimato ativos.

O tempo de espera $\delta_{AS_{1,j}}$ é reinicializado a cada novo certificado digital de conjunto anonimato enviado pelo veículo malicioso, como detalhado na Seção 4.3.1. Entretanto, após o veículo malicioso apresentar seus certificados digitais de todos os níveis, o temporizador $\delta_{AS_{1,j}}$ do nó avaliador é expirado e este pode deduzir que as mensagens com os mesmos certificados digitais de conjuntos anonimato são oriundas de um nó malicioso. Finalmente, está ilustrado nos gráficos da Figura 5.6 o tempo médio para detectar um ataque *sybil*. O tempo médio para detectar o veículo malicioso é maior quando compa-

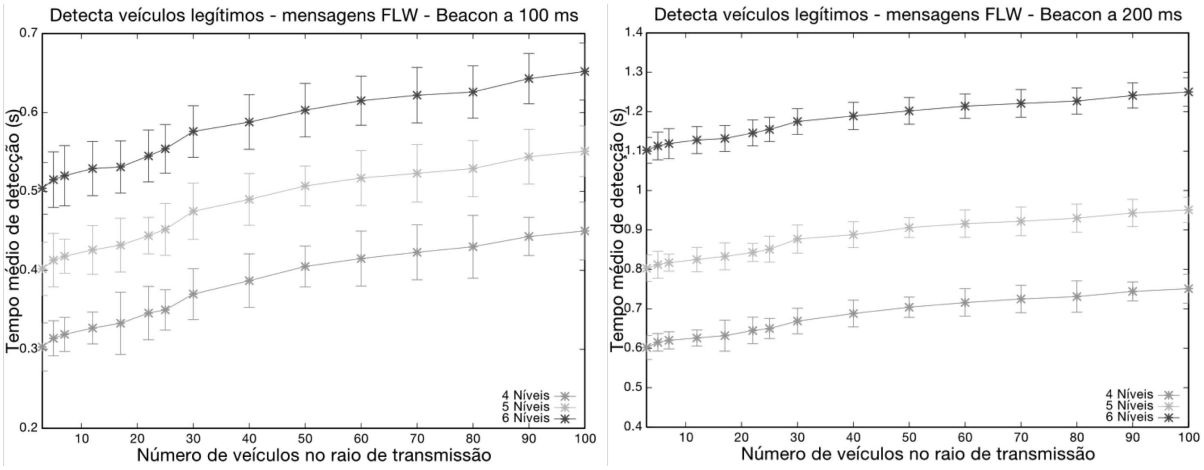
rado a um cenário com veículos legítimos pois ao receber o certificado digital do conjunto anonimato $m-1$, um veículo avaliador v_a ainda deve aguardar $\delta_{AS_{1,j}}$ ms para concluir o ataque. Devido à contenção de acesso ao meio, o tempo para detectar um veículo malicioso cresce linearmente. Outro fator que impacta neste aumento refere-se ao uso de múltiplas identidades pelo veículo malicioso v_e. Neste caso, v_e utiliza o canal por um tempo maior que um veículo legítimo. Consequentemente, veículos legítimos tendem a atrasar o envio de mensagens periódicas, aumentando o tempo de detecção.

É importante destacar que um ataque *sybil* oriundo de mensagens periódicas não tem efeitos na confiabilidade da rede se um veículo legítimo, que transmite mensagens periódicas com certificado digital do conjunto anonimato de primeiro nível $AS_{1,j}$ de um mesmo veículo malicioso, não estiver presente na região. Ou seja, se um veículo legítimo v_c transmite mensagens periódicas com certificado digital de primeiro nível $cert_{AS_{1,j}} \in CERT^t_{AS_c}$, então um veículo malicioso v_e pode explorar um ataque *sybil* com efeitos negativos a confiabilidade das mensagens de v_c se $cert_{AS_{1,j}} \in CERT^t_{AS_e}$. Caso contrário, um veículo malicioso v_e terá apenas suas mensagens armazenadas para futuras mensagens de acusação, não afetando as mensagens transmitidas pelos demais veículos no raio de transmissão. Desta forma, a abordagem do protocolo $ASAP$-V para detectar um veículo malicioso também limita os possíveis cenários de ataques *sybil* em mensagens periódicas.

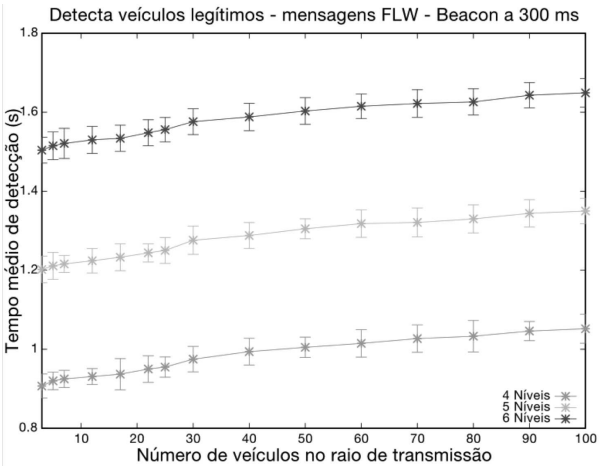
Detecção de Veículos Legítimos por Mensagens FLW

Nesta seção, apresentam-se os resultados para detectar dois veículos legítimos v_a e v_c em cenários de desvanecimento das forças dos sinais transmitidos por ambos. Mensagens FLW são enviadas pelos veículos no raio de transmissão com o objetivo de evitar detecções *falso-positivo*.

Estão ilustrados nos gráficos da Figura 5.7 o tempo médio e os respectivos intervalos de confiança para que um nó avaliador v_b detecte ambos os veículos v_a e v_c como legítimos. À medida que o número de veículos aumenta, o tempo médio também aumenta linearmente. Este comportamento se deve principalmente por dois motivos, a saber: primeiro, um cenário de *terminal oculto* [202], pois como v_a e v_c não recebem os sinais transmitidos por ambos, então há uma ocorrência maior de colisões de pacotes quando veículos no raio de transmissão recebem mensagens de v_a e v_c ao mesmo tempo; e, segundo, ambos os veículos não adicionam os certificados digitais de conjuntos anonimato em blocos de dois em dois, como discutido na Seção 5.5.2, mas sim de forma sincronizada um a um.



(a) (b)



(c)

Figura 5.7: Tempo médio para detectar dois veículos legítimos em cenários de desvanecimento das forças dos sinais transmitidos por ambos.

5.6 Comparativo entre as Soluções

Nesta seção, buscou-se elaborar, sucintamente, um comparativo com pelo menos uma abordagem para cada categoria de detecção de ataques *sybil*, tais como as baseadas em suporte de pontos fixos, as baseadas em relação espaço/tempo e as baseadas em monitoramento de veículos vizinhos. Sob a ótica de categorização de soluções, as discussões apresentadas a seguir também podem ser aplicadas para outras abordagens existentes.

A abordagem proposta por Zhou et al [53, 54], chamada P^2DAP, permite o prévio armazenamento de múltiplas identidades e faz uso de RSUs e C.As para detectar potencial ataques *sybil*. Entretanto, como ilustrado no gráfico da Figura 5.8, o tempo mínimo para detectar um ataque *sybil* ultrapassa os 20 segundos, inviabilizando diversos cenários reais em ambientes veiculares. Este tempo é ocasionado devido principalmente à dois fatores, a saber: a sobrecarga de mensagens enviadas para a RSU e para a C.A; e a quantidade

de identidades suspeitas identificadas nas mensagens periódicas. Os resultados foram obtidos considerando 3 mensagens periódicas por segundo (ou um período de 300 *ms*). Para este mesmo cenário (período de mensagens periódicas e quantidade de nós na rede), o protocolo proposto neste trabalho é capaz de detectar um veículo malicioso em menos de 1,5 segundo, inferior em 90%.

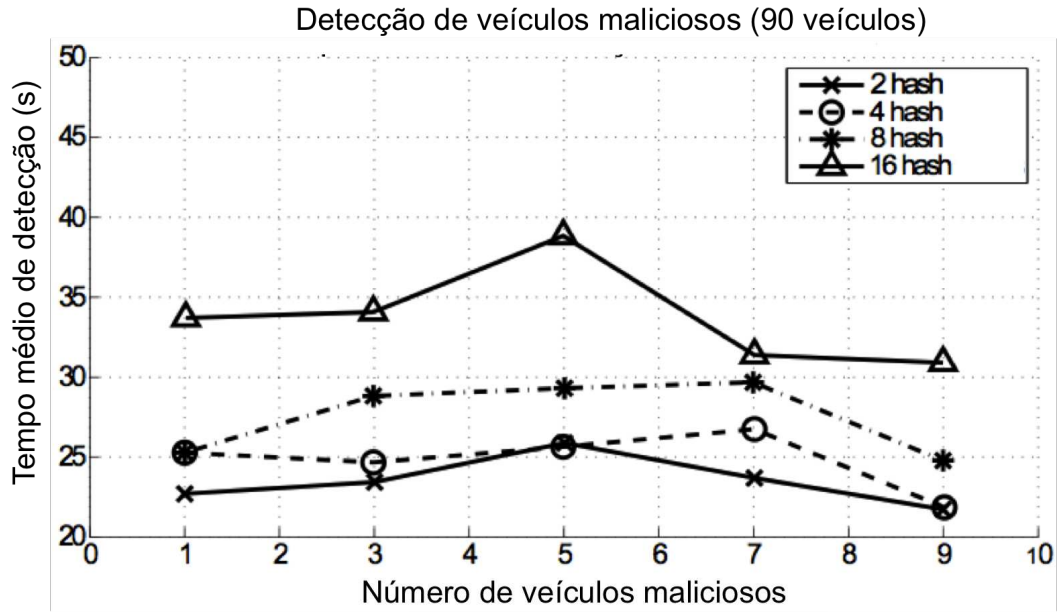


Figura 5.8: Tempo de detecção de ataques *sybil* da proposta P^2DAP inviabiliza cenários reais (Adaptada de: [54]).

Em uma outra vertente, as soluções que exploram a relação espaço/tempo podem gerar resultados *falso-positivo* e *falso-negativo* devido à dinâmica do fluxo de veículos na rodovia. Tais resultados ocorrem, respectivamente, quando um veículo legítimo é detectado como *sybil*, e quando veículo *sybil* não é detectado. Como ilustrado no gráfico da Figura 5.9, dependendo da quantidade de RSUs disponíveis nas rodovias, a taxa de resultados *falso-positivo* pode chegar a aproximadamente 50%, embora apresente baixa taxa de resultados *falso-negativo* [58]. O tempo de detecção dependerá do esquema de assinaturas digitais a ser utilizado para a geração de marcas de tempo. Por outro lado, o protocolo $ASAP$-V proposto neste trabalho de tese é resiliente a resultados *falso-positivo* e *falso-negativo*.

Estão ilustrados nos gráficos das Figuras 5.10 e 5.11 a taxa de detecção de ataques *sybil* e as taxas de detecção *falso-positivo* e *falso-negativo* considerando a abordagem proposta por Grover et al [62] para 40 veículos no raio de transmissão. Tal abordagem realiza um monitoramento dos veículos vizinhos para detectar ataques *sybil* partindo da hipótese de que, à medida que um veículo se desloca, identidades oriundas de veículos maliciosos são continuamente apresentadas em mensagens periódicas para um dado intervalo de tempo.

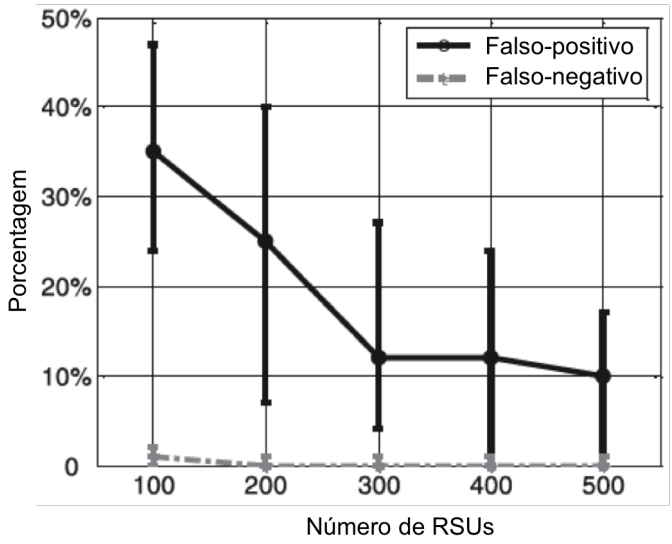


Figura 5.9: Resultados *falso-positivo* e *falso-negativo* podem ser gerados em soluções que exploram a relação espaço/tempo (Adaptada de: [58]).

No geral, Grover concluiu que o tempo ideal de monitoramento de veículos vizinhos está em torno de 80 segundos, uma vez que as taxas de *falso-positivo* e *falso-negativo* são pequenas. Novamente, tempo considerado inviável para diversos cenários de aplicações reais em ambientes veiculares. Para o mesmo cenário, o protocolo *ASAP*-V detecta ataques *sybil* com tempo médio de 1.5 segundos, de aproximadamente 90% inferior.

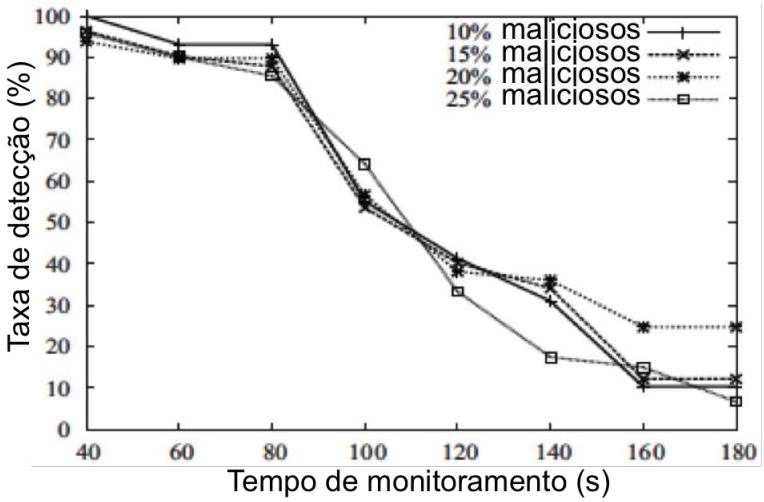
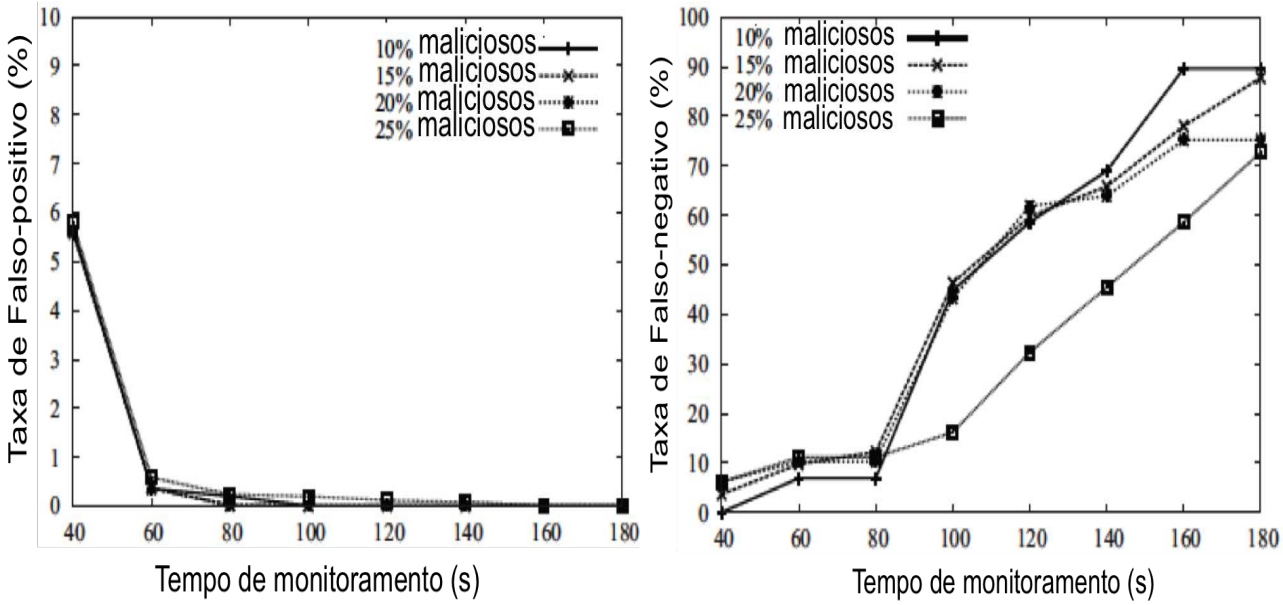


Figura 5.10: Taxa de detecção de ataques *sybil* para a abordagem de monitoramento e colaboração de nós vizinhos (Adaptada de: [62]).

À medida que o tempo de monitoramento (*threshold*) de nós vizinhos aumenta, as taxas de detecção de ataque *sybil* e de resultados *falso-positivo* diminuem, e a taxa de *falso-negativo* aumenta. A partir de uma análise de deslocamento dos veículos, é natural observar que a presença de diferentes identidades em um intervalo de tempo (ex.: *threshold*

= 40) não caracteriza, necessariamente, que tais identidades são oriundas de um ataque *sybil*, isto é, diferentes veículos podem permanecer próximos por tempo indeterminado. Desta forma, para um intervalo de tempo de monitoramento relativamente curto, a taxa de detecção *falso-positivo* tende a ser maior, uma vez que a probabilidade de que diferentes veículos estarão juntos (ou diferentes identidades estarão juntas) é alta.



(a) Taxa de detecção *falso-positivo*.

(b) Taxa de detecção *falso-negativo*.

Figura 5.11: Resultados *falso-positivo* e *falso-negativo* para a abordagem de monitoramento e colaboração de nós vizinhos (Adaptadas de: [62]).

5.7 Considerações Finais

Neste capítulo, foram apresentados os principais resultados alcançados com a presente pesquisa de tese. O capítulo contemplou inicialmente uma análise do protocolo de autenticação e do modelo de controle de anonimato propostos, prosseguindo com uma avaliação da sobrecarga computacional imposta pelo protocolo *ASAP*-V e dos principais resultados no que tange o tempo para detectar veículos legítimos e ataques *sybil*. Por fim, foi realizada uma comparação com uma abordagem de cada categoria introduzida no Capítulo 3, selecionadas por terem apresentado resultados mais eficientes e uma arquitetura mais robusta na detecção de ataques *sybil*.

Na etapa inicial do presente trabalho, fundamentou-se inicialmente três hipóteses, a saber: o uso do esquema de assinatura de grupo para autenticação e não-repúdio de mensagens com suporte ao anonimato das mensagens trafegadas na rede; a aplicação do modelo de conjuntos anonimato como mecanismo para proporcionar níveis de privaci-

dade durante detecção de ataques *sybil*; e, por fim, a existência de uma combinação de atributos para cada veículo específico que o diferencie, ao menos temporariamente, dos demais veículos no sistema, permitindo, assim, detectar ataques *sybil* sem a presença de infraestruturas fixas ou mecanismos de confiança e reputação, enquanto provê o controle de anonimato dos usuários.

Para a primeira hipótese, o esquema de assinaturas de grupo permitiu definir um esquema em que uma mensagem seja autenticada, embora a real identidade da origem da mensagem seja preservada. Desta forma, o processo de negociação de identidades temporárias do protocolo *ASAP*-V dificulta a construção de um perfil de rotas baseado em RSUs ou até mesmo baseado no monitoramento das mensagens transmitidas. Além disso, o esquema de assinaturas de grupo permite identificar a real identidade de um veículo durante a fase de acusação de ataques *sybil* (Fase 4), garantindo mecanismos de não-repúdio.

Para a segunda hipótese, mensagens transmitidas na rede não poderão ser exclusivamente associadas a uma identidade real de um usuário apenas a partir do certificado digital do primeiro nível. Desta forma, a partir de uma análise baseada na entropia de Shannon, pôde-se observar que o protocolo *ASAP*-V provê controle de anonimato (principalmente na fase de detecção de ataques *sybil*) uma vez que a probabilidade de que dois ou mais veículos escolherão os mesmos certificados de $m - 1$ conjuntos anonimato ativos é baixa.

Por fim, para a terceira hipótese, foram definidos múltiplos conjuntos anonimato, organizados em uma estrutura de múltiplos níveis. Cada conjunto tem a ele associado um atributo (certificado digital), o qual é compartilhado entre os veículos pertencentes ao mesmo conjunto. A partir desta arquitetura, foi possível definir uma abordagem para detectar ataques *sybil* em um tempo inferior às abordagens encontradas na literatura, e sem a participação direta de infraestruturas fixas. Ademais, o protocolo *ASAP*-V é resiliente a detecções *falso-positivo* e *falso-negativo* pois mensagens FLW disseminam informações sobre veículos nos mesmos conjuntos anonimato, evitando, assim, detecções *falso-positivo*, e mensagens com os mesmos certificados digitais de conjuntos anonimato são previamente armazenadas como suspeitas, sendo posteriormente informadas ao sistema (C.A) através do mecanismo de acusação (Fase 4) e evitando, desta forma, resultados *falso-negativo*.

Capítulo 6

Conclusão

O uso de múltiplas identidades para prover autenticação e controle de anonimato em redes VANETs permite que um veículo malicioso realize um ataque denominado *sybil*. A principal motivação para o desenvolvimento deste trabalho de tese é o impacto negativo trazido por tal ataque na qualidade dos serviços providos por uma rede veicular, incluindo, por exemplo, o mau funcionamento dos algoritmos de roteamento e a probabilidade de disseminação de eventos falsos sobre o tráfego de veículos. Ademais, o *trade-off* entre os requisitos de autenticação e controle de anonimato, com a capacidade de detectar um ataque *sybil*, dificulta a construção de uma solução efetiva na detecção confiável de veículos maliciosos.

Nesta perspectiva, o objetivo central desta tese foi o desenvolvimento de um protocolo para autenticação de veículos e detecção de ataques *sybil* em VANETs, visando também prover suporte ao controle de anonimato dos usuários. Com efeito, a solução proposta, denominada *ASAP*-V, desenvolveu-se seguindo uma direção situada inicialmente num levantamento bibliográfico e análise das soluções encontradas na literatura, em particular, nas abordagens para detecção de ataques *sybil* com suporte ao controle de anonimato.

Percebeu-se, então, que tais abordagens apresentavam diversas limitações, a saber: não são efetivas na detecção de nós maliciosos, permitindo que esses não sejam detectados ou que nós legítimos fossem detectados como maliciosos; possuem dependência de infraestruturas fixas, tais como RSU e/ou C.A; e apresentam um tempo médio elevado para detectar ataques *sybil*, inviabilizando cenários reais dentro do contexto de transporte urbano.

A partir da identificação destes problemas, o protocolo *ASAP*-V foi concebido. Foi introduzida uma abordagem baseada numa arquitetura em múltiplos níveis de conjuntos anonimato, aliado aos esquemas de pseudônimos e assinaturas de grupo para detectar ataques *sybil* e, ao mesmo tempo, manter o controle de anonimato dos usuários.

Com base na análise formal e em experimentos utilizando simuladores, observou-se a

viabilidade da solução e a eficiência do protocolo *ASAP*-V para detectar veículos legítimos e maliciosos com um tempo 90% inferior quando comparado com as demais abordagens encontradas na literatura. O controle de anonimato e a detecção de ataques *sybil* são garantidos uma vez que a probabilidade é cada vez menor de que dois ou mais veículos, situados no mesmo raio de transmissão, compartilharão os mesmos certificados digitais de conjuntos anonimato em diferentes níveis.

A seguir, são apresentadas as principais contribuições da presente pesquisa e as perspectivas futuras do presente trabalho.

6.1 Contribuições

Em linhas gerais, com o desenvolvimento desta tese, contribui-se para a área de segurança em redes veiculares (VANETs), oferecendo uma abordagem original para autenticação, controle de anonimato e detecção de ataques *sybil* em VANETs. Pode-se pontuar também as seguinte contribuições verticais:

- **Uma nova abordagem para autenticação de veículos**: foi proposto um novo protocolo para autenticação de veículos com suporte ao controle de anonimato. Através dos esquemas de assinaturas de grupo e pseudônimos, o protocolo de autenticação permite que um veículo armazene múltiplas identidades e que veículos maliciosos, uma vez identificados, não possam obter novas identidades. Ademais, apesar do uso de diferentes esquemas de criptografia, um veículo pode processar uma quantidade suficiente de mensagens em um curto intervalo de tempo;

- **Uma arquitetura multinível para agrupamento de veículos**: foi definida uma arquitetura multinível de conjuntos anonimato, permitindo que veículos compartilhem um subconjuto de atributos. Desta forma, torna-se mais complexa a identificação de uma mensagem transmitida na rede e, consequentemente, a potencial violação de anonimato de um veículo específico;

- **Um protocolo para acusação de veículos maliciosos**: foi definido um protocolo para informar a um sistema de gerenciamento de redes veiculares potenciais ataques detectados na rede. Desta forma, pode-se identificar um veículo malicioso através das assinaturas de grupo, tomar medidas preventivas e evitar que veículos maliciosos continuem executando os ataques;

- **Descentralização do processo de detecção de ataques *sybil***: foi desenvolvida uma abordagem para detectar ataques *sybil* de forma distribuída e independente da presença de uma infraestrutura fixa. Desta forma, o protocolo *ASAP*-V é capaz de

detectar ataques *sybil* mesmo sem a presença física de uma RSU e conectividade com uma C.A. Ou seja, se um ataque *sybil* é explorado em conjunto com outros ataques de rede mais sofisticados, tal como DoS/DDoS executados contra RSUs e C.As, o protocol *ASAP*-V pode ainda detectar o veículo malicioso;

- **Resiliência a detecções *falso-positivo* e *falso-negativo***: a abordagem proposta para detectar ataques *sybil* é imune a resultados *falso-positivo* - ou seja, quando um veículo legítimo é detectado como malicioso - e *falso-negativo* - quando um veículo malicioso não é detectado como tal. Assim, o protocolo *ASAP*-V torna-se mais confiável e impede que serviços de rede, tais como algoritmos de roteamento, sejam afetados pela presença de nós maliciosos ou pela disseminação de informações inconsistentes sobre veículos legítimos.

6.2 Perspectivas Futuras

Como trabalhos futuros, pode-se investigar as seguintes linhas de pesquisa:

- **Avaliação da qualidade do canal para estimar intervalos de espera**: durante a fase de detecção de ataques *sybil* em mensagens periódicas, o tempo de espera máximo que um nó avaliador deve aguardar por novos certificados digitais de conjuntos anonimato pode também levar em consideração, além do número de nós, o estado atual da rede. Desta forma, pode-se considerar na Equação 4.6 dados adicionais que caracterizem a *qualidade do canal* de transmissão. Nesse contexto, há duas variáveis que podem ser aplicadas, a saber: número de colisões observados no canal; e a relação sinal-ruído (SNR, do inglês *Signal to Noise Ratio*). A mesma análise é proposta por Sommer et. al. [90] para adaptar o intervalo de envio de mensagens periódicas;

- **Controle de Anonimato**: sob a perspectiva de controle de anonimato, pode-se utilizar mineração de dados e/ou técnicas de Big Data [203] para avaliar a probabilidade de construção de rotas de um veículo específico. Esta abordagem é chamada de *de-anonimato* e tem sido foco de diversas pesquisas na área de controle de privacidade na Web [204, 205], bem como em serviços baseados em localização para redes veiculares [164]. Ademais, deve-se considerar, para futuras análises do controle de anonimato, a estimativa do tempo δ_{CERT} o qual limita a transição entre dois conjuntos de certificados digitais de conjuntos anonimato ativos;

- **Arquitetura multinível heterogênia**: estudar o protocolo *ASAP*-V utilizando diferentes abordagens para distribuição dos veículos nos conjuntos anonimato. Como

exemplo, pode-se considerar a alocação de veículos em quantidades variadas de conjuntos por nível, e uma quantidade variada de conjuntos anonimato por nível;

- **Técnicas para estimar potências de sinais recebidas em ambientes veiculares**: pode-se investigar e estudar técnicas para estimar potências de sinais recebidos entre os nós em ambientes veiculares. Tais ambientes possuem características peculiares e que podem impactar negativamente na qualidade do sinal transmitido;

- **Avaliação do protocolo *ASAP*-V em cenários de execução híbrida**: nesse contexto, dois veículos legítimos, os quais se deslocam em direções opostas, transmitem mensagens com os mesmos certificados digitais de conjuntos anonimatos. À medida que se afastam um do outro, o protocolo *ASAP*-V entra na fase de transmissão de mensagens FLW. Por fim, pode-se, então, avaliar o comportamento do protocolo no tocante ao tempo para detectar ambos os veículos.

Referências Bibliográficas

[1] C. Liu and J. Kaiser. *A survey of mobile ad hoc network routing protocols*. Universität Ulm, Fakultät für Informatik., 2003.

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

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

[4] Kamini Kamini and Rakesh Kumar. VANET parameters and applications: A review. *Global Journal of Computer Science and Technology*, 10(7), 2010.

[5] IEEE. IEEE approved draft standard for wireless access in vehicular environments - security services for applications and management messages. pages 1–289, 2012.

[6] R. Hussain, S. Kim, and H. Oh. Towards privacy aware pseudonymless strategy for avoiding profile generation in VANET. *Information Security Applications*, pages 268–280, 2009.

[7] F. Dötzer. Privacy issues in vehicular ad hoc networks. In *Privacy Enhancing Technologies*, pages 197–209. Springer, 2006.

[8] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computuer Security*, 15(1):39–68, January 2007.

[9] Albert Wasef, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. Complementing public key infrastructure to secure vehicular ad hoc networks. *Wireless Communications*, 17(5):22–28, October 2010.

[10] Albert Wasef, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. *Managing and Complementing Public Key Infrastructure for Securing Vehicular Ad Hoc Networks*. PhD thesis, University of Waterloo, 2011.

[11] Amira Bradai and Hossam Afifi. A framework using ibc achieving non-repudiation and privacy in vehicular network. In *Network and Information Systems Security (SAR-SSI), 2011 Conference on*, pages 1–6. IEEE, 2011.

[12] Andreas Pfitzmann and Marit Hansen. Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology. Technical report, February 2008.

[13] Jason J Haas, Yih-Chun Hu, and Kenneth P Laberteaux. The impact of key assignment on VANET privacy. *Security and Communication Networks*, 3(2-3):233–249, 2010.

[14] John R. Douceur. The sybil attack. In *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, IPTPS '01, pages 251–260, London, UK, UK, 2002. Springer-Verlag.

[15] K. Garg, A. Agarwal, M. Gaikwad, S. Nanwani, and V. Inamdar. Sybil-a tricky facsimile. In *Engineering Education: Innovative Practices and Future Trends (AICERA), 2012 IEEE International Conference on*, pages 1–3. IEEE, 2012.

[16] Hsu-Chun Hsiao, Ahren Studer, Rituik Dubey, Elaine Shi, and Adrian Perrig. Efficient and secure threshold-based event validation for VANETs. In *Proceedings of the fourth ACM conference on Wireless network security*, pages 163–174. ACM, 2011.

[17] Mahmoud Al-Qutayri, Chan Yeun, and Faisal Al-Hawi. Security and privacy of intelligent VANETs. In *Computational Intelligence and Modern Heuristics*, chapter 13. InTech, 2010.

[18] Rasheed Hussain, Sangjin Kim, and Heekuck Oh. Privacy-aware VANET security: Putting data-centric misbehavior and sybil attack detection schemes into practice. 7690:296–311, 2012.

[19] Y. Zhang and Guohong Cao. V-pada: Vehicle-platoon-aware data access in VANETs. *IEEE Transactions on Vehicular Technology*, 60(5):2326–2339, 2011.

[20] Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels, and J-P Hubaux. Eviction of misbehaving and faulty nodes in vehicular networks. *Selected Areas in Communications, IEEE Journal on*, 25(8):1557–1568, 2007.

[21] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and correcting malicious data in VANETs. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 29–37. ACM, 2004.

[22] Mainak Ghosh, Anitha Varghese, Arobinda Gupta, Arzad A Kherani, and Skanda N Muthaiah. Detecting misbehaviors in VANET with integrated root-cause analysis. *Ad Hoc Networks*, 8(7):778–790, 2010.

[23] Sushmita Ruj, Marcos Antonio Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic. On data-centric misbehavior detection in VANETs. In *Vehicular Technology Conference (VTC Fall), 2011 IEEE*, pages 1–5. IEEE, 2011.

[24] Tim Leinmüller and Elmar Schoch. Greedy routing in highway scenarios: The impact of position faking nodes. In *Proceedings of Workshop On Intelligent Transportation (WIT 2006)(Mar. 2006)*, 2006.

[25] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, 1(2):293–315, 2003.

[26] J. Grover, D. Kumar, M. Sargurunathan, MS Gaur, and V. Laxmi. Performance evaluation and detection of sybil attacks in vehicular ad-hoc networks. *Recent Trends in Network Security and Applications*, pages 473–482, 2010.

[27] Hélio Almeida, Tiago Macambira, Dorgival Guedes, Virgílio Almeida, and Wagner Meira Jr. Um sistema de reputação resistente a ataques sybil para redes overlay. pages 63–74. Anais do III Workshop em Peer-to-Peer (WP2P), 2007.

[28] Gustavo Huff Mauch. Dois pesos, duas medidas : gerenciamento de identidades orientado a desafios adaptativos para contenção de sybils. Master's thesis, Universidade Federal do Rio Grande do Sul, 2010.

[29] Brad Karp and Hsiang-Tsung Kung. Gpsr: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254. ACM, 2000.

[30] Si-Ho Cha. Comparison of greedy routing protocols for vehicular ad hoc networks. In *ICT Convergence (ICTC), 2012 International Conference on*, pages 565–566, 2012.

[31] Hao Wu, Richard Fujimoto, Randall Guensler, and Michael Hunter. Mddv: a mobility-centric data dissemination algorithm for vehicular networks. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, VANET '04, pages 47–56, New York, NY, USA, 2004. ACM.

[32] Fan Li and Yu Wang. Routing in vehicular ad hoc networks: A survey. *Vehicular Technology Magazine, IEEE*, 2(2):12–22, 2007.

[33] Charles E Perkins and Elizabeth M Royer. Ad-hoc on-demand distance vector routing. In *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on*, pages 90–100. IEEE, 1999.

[34] Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, and Jang-Ping Sheu. The broadcast storm problem in a mobile ad hoc network. In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, MobiCom '99, pages 151–162, New York, NY, USA, 1999. ACM.

[35] Leandro A. Villas, Heitor S. Ramos, Azzedine Boukerche, Daniel L. Guidoni, Regina B. Araujo, and Antonio A.F. Loureiro. An efficient and robust data dissemination protocol for vehicular ad hoc networks. In *Proceedings of the 9th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, PE-WASUN '12, pages 39–46, New York, NY, USA, 2012. ACM.

[36] Gökhan Korkmaz, Eylem Ekici, Füsun Özgüner, and Ümit Özgüner. Urban multi-hop broadcast protocol for inter-vehicle communication systems. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 76–85. ACM, 2004.

[37] Ozan K Tonguz, Nawaporn Wisitpongphan, and Fan Bai. Dv-cast: A distributed vehicular broadcast protocol for vehicular ad hoc networks. *Wireless Communications, IEEE*, 17(2):47–57, 2010.

[38] Mohamed Bakhouya, Jaafar Gaber, and Pascal Lorenz. An adaptive approach for information dissemination in vehicular ad hoc networks. *Journal of Network and Computer Applications*, 34(6):1971–1978, 2011.

[39] Harshvardhan P Joshi, Mihail L Sichitiu, and Maria Kihl. Distributed robust geocast multicast routing for inter-vehicle communication. In *Proceedings of WEIRD Workshop on WiMax, Wireless and Mobility*, pages 9–21, 2007.

[40] Yuh-Shyan Chen, Yun-Wei Lin, and Sing-Ling Lee. A mobicast routing protocol in vehicular ad-hoc networks. *Mobile Networks and Applications*, 15(1):20–35, 2010.

[41] Min-Te Sun, Wu-Chi Feng, Ten-Hwang Lai, Kentaro Yamada, Hiromi Okada, and Kikuo Fujimura. Gps-based message broadcast for adaptive inter-vehicle communications. In *Vehicular Technology Conference, 2000. IEEE VTS-Fall VTC 2000. 52nd*, volume 6, pages 2685–2692. IEEE, 2000.

[42] K. Kaur, S. Batish, and A. Kakaria. Survey of various approaches to countermeasure sybil attack. *International Journal of Computer Science and Informatics*, 1, 2012.

[43] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pages 259–268. ACM, 2004.

[44] D. Monica, J. Leitao, L. Rodrigues, and C. Ribeiro. On the use of radio resource tests in wireless ad hoc networks. In *Proceedings of the 3rd Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS)*, pages 21–26, 2009.

[45] D.M.C. e Castro and M. Oliveira. Thwarting the sybil attack in wireless ad hoc networks. 2009.

[46] Yong Hao, Yu Chengcheng, Chi Zhou, and Wei Song. A distributed key management framework with cooperative message authentication in VANETs. *IEEE J.Sel. A. Commun.*, 29(3):616–629, March 2011.

[47] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, and Pin-Han Ho. Raise: An efficient rsu-aided message authentication scheme in vehicular communication networks. In *Communications, 2008. ICC '08. IEEE International Conference on*, pages 1451–1457, may 2008.

[48] M. Verma and D. Huang. Segcom: secure group communication in VANETs. In *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*, pages 1–5. IEEE, 2009.

[49] Bayrem Triki, Slim Rekhis, Mhadmed Chammem, and Boudriga Noureddine. A privacy preserving solution for the protection against sybil attacks in vehicular ad hoc networks. *IFIP Wireless and Mobile Networking Conference*, 2013.

[50] Jyoti Grover, Manoj Singh Gaur, and Vijay Laxmi. A novel defense mechanism against sybil attacks in VANET. In *Proceedings of the 3rd international conference on Security of information and networks*, pages 249–255. ACM, 2010.

[51] B. Xiao, B. Yu, and C. Gao. Detection and localization of sybil nodes in VANETs. In *International Conference on Mobile Computing and Networking: Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, volume 26, pages 1–8. Citeseer, 2006.

[52] Jyoti Grover, Manoj Singh Gaur, and Vijay Laxmi. Position forging attacks in vehicular ad hoc networks: Implementation, impact and detection. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, pages 701–706. IEEE, 2011.

[53] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty. Privacy-preserving detection of sybil attacks in vehicular ad hoc networks. In *Mobile and Ubiquitous Systems: Networking & Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on*, pages 1–8. IEEE, 2007.

[54] T. Zhou, R.R. Choudhury, P. Ning, and K. Chakrabarty. P2dap-sybil attacks detection in vehicular ad hoc networks. *Selected Areas in Communications, IEEE Journal on*, 29(3):582–594, 2011.

[55] T.J. Wu, W. Liao, and C.J. Chang. A cost-effective strategy for road-side unit placement in vehicular networks. *IEEE Transactions on Communications*, 60(8):2295–2303, 2012.

[56] O. Trullols, M. Fiore, C. Casetti, C.F. Chiasserini, and J.M. Barcelo Ordinas. Planning roadside infrastructure for information dissemination in intelligent transportation systems. *Computer Communications*, 33(4):432–442, 2010.

[57] Evellyn S. Cavalcante, André L.L. Aquino, Gisele L. Pappa, and Antonio A.F. Loureiro. Roadside unit deployment for information dissemination in a VANET: an evolutionary approach. In *Proceedings of the fourteenth international conference on Genetic and evolutionary computation conference companion*, GECCO Companion '12, pages 27–34, New York, NY, USA, 2012. ACM.

[58] Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao, and Xuemin Shen. Footprint: Detecting sybil attacks in urban vehicular networks. *IEEE Transactions on Parallel and Distributed Systems*, 23(6):1103–1114, 2012.

[59] Chen Chen, Xin Wang, Weili Han, and Binyu Zang. A robust detection of the sybil attack in urban VANETs. In *Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on*, pages 270–276. IEEE, 2009.

[60] S. Park, B. Aslam, D. Turgut, and C.C. Zou. Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In *Military Communications Conference, 2009. MILCOM 2009. IEEE*, pages 1–7. IEEE, 2009.

[61] C. Piro, C. Shields, and B.N. Levine. Detecting the sybil attack in mobile ad hoc networks. In *Securecomm and Workshops, 2006*, pages 1–11. IEEE, 2006.

[62] J. Grover, M.S. Gaur, V. Laxmi, and N.K. Prajapati. A sybil attack detection approach using neighboring vehicles in vanet. In *Proceedings of the 4th international conference on Security of information and networks*, pages 151–158. ACM, 2011.

[63] Yong Hao, Jin Tang, and Yu Cheng. Cooperative sybil attack detection for position based applications in privacy preserved vanets. In *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pages 1–5. IEEE, 2011.

[64] Athichart Tangpong, George Kesidis, Hung-yuan Hsu, and Ali Hurson. Robust sybil detection for manets. In *Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th Internatonal Conference on*, pages 1–6. IEEE, 2009.

[65] Muhammad Al-Mutaz, Levi Malott, and Sriram Chellappan. Detecting sybil attacks in vehicular networks. *Journal of Trust Management*, 1(1):4, 2014.

[66] D. Chaum and E. Van Heyst. Group signatures. In *Advances in Cryptology-EUROCRYPT'91*, pages 257–265. Springer, 1991.

[67] Latanya Sweeney. k-anonymity: a model for protecting privacy. *International. Journal of Uncertainty Fuzziness Knowledge.-Based Systems.*, 10(5):557–570, October 2002.

[68] Jakob Jonsson and Burt Kaliski. Public-key cryptography standards (pkcs)# 1: Rsa cryptography specifications version 2.1. 2003.

[69] Neal Koblitz. Elliptic curve cryptography. *Mathematics of Computation*, 48(177), 1987.

[70] Shyang-Lih Chang, Li-Shien Chen, Yun-Chung Chung, and Sei-Wan Chen. Automatic license plate recognition. *IEEE Transactions on Intelligent Transportation Systems*, 5(1):42–53, 2004.

[71] George Danezis and Stefan Schiffner. On network formation,(sybil attacks and reputation systems). In *DIMACS Workshop on Information Security Economics*, pages 18–19, 2006.

[72] F. Pontes, F. Brasileiro, and N. Andrade. Sobre calotes e múltiplas personalidades no bittorrent. *Campina Grande, PB, Brasil. Departamento de Sistemas e Computação*, 2007.

[73] Ali Bohlooli and Kamal Jamshidi. A gps-free method for vehicle future movement directions prediction using som for VANET. *Applied Intelligence*, 36:685–697, 2012.

[74] Nivedita N.Kadam Uma Nagaraj. Study of statistical models for route prediction algorithms in VANET. *Journal of Information Engineering and Applications*, 1(4):28–33, 2011.

[75] P. Lytrivis, G. Thomaidis, M. Tsogas, and A. Amditis. An advanced cooperative path prediction algorithm for safety applications in vehicular networks. *Trans. Intell. Transport. Sys.*, 12(3):669–679, September 2011.

[76] Al-Sakib Khan Pathan. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. Auerbach Pub, 2010.

[77] Jolyon Clulow and Tyler Moore. Suicide for the common good: a new strategy for credential revocation in self-organizing systems. *ACM SIGOPS Operating Systems Review*, 40(3):18–21, 2006.

[78] Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels, and J-P Hubaux. Eviction of misbehaving and faulty nodes in vehicular networks. *Selected Areas in Communications, IEEE Journal on*, 25(8):1557–1568, 2007.

[79] Hiroshi Sekido, Tadashi Sakuma, and Toshimichi Hioki. Vehicle seat with automatic adjustment mechanisms utilizing inflatable air bags, January 21 1992. US Patent 5,082,326.

[80] Yunxin(Jeff) Li. An overview of the dsrc/wave technology. In Xi Zhang and Daji Qiao, editors, *Quality, Reliability, Security and Robustness in Heterogeneous Networks*, volume 74 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 544–558. Springer Berlin Heidelberg, 2012.

[81] Prasan Kumar Sahoo, Ming-Jer Chiang, and Shih-Lin Wu. SVANET: A smart vehicular ad hoc network for efficient data transmission with wireless sensors. *Sensors*, 14(12):22230–22260, 2014.

[82] Daniel Jiang and Luca Delgrossi. Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2036–2040. IEEE, 2008.

[83] Yunxin Jeff Li. An overview of the dsrc/wave technology. pages 544–558, 2012.

[84] Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments. *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)*, pages 1–51, 2010.

[85] Vaishali D Khairnar and Ketan Kotecha. Performance of vehicle-to-vehicle communication using ieee 802.11p in vehicular ad-hoc network environment. *arXiv preprint arXiv:1304.3357*, 2013.

[86] M.J. Booysen. Performance comparison of media access control protocols for vehicular ad hoc networks. *IET Networks*, 1:10–19(9), March 2012.

[87] TS ETSI. 102 637-2, intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of co-operative awareness basic service. *ETSI, Sophia Antipolis Cedex, France*, 2010.

[88] TS ETSI. 102 637-2, intelligent transport systems (its); vehicular communications; basic set of applications; part 3: Specifications of decentralized environmental notification basic service. *ETSI, Sophia Antipolis Cedex, France*, 2010.

[89] Hoa-Hung Nguyen, Adhitya Bhawiyuga, and Han-You Jeong. A comprehensive analysis of beacon dissemination in vehicular networks. In *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th*, pages 1–5. IEEE, 2012.

[90] Christoph Sommer, Ozan K Tonguz, and Falko Dressler. Traffic information systems: efficient message dissemination via adaptive beaconing. *Communications Magazine, IEEE*, 49(5):173–179, 2011.

[91] Subir Biswas, Raymond Tatchikou, and Francois Dion. Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. *Communications Magazine, IEEE*, 44(1):74–82, 2006.

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

[93] VSCC. Vehicle safety communications project task 3 final report: Identify intelligent vehicle safety applications enabled by dsrc. Technical report, National Highway Traffic Safety Administration, 2005.

[94] Meng Guo, Mostafa H Ammar, and Ellen W Zegura. V3: A vehicle-to-vehicle live video streaming architecture. *Pervasive and Mobile Computing*, 1(4):404–424, 2005.

[95] Stephan Eichler, Christoph Schroth, and Jörg Eberspächer. Car-to-car communication. In *VDE-Kongress 2006*. VDE VERLAG GmbH, 2006.

[96] Johan Pouwelse, Paweł Garbacki, Dick Epema, and Henk Sips. The bittorrent p2p file-sharing system: Measurements and analysis. *Peer-to-Peer Systems IV*, pages 205–216, 2005.

[97] Shirshanka Das, Alok Nandan, and Giovanni Pau. Spawn: a swarming protocol for vehicular ad-hoc wireless networks. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, VANET '04, pages 93–94, New York, NY, USA, 2004. ACM.

[98] K Lee and I Yap. Cartorrent: A bit-torrent system for vehicular ad-hoc networks. *Los Angeles*.

[99] Uichin Lee, Joon-Sang Park, Joseph Yeh, Giovanni Pau, and Mario Gerla. Code torrent: content distribution using network coding in VANET. In *Proceedings of the 1st international workshop on Decentralized resource sharing in mobile computing and networking*, pages 1–5. ACM, 2006.

[100] Murat Caliskan, Daniel Graupner, and Martin Mauve. Decentralized discovery of free parking places. In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 30–39. ACM, 2006.

[101] Ramu Panayappan, Jayini Mukul Trivedi, Ahren Studer, and Adrian Perrig. VANET-based approach for parking space availability. In *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, pages 75–76. ACM, 2007.

[102] Piotr Szczurek, Bo Xu, Ouri Wolfson, Jie Lin, and Naphtali Rishe. Learning the relevance of parking information in VANETs. In *Proceedings of the seventh ACM international workshop on VehiculAr InterNETworking*, pages 81–82. ACM, 2010.

[103] Guey-Yun Chang, Jang-Ping Sheu, and Cheng-Yu Chung. Zooming: A zoom-based approach for parking space availability in VANET. In *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st*, pages 1–5. IEEE, 2010.

[104] Rongxing Lu, Xiaodong Lin, Haojin Zhu, and Xuemin Shen. Spark: a new VANET-based smart parking scheme for large parking lots. In *INFOCOM 2009, IEEE*, pages 1413–1421. IEEE, 2009.

[105] Ramon Bauza Javier Gozalvez, Miguel Sepulcre. Impact of the radio channel modelling on the performance of VANET communication protocols. In *Telecommunication Systems*, pages 149–167. Springer US, 2012.

[106] H. Boeglen, B. Hilt, P. Lorenz, J. Ledy, A.-M. Poussard, and R. Vauzelle. A survey of v2v channel modeling for VANET simulations. In *Wireless On-Demand Network Systems and Services (WONS), 2011 Eighth International Conference on*, pages 117 –123, jan. 2011.

[107] Robert Nagel and Stephan Eichler. Efficient and realistic mobility and channel modeling for VANET scenarios using omnet++ and inet-framework. In *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, Simutools '08, pages 89:1–89:8, ICST, Brussels, Belgium, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[108] Anne-Marie Poussard Benoît Hilt Rodolphe Vauzelle Jonathan Ledy, Hervé Boeglen. A semi deterministic channel model for VANETs simulations. In *International Journal of Vehicular Technology*, pages 89:1–89:8, 2012.

[109] Min-Woo Ryu, Si-Ho Cha, and Kuk-Hyun Cho. Dsrc-based channel allocation algorithm for emergency message dissemination in VANETs. In *Proceedings of the 5th international conference on Convergence and hybrid information technology*, ICHIT'11, pages 105–112, Berlin, Heidelberg, 2011. Springer-Verlag.

[110] Zaydoun Yahya Rawashdeh. *Efficient channel allocation and medium access organization algorithms for vehicular networking.* Phd, Wayne State University, 2011.

[111] Ranjeet Singh Tomar and Shekhar Verma. Rsu assisted channel allocation in VANETs. In *International Journal of Contemporary Research in Engg. and Tech*, volume 1, pages 25–36, 2011.

[112] M.J. Booysen, S. Zeadally, and G.-J. van Rooyen. Survey of media access control protocols for vehicular ad hoc networks. *Communications, IET*, 5(11):1619 –1631, 22 2011.

[113] Supeng Leng, Huirong Fu, Qing Wang, and Yan Zhang. Medium access control in vehicular ad hoc networks. *Wirel. Commun. Mob. Comput.*, 11(7):796–812, July 2011.

[114] K.A. Hafeez, Lian Zhao, Zaiyi Liao, and B.N.-W. Ma. A novel medium access control (mac) protocol for VANETs. In *Communications and Networking in China (CHINACOM), 2011 6th International ICST Conference on*, pages 685 –690, August 2011.

[115] Zaydoun Yahya Rawashdeh. Efficient medium access control protocol for vehicular ad-hoc networks. Master's thesis, Faculty of Computing, Health and Science, 2011.

[116] S.A. Arzil, M.H. Aghdam, and M.A.J. Jamali. Adaptive routing protocol for VANETs in city environments using real-time traffic information. In *Information*

Networking and Automation (ICINA), 2010 International Conference on, volume 2, pages V2–132 –V2–136, oct. 2010.

[117] Abu Naser Bikas Bijan Paul, Ibrahim. VANET routing protocols: Pros and cons. 20(3):28–34, 2011.

[118] SING-LING LEE YUN-WEI LIN, YUH-SHYAN CHEN. Routing protocols in vehicular ad hoc networks: A survey and future perspectives. 26:913–932, 2010.

[119] A survey on routing mechanism and techniques in vehicle to vehicle communication (VANET). 2:135–143, 2011.

[120] Chen Chao. A routing algorithm for VANET based on geographic location. In *Electronics, Communications and Control (ICECC), 2011 International Conference on*, pages 2483 –2487, September 2011.

[121] Razvan Stanica, Emmanuel Chaput, and André-Luc Beylot. Loss reasons in safety VANETs and implications on congestion control. In *Proceedings of the 9th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, PE-WASUN '12, pages 1–8, New York, NY, USA, 2012. ACM.

[122] Razvan Stanica. *Congestion Control in Vehicular Ad Hoc Networks*. Phd, Institut National Polytechnique de Toulouse, 2011.

[123] Mohamed Salah Bouassida and M. Shawky. A cooperative congestion control approach within VANETs: formal verification and performance evaluation. *EURASIP J. Wirel. Commun. Netw.*, 2010:11:1–11:12, April 2010.

[124] S. Konur and M. Fisher. Formal analysis of a VANET congestion control protocol through probabilistic verification. In *Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd*, pages 1 –5, may 2011.

[125] Maria Fazio, Claudio E Palazzi, Shirshanka Das, and Mario Gerla. Automatic ip address configuration in s. In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 100–101. ACM, 2006.

[126] Todd Arnold, Wyatt Lloyd, Jing Zhao, and Guohong Cao. Ip address passing for VANETs. In *Pervasive Computing and Communications, 2008. PerCom 2008. Sixth Annual IEEE International Conference on*, pages 70–79. IEEE, 2008.

[127] Zhenyu Yang, Ming Li, and Wenjing Lou. Codeplay: Live multimedia streaming in VANETs using symbol-level network coding. In *Proceedings of the The 18th*

IEEE International Conference on Network Protocols, ICNP '10, pages 223–232, Washington, DC, USA, 2010. IEEE Computer Society.

[128] Yi-Ling Hsieh and Kuochen Wang. Dynamic overlay multicast for live multimedia streaming in urban VANETs. *Computer Networks*, 56(16):3609 – 3628, 2012.

[129] Fabio Soldo, Claudio Casetti, Carla-Fabiana Chiasserini, and Pedro Alonso Chaparro. Video streaming distribution in VANETs. *IEEE Trans. Parallel Distrib. Syst.*, 22(7):1085–1091, July 2011.

[130] N. Qadri, M. Fleury, M. Altaf, B. R. Rofoee, and M. Ghanbari. Resilient p2p multimedia exchange in a VANET. In *Proceedings of the 2nd IFIP conference on Wireless days*, WD'09, pages 18–23, Piscataway, NJ, USA, 2009. IEEE Press.

[131] Kayhan Zrar Ghafoor and Kamalrulnizam Abu Bakar. Inter-vehicle communication protocols for multimedia transmission. In *International Multiconference of Engeeners and Computer Scientists*, volume 2, pages 1–5, 2010.

[132] N. Qadri, M. Altaf, M. Fleury, M. Ghanbari, and Hanadi Sammak. Robust video streaming over an urban VANET. In *Proceedings of the 2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, WIMOB '09, pages 429–434, Washington, DC, USA, 2009. IEEE Computer Society.

[133] F. Martelli, M. Elena Renda, P. Santi, and M. Volpetti. Measuring voip performance in ieee 802.11p vehicular networks. In *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th*, pages 1–5, 2012.

[134] Fu-Hsing Sung Min-Xiou Chen and Bing-Yang Lin. Service discovery protocol for network mobility environment. *International Journal of Innovative Computing, Information and Control*, 8(8):5573–5590, 2012.

[135] Suk-Bok Lee, Gabriel Pan, Joon-Sang Park, Mario Gerla, and Songwu Lu. Secure incentives for commercial ad dissemination in vehicular networks. In *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*, MobiHoc '07, pages 150–159, New York, NY, USA, 2007. ACM.

[136] Ciprian Dobre and George Cristian Tudor. Mobile advertisement in vehicular ad-hoc networks. *arXiv preprint arXiv:1202.2573*, 2012.

[137] Tamer Nadeem, Pravin Shankar, and Liviu Iftode. A comparative study of data dissemination models for VANETs. In *Mobile and Ubiquitous Systems-Workshops, 2006. 3rd Annual International Conference on*, pages 1–10. IEEE, 2006.

[138] Rasheed Hussain, Junggab Son, Hasoo Eun, Sangjin Kim, and Heekuck Oh. Rethinking vehicular communications: Merging VANET with cloud computing. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, pages 606–609. IEEE, 2012.

[139] R.M. Scopigno. Physical phenomena affecting VANETs: Open issues in network simulations. In *Transparent Optical Networks (ICTON), 2012 14th International Conference on*, pages 1 –4, july 2012.

[140] Francisco J. Martinez, Chai Keong Toh, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni. A survey and comparative study of simulators for vehicular ad hoc networks (VANETs). *Wirel. Commun. Mob. Comput.*, 11(7):813–828, July 2011.

[141] Pedro Gomes, Cristina Olaverri-Monreal, Michel Ferreira, and Luís Damas. Driver-centric VANET simulation. In *Proceedings of the Third international conference on Communication technologies for vehicles*, Nets4Cars/Nets4Trains'11, pages 143–154, Berlin, Heidelberg, 2011. Springer-Verlag.

[142] J. Härri, F. Filali, C. Bonnet, and Marco Fiore. Vanetmobisim: generating realistic mobility patterns for VANETs. In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, VANET '06, pages 96–97, New York, NY, USA, 2006. ACM.

[143] M. Fiore, J. Harri, F. Filali, and C. Bonnet. Vehicular mobility simulation for VANETs. In *Simulation Symposium, 2007. ANSS '07. 40th Annual*, pages 301 –309, march 2007.

[144] C. Sommer, I. Dietrich, and F. Dressler. Realistic simulation of network protocols in VANET scenarios. In *2007 Mobile Networking for Vehicular Environments*, pages 139 –143, may 2007.

[145] Jérôme Härri, Marco Fiore, Fethi Filali, and Christian Bonnet. Vehicular mobility simulation with vanetmobisim. *Simulation*, 87(4):275–300, April 2011.

[146] Ahmad Yusri Dak, Saadiah Yahya, and Murizah Kassim. A literature survey on security challenges in VANETs. In *The International Conference of Information Security*, 2011.

[147] Antonios Stampoulis and Zheng Chai. Survey of security in vehicular networks. *Project CPSC*, 534, 2007.

[148] Bryan Parno and Adrian Perrig. Challenges in securing vehicular networks. In *Workshop on Hot Topics in Networks (HotNets-IV)*, pages 1–6, 2005.

[149] Albert Wasef, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]. *Wireless Communications, IEEE*, 17(5):22–28, 2010.

[150] Valentina Casola, Jesus Luna, Antonino Mazzeo, Manel Medina, Massimiliano Rak, and Jetzabel Serna. An interoperability system for authentication and authorisation in VANETs. *International Journal of Autonomous and Adaptive Communications Systems*, 3(2):115–135, 2010.

[151] Albert Wasef, Yixin Jiang, and Xuemin Shen. Ecmv: efficient certificate management scheme for vehicular networks. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5. IEEE, 2008.

[152] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han Ho, and Xuemin Shen. Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 1229–1237. IEEE, 2008.

[153] José María de Fuentes, Ana Isabel González-Tablas, and Arturo Ribagorda. Overview of security issues in vehicular ad-hoc networks. 2010.

[154] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly. Impact of denial of service attacks on ad hoc networks. *IEEE/ACM Transations of Networks*, 16(4):791–802, August 2008.

[155] K. Pelechrinis, M. Iliofotou, and S.V. Krishnamurthy. Denial of service attacks in wireless networks: The case of jammers. *Communications Surveys Tutorials, IEEE*, 13(2):245 –257, quarter 2011.

[156] Anu Bala, Munish Bansal, and Jagpreet Singh. Performance analysis of manet under blackhole attack. In *Proceedings of the 2009 First International Conference on Networks & Communications*, NETCOM '09, pages 141–145, Washington, DC, USA, 2009. IEEE Computer Society.

[157] Kumar Balwant Singh Vimal Bibhu, Kumar Roshan and Dhirendra Kumar Singh. Performance analysis of black hole attack in VANET. In *Computer Network and Information Security*, volume 11, pages 47–54. MECS, 2012.

[158] Ghassan Samara, Wafaa AH Al-Salihy, and R Sures. Security issues and challenges of vehicular ad hoc networks (VANET). In *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on*, pages 393–398. IEEE, 2010.

[159] Marshall Riley, Kemal Akkaya, and Kenny Fong. A survey of authentication schemes for vehicular ad hoc networks. *Security and Communication Networks*, 4(10):1137–1152, 2011.

[160] Paul Syverson. A taxonomy of replay attacks [cryptographic protocols]. In *Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings*, pages 187–191. IEEE, 1994.

[161] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful gps spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 75–86. ACM, 2011.

[162] Mohammad Fanaei, Ali Fanian, and Mehdi Berenjkoub. Prevention of tunneling attack in endaira. pages 994–999, 2009.

[163] Emanuel Fonseca, Andreas Festag, Roberto Baldessari, and Rui L Aguiar. Support of anonymity in VANETs-putting pseudonymity into practice. In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pages 3400–3405. IEEE, 2007.

[164] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura, and Kaoru Sezaki. Caravan: Providing location privacy for VANET. In *in Embedded Security in Cars (ESCAR)*, 2005.

[165] D. Chaum. The dining cryptographers problem: unconditional sender and recipient untraceability. *J. Cryptol.*, 1(1):65–75, March 1988.

[166] Alastair R Beresford and Frank Stajano. Location privacy in pervasive computing. *Pervasive Computing, IEEE*, 2(1):46–55, 2003.

[167] Rongxing Lu, Xiaodong Li, Tom H Luan, Xiaohui Liang, and Xuemin Shen. Pseudonym changing at social spots: An effective strategy for location privacy in VANETs. *IEEE Transactions on Vehicular Technology*, 61(1):86–96, 2012.

[168] Julien Freudiger, Maxim Raya, Márk Félegyházi, Panos Papadimitratos, et al. Mix-zones for location privacy in vehicular networks. In *Proceedings of the first international workshop on wireless networking for intelligent transportation systems (Win-ITS)*, 2007.

[169] Levente Buttyán, Tamás Holczer, and István Vajda. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In *Security and Privacy in Ad-hoc and Sensor Networks*, pages 129–141. Springer, 2007.

[170] Levente Buttyán, Tamás Holczer, André Weimerskirch, and William Whyte. Slow: A practical pseudonym changing scheme for location privacy in VANETs. In *Vehicular Networking Conference (VNC), 2009 IEEE*, pages 1–8. IEEE, 2009.

[171] Sushmita Ruj, Marcos Antonio Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic. On data-centric misbehavior detection in VANETs. In *Vehicular Technology Conference (VTC Fall), 2011 IEEE*, pages 1–5. IEEE, 2011.

[172] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and correcting malicious data in VANETs. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 29–37. ACM, 2004.

[173] Tim Leinmüller, Elmar Schoch, Frank Kargl, and Christian Maihöfer. Influence of falsified position data on geographic ad-hoc routing. In *Security and Privacy in Ad-hoc and Sensor Networks*, pages 102–112. Springer, 2005.

[174] Al-Sakib Khan Pathan. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. Taylor & Francis, 2010.

[175] L. Page, S. Brin, R. Motwani, and T. Winograd. The pagerank citation ranking: Bringing order to the web. In *Proceedings of the 7th International World Wide Web Conference*, pages 161–172, Brisbane, Australia, 1998.

[176] Alice Cheng and Eric Friedman. Manipulability of pagerank under sybil strategies, 2006.

[177] Nazareno Ferreira de Andrade. Reputação autônoma como incentivo à colaboração no compartilhamento de recursos computacionais. Master's thesis, Pós-Graduação em Informática, Universidade Federal de Campina Grande, 2004.

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

[179] Florian Dotzer, Lars Fischer, and Przemyslaw Magiera. Vars: A vehicle ad-hoc network reputation system. In *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*, pages 454–456. IEEE, 2005.

[180] D. I. Robertson. Transyt - a traffic network study tool. *Report No TRRL-LR-253 (Transport and Road Research Laboratory, Crowthorne)*, 1969.

[181] GM Pacey. The progress of a bunch of vehicles released from a traffic signal. *Road Research Laboratory Note RN/2665/GMP*, 1956.

[182] Lo Nai-Wei and Tsai Hsiao-Chien. A reputation system for traffic safety event on vehicular ad hoc networks. *EURASIP Journal on Wireless Communications and Networking*, 2009, 2009.

[183] Klaus Plößl and Hannes Federrath. A privacy aware and efficient security infrastructure for vehicular ad hoc networks. *Computer Standards & Interfaces*, 30(6):390–397, 2008.

[184] Brijesh Kumar Chaurasia and Shekhar Verma. Infrastructure based authentication in VANETs. *International Journal of Multimedia and Ubiquitous Engineering*, 6(2):41–54, 2011.

[185] Youngho Park, Chul Sur, Chae Duk Jung, and Kyung Hyune Rhee. An efficient anonymous authentication protocol for secure vehicular communications. *J. Inf. Sci. Eng.*, 26(3):785–800, 2010.

[186] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. The security and privacy of smart vehicles. *Security & Privacy, IEEE*, 2(3):49–55, 2004.

[187] Tim Leinmuller, Elmar Schoch, and Christian Maihofer. Security requirements and solution concepts in vehicular ad hoc networks. In *Wireless on Demand Network Systems and Services, 2007. WONS'07. Fourth Annual Conference on*, pages 84–91. IEEE, 2007.

[188] Gilles Guette and Ciarán Bryce. Using tpms to secure vehicular ad-hoc networks (VANETs). In *Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks*, pages 106–116. Springer, 2008.

[189] Dan Boneh and Hovav Shacham. Group signatures with verifier-local revocation. In *Proceedings of the 11th ACM conference on Computer and communications security*, pages 168–177. ACM, 2004.

[190] J.F. Kurose and K.W. Ross. *Computer Networking: A Top-down Approach*. Always learning. Pearson, 2013.

[191] Gregor V Bochmann and Carl A Sunshine. Formal methods in communication protocol design. *IEEE Transactions on Communications*, 28(4):624–631, 1980.

[192] W.H.H.J.J.A. Buck. *Eletromagnetismo*. McGraw Hill Brasil, 4 edition.

[193] Michael Burrows, Martin Abadi, and Roger M Needham. A logic of authentication. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 426(1871):233–271, 1989.

[194] DU Jin-hui HU Ming-zeng and Zhao-xin ZHANG. Security analysis of needham-schroeder symmetric key authentication protocol. *Microcomputer information*, 12:025, 2008.

[195] Klaus Gaarder and Einar Snekkenes. Applying a formal analysis technique to the ccitt x. 509 strong two-way authentication protocol. *Journal of cryptology*, 3(2):81–98, 1991.

[196] Giampaolo Bella and Lawrence C Paulson. Kerberos version iv: Inductive analysis of the secrecy goals. pages 361–375, 1998.

[197] Claudia Dıaz, Joris Claessens, Stefaan Seys, and Bart Preneel. Information theory and anonymity. In *Proceedings of the 23rd Symposium on Information Theory in the Benelux*, pages 179–186, 2002.

[198] Benoît Libert, Thomas Peters, and Moti Yung. Group signatures with almost-for-free revocation. In *Advances in Cryptology–CRYPTO 2012*, pages 571–589. Springer, 2012.

[199] Sung-Hwa Lim, Se Won Lee, Mye Sohn, and Byoung-Hoon Lee. Energy-aware optimal cache consistency level for mobile devices". *Information Sciences*, 230:94 – 105, 2013.

[200] Christoph Sommer, Reinhard German, and Falko Dressler. Bidirectionally coupled network and road traffic simulation for improved ivc analysis. *IEEE Transactions on Mobile Computing*, 10(1):3–15, 2011.

[201] Michael Behrisch, Laura Bieker, Jakob Erdmann, and Daniel Krajzewicz. Sumo-simulation of urban mobility-an overview. In *SIMUL 2011, The Third International Conference on Advances in System Simulation*, pages 55–60, 2011.

[202] Robert Karl Schmidt, Thomas Köllmer, Tim Leinmüller, Bert Böddeker, and Günter Schäfer. Degradation of transmission range in VANETs caused by interference. *PIK-Praxis der Informationsverarbeitung und Kommunikation*, 32(4):224–234, 2009.

[203] James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, Angela Hung Byers, and McKinsey Global Institute. Big data: The next frontier for innovation, competition, and productivity. 2011.

[204] Arvind Narayanan and Vitaly Shmatikov. How to break anonymity of the netflix prize dataset. *arXiv preprint cs/0610105*, 2006.

[205] Arvind Narayanan and Vitaly Shmatikov. Robust de-anonymization of large sparse datasets. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 111–125. IEEE, 2008.