Universidade Federal de Pernambuco

Centro de Informática

Pós-graduação em Ciência da Computação

UM MECANISMO HÍBRIDO PARA MITIGAÇÃO DE RASTREAMENTOS EM VANETS

Eduardo Ferreira de Souza

DISSERTAÇÃO DE MESTRADO

Recife

21 de junho de 2013

Universidade Federal de Pernambuco

Centro de Informática

Eduardo Ferreira de Souza

UM MECANISMO HÍBRIDO PARA MITIGAÇÃO DE RASTREAMENTOS EM VANETS

Trabalho apresentado ao Programa de Pós-graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Ciência da Computação.

Orientador: *Paulo André da Silva Gonçalves*

Recife

21 de junho de 2013

Este trabalho é dedicado à minha família e todas as pessoas que me apoiaram nessa jornada.

AGRADECIMENTOS

Agradeço a Deus por me guiar nos momentos decisivos da vida. Sou grato pela oportunidade que me foi concedida de desenvolver este trabalho. A Ele seja dada toda a glória e todo o louvor.

Aos meus pais, Mário e Celma, por toda dedicação que sempre tiveram comigo, me apoiando e aconselhando nas situações de dificuldade. Sou eternamente grato por todo apoio que sempre me deram, não me deixando desanimar e me ajudando a enxergar os melhores caminhos a trilhar.

À minha irmã Mariana e minhas sobrinhas Marina e Manuela, que me fazem viver em constante sentimento de saudades. Agradeço por serem fontes de felicidade para minha vida.

À minha noiva e futura esposa, Karol, por ser minha companheira, minha amiga, meu orgulho... Obrigado por estar comigo em todos os momentos, por me trazer motivação nas horas de desânimo e por se alegrar comigo nas horas de alegria. Obrigado por estar sempre perto, mesmo quando estamos longe.

Ao professor Paulo Gonçalves, por ter me acolhido no grupo de pesquisa e por ser um grande conselheiro nos momentos decisivos de minha vida acadêmica até então. Agradeço por se mostrar sempre pronto para me apoiar e me ajudar a obter os melhores resultados.

Por fim, aos meus colegas do grupo de pesquisa, pela troca de experiências e pelos conselhos que me foram dados. Sou grato por tudo que aprendi nesse grupo, por cada reunião e por cada crítica.

No pain, No gain

—BENJAMIN FRANKLIN

RESUMO

Cada veículo nas VANETs transmite periodicamente mensagens com informações de sua localização geográfica atual. Contudo, tais mensagens permitem que atacantes rastreiem indevidamente os veículos. Os principais mecanismos propostos para mitigar esse problema, denominados Stübing e SafeAnon, se baseiam no uso de grupos criptográficos e de ofuscações, respectivamente. A primeira abordagem permite a proteção dos veículos apenas enquanto eles pertencem a algum grupo. Contudo, os veículos fora dos grupos podem ser facilmente rastreados. A segunda abordagem utiliza uma técnica de ofuscação para evitar que um atacante conheça as localizações exatas dos veículos. Em tal mecanismo, contudo, os veículos próximos entre si precisam trocar mensagens em claro contendo suas localizações exatas para detectar situações de risco de colisão. Essa troca de mensagens em claro é um facilitador para que um atacante rastreie os veículos comunicantes. Este trabalho propõe um mecanismo híbrido, denominado HybSec, que mitiga os problemas de rastreamento em VANETs. O mecanismo proposto é baseado simultaneamente em grupos criptográficos e ofuscação de localizações. As avaliações de desempenho realizadas demonstram que o tempo de rastreamento sofrido pelos veículos na solução proposta é significativamente inferior ao tempo obtido com os demais mecanismos analisados.

Palavras-chave: Redes veiculares, rastreamento, privacidade, ofuscação, grupos criptográficos

ABSTRACT

Each vehicle in VANETs periodically broadcasts messages with its current location. However, these messages allow attackers to improperly track any vehicle. The main mechanisms proposed to mitigate this problem, named Stübing and SafeAnon, are based on cryptographic groups and obfuscations, respectively. The first approach protects vehicles while they are in a group. However, vehicles that are not in any group can be easily tracked. The second approach uses an obfuscation scheme to prevent an attacker to know the precise locations of vehicles. In such scheme, however, vehicles close together need to broadcast messages containing their exact locations in order to detect situations of collision risk. This plaintext broadcast is a vulnerability that allows an attacker to track vehicles. In this work, we propose a hybrid mechanism called HybSec, that mitigates tracking problems in VANETs. The proposed mechanism is based both on cryptographic groups and location obfuscation. Performance evaluations show that the tracking time in the proposed mechanism is significantly shorter than that obtained by studied related work.

Keywords: Vehicular networks, tracking, privacy, obfuscation, cryptographic groups

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

AC Autoridade Certificadora. 6, 7, 21, 28

AES *Advanced Encryption Standard*. 28

CAM *Cooperative Awareness Messages*. 2, 17, 20–25, 31, 42, 45, 49, 61, 62

DSRC *Dedicated Short Range Communication*. 2

IEEE *Institute of Electrical and Electronics Engineers*. 9, 47

IEEE 1609.2 Padrão para a troca de mensagens seguras entre veículos. 9

ITS *Intelligent Transportation System*. 1

NIST *National Institute of Standards and Technology*. 28

OBU *On-Board Unit*. 6, 7, 14, 21

RSP *Random Silent Period*. 15, 16

RSU *Roadside Unit*. 1, 3, 4, 6, 7, 13–15, 20, 25, 28

SHA *Secure Hash Algorithm*. 27, 28

VANET *Vehicular Ad-Hoc Network* ou Rede Veicular Ad-Hoc. 1–3, 6–11, 16, 17, 28, 48, 64

ZM Zona Mista. 12, 13

CAPÍTULO 1

INTRODUÇÃO

As redes veiculares ad-hoc (VANETs) proveem um ambiente colaborativo de troca de informações entre os veículos. Desse modo, as VANETs tornam-se significantemente importantes para a criação de um sistema de transporte inteligente (*Intelligent Transportation System* - ITS). Através delas, é possível auxiliar os motoristas a tomarem decisões no trânsito ou, até mesmo, fornecer subsídios para a movimentação autônoma dos veículos. Os veículos atuam como os principais atores nas VANETs, porém não são os únicos. Essas redes também podem ser integradas pelas entidades da infraestrutura, estabelecimentos comerciais, equipamentos de sinalização, pedestres munidos de dispositivos portáteis, dentre outros. Portanto, as possibilidades de crescimento dessas redes são grandes e os benefícios de sua implantação em larga escala estendem-se não só aos motoristas, mas também às autoridades de trânsito, autoridades policiais, pedestres e empresas de seguros, por exemplo. Juntamente com os potenciais benefícios dessas redes, também estão os desafios a serem superados para sua adoção em larga escala. Assim como nas redes móveis tradicionais, a segurança na comunicação das entidades é um desafio. Contudo, a preocupação com desenvolvimento de mecanismos de segurança nas VANETs é ainda maior, dado que falhas de segurança nessas redes podem comprometer a integridade física de seus usuários. A possibilidade de alertas falsos ou rastreamentos indevidos dos veículos, por exemplo, podem colocar os motoristas em situações de risco.

1.1 MOTIVAÇÃO

Em geral, as VANETs são compostas pelos veículos e pelas RSUs (*Roadside Units*), que são entidades da infraestrutura da rede localizadas às margens das rodovias. As

VANETs se baseiam na tecnologia DSRC (*Dedicated Short Range Communication*) para comunicação entre veículos (*vehicle to vehicle* ou V2V) e dos veículos com a infraestrutura da rede (*vehicle to infrastructure* ou V2I) [Yin et al. 2004].

Um dos grandes impulsionadores para a implantação das VANETs são as aplicações de segurança no trânsito, isto é, aplicações que informam aos motoristas sobre riscos de colisão [Hartenstein and Laberteaux 2008]. As principais aplicações voltadas para segurança no trânsito utilizam mensagens conhecidas como *CAMs* (*Cooperative Awareness Messages*), as quais são enviadas periodicamente por cada veículo. Essas mensagens contêm informações de localização do emissor da mensagem, isto é, as coordenadas da localização geográfica do emissor ou de uma região onde o emissor está contido. Através de tais mensagens, os veículos são capazes de monitorar a situação do trânsito, permitindo que sejam evitados acidentes.

Apesar dos benefícios obtidos através da troca de informações de localização, essa comunicação impacta na privacidade dos usuários. Através da captura de sucessivas *CAMs*, é possível que uma entidade maliciosa rastreie indevidamente os veículos. Naturalmente, a possibilidade de rastreamentos abre uma vasta possibilidade de atividades ilegais a serem realizadas. Essa informação pode, por exemplo, indicar que um veículo se locomoveu de um banco até sua residência.

O principal desafio no contexto de privacidade em VANETs é evitar os rastreamentos, porém permitindo que sejam trocadas informações de localizações para viabilizar as aplicações [Zhang and Delgrossi 2012]. Apesar de haver diversas pesquisas focadas em mitigar os problemas de rastreamentos, ainda são grandes as deficiências em tais abordagens com relação ao tempo que os veículos permanecem protegidos, como demonstrado em [Pan and Li 2012].

Os pseudônimos são adotados nas VANETs para evitar que cada veículo envie sua identificação real ao trocar mensagens na rede. Um pseudônimo é um identificador de uma entidade, mas que difere do seu identificador real. Além disso, os pseudônimos não são utilizados por longos períodos de tempo. Contudo, eles apenas oferecem uma segurança inicial à privacidade dos usuários. Mesmo substituindo frequentemente seus pseudônimos,

os veículos ainda são vulneráveis a rastreamentos [Wiedersheim et al. 2010, Pan and Li 2012].

Alguns trabalhos propõem que os veículos formem grupos criptográficos para a substituição de pseudônimos de forma coletiva para mitigar os rastreamentos [Freudiger et al. 2007, Stübing et al. 2011, Wasef and Shen 2010]. Um grupo criptográfico é formado por um conjunto de veículos, podendo contar com a presença de elementos da infraestrutura (RSUs), e é utilizado para que sejam trocadas informações sigilosas de forma criptografada. A principal dessas informações é a localização de cada veículo, de modo que um atacante não é capaz de obtê-la enquanto os veículos permanecem no grupo. Contudo, os mecanismos baseados puramente em grupos protegem as localizações apenas enquanto os veículos pertencem a algum grupo.

Também com foco em mitigar rastreamentos em VANETs, em [Chen and Wei 2012] é proposto um mecanismo baseado em técnicas de ofuscação. A ofuscação é a adulteração deliberada da precisão das localizações enviadas para que os receptores não identifiquem exatamente a localização do emissor da mensagem. Em VANETs, no entanto, cada veículo precisa conhecer a localização exata dos veículos em sua proximidade para que possam ser evitadas colisões entre eles. Para adequar-se a tal necessidade, em [Chen and Wei 2012] é proposto que os veículos próximos entre si informem suas localizações exatas em claro na rede. Contudo, os veículos tornam-se suscetíveis a rastreamentos nesses contextos.

Como citado, isoladamente as técnicas de grupos criptográficos e ofuscação de localizações utilizadas nos trabalhos relacionados apresentam vulnerabilidades de rastreamentos. Apesar de cada abordagem possuir aspectos positivos, em ambas há contextos em que as localizações exatas dos veículos não são protegidas.

1.2 OBJETIVOS

O objetivo geral deste trabalho é explorar os pontos positivos das abordagens de ofuscação e grupos criptográficos, criando uma solução híbrida que minimize o tempo de rastrea-

mento dos veículos em relação aos trabalhos relacionados. Ao utilizar os benefícios de cada abordagem, a solução proposta, denominada HybSec (*Hybrid Security*), evita que atacantes obtenham as localizações exatas dos veículos em qualquer contexto.

Além de mitigar o tempo de rastreamento, o mecanismo proposto deve se adequar aos requerimentos das aplicações de segurança e monitoramento no trânsito. Portanto, a solução deve permitir a troca informações de localizações exatas entre veículos próximos, garantindo que os motoristas possam ser alertados sobre situações de risco de colisão. Além disso, deve permitir que qualquer veículo receba mensagens que o permita estimar as localizações dos veículos em seu raio de alcance.

A proposta também deve contemplar a característica de ser autogerenciável pelos veículos. Isto é, sem a necessidade de intervenção da infraestrutura da rede para que a solução funcione adequadamente. Dessa forma, aumenta-se a viabilidade de implantação, visto que não é necessária a presença de RSUs para que o mecanismo possa atuar.

Para alcançar o objetivo geral, os seguintes objetivos específicos são definidos:

- Analisar os desafios e necessidades das aplicações das redes veiculares;
- Analisar os trabalhos propostos na literatura para mitigar os problemas de rastreamento;
- Verificar os aspectos positivos e negativos dos trabalhos relacionados, bem como os seus respectivos desempenhos;
- Avaliar o desempenho do mecanismo proposto, comparando-o com as principais soluções propostas na literatura.

1.3 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado da seguinte forma: o Capítulo 2 mostra os conceitos básicos relativos às redes veiculares, necessários para um melhor entendimento da solução proposta. O Capítulo 3 apresenta os trabalhos relacionados, bem como suas principais limitações. Em seguida, o Capítulo 4 descreve o mecanismo proposto, apresentando

como as abordagens de ofuscação e grupos criptográficos são utilizadas conjuntamente para mitigar os problemas de rastreamentos. No Capítulo 5 é apresentado o resultado da avaliação de desempenho do mecanismo proposto em comparação com os trabalhos relacionados. Por fim, o Capítulo 6 apresenta as conclusões e considerações finais.

CAPÍTULO 2

CONCEITOS BÁSICOS

Este capítulo descreve os conceitos básicos relativos às redes veiculares. São apresentadas as entidades participantes da rede e suas responsabilidades. Também é mostrada a forma como os pseudônimos são utilizados pelos veículos. Além disso, são apresentadas as principais aplicações das VANETs.

2.1 ENTIDADES

Existem diversas entidades que podem participar da comunicação em redes veiculares. Os veículos convencionais são as principais entidades, contudo, podem existir entidades móveis com permissões especiais, como veículos de alerta (ex: ambulâncias) ou pedestres. Além disso, podem participar da rede entidades imóveis como prestadores de serviços, estabelecimentos comerciais, placas indicativas e centrais de informações.

Para ser considerada autêntica, cada entidade deve estar munida ou de uma RSU (*Roadside Unit*) ou de uma OBU (*On-Board Unit*). Tais dispositivos, ilustrados na Figura 2.1 são gerenciados e homologados por uma ou mais ACs (Autoridade Certificadoras). Abaixo são apresentadas suas principais características.

Roadside Units (RSUs): Dispositivos integrantes da infraestrutura e localizados ao longo das rodovias. Podem ser, por exemplo, integrados às placas de trânsito ou semáforos. Comunicam-se com as OBUs e podem ser utilizados com provedores de serviços.

On-Board Units (OBUs): Dispositivos que operam em movimento e dão suporte a comunicação com outras OBUs e com as RSUs. Todos os veículos possuem OBUs

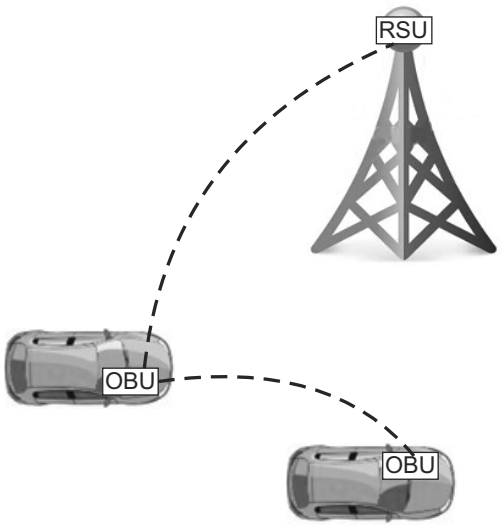

Figura 2.1 Comunicação entre dispositivos da rede.

embutidos, porém estes dispositivos não são restritos aos veículos, visto que OBUs podem ser utilizadas de forma portátil.

Autoridade Certificadora (AC): Entidades responsáveis pela emissão de chaves públicas e certificados digitais às entidades da rede. Através dessas informações, é possível que seja verificada a autenticidade dos emissores das mensagens enviadas na rede. Nas VANETs, a AC também possui a responsabilidade de autorizar e revogar a participação de dispositivos na rede. Através da infraestrutura da rede, a AC é capaz de se comunicar com as RSUs.

2.2 PSEUDÔNIMOS

O uso de pseudônimos foi introduzido em [Chaum 1981] e, desde então, vem sendo utilizado em comunicações onde é necessária a identificação das entidades. Tal solução é utilizada em tecnologias como RFID [Alomair et al. 2012], redes P2P [Peng et al. 2011] e, mais frequentemente, em VANETs [Hartenstein and Laberteaux 2008, Lu et al. 2012].

Um pseudônimo é um identificador de uma entidade, mas que difere do seu ID real. A ideia de utilizá-los é permitir que duas ou mais entidades se identifiquem durante

uma comunicação, porém que essa identificação não revele informações sigilosas sobre as entidades. Portanto, um pseudônimo não deve conter informações que permitam que entidades maliciosas obtenham o identificador real relativo a cada pseudônimo.

Existem diversos esforços para padronizar a comunicação em redes veiculares [IEEE P1609.1 Working Group 2006,IEEE P1609.2 Working Group 2006,IEEE P1609.3 Working Group 2010,IEEE P1609.4 Working Group 2010,IEEE 802.11p Task Group 2010], porém o único direcionamento para lidar com os problemas de rastreamento é dado através da indicação do uso de pseudônimos. Apesar de ainda não especificada a sua utilização, o uso dos pseudônimos é geralmente considerado nas soluções para lidar com os problemas de rastreamentos em VANETs. Contudo, algumas soluções baseiam sua segurança na eficiência dos pseudônimos em evitar rastreamentos.

Para que os pseudônimos possam ser eficazes, os veículos devem modificá-los frequentemente. Dessa forma, é possível evitar que o atacante correlacione todas as localizações obtidas de um mesmo emissor através de seu pseudônimo. Essa mudança de pseudônimos, porém, precisa ser realizada de forma que os emissores das mensagens possam ser identificados em caso auditorias. Assim sendo, é necessário que todos os pseudônimos sejam conhecidos e homologados na Autoridade Certificadora. Isto é, a AC deve conhecer o ID real de cada veículo da rede e a lista de todos os pseudônimos correspondentes a esse ID.

Na prática, cada pseudônimo é uma chave pública associada ao veículo que o possui. Portanto, o pseudônimo de um veículo não é utilizado apenas como seu identificador, mas também como uma chave que permite que outros veículos cifrem mensagens que só poderão ser decifradas pelo dono do pseudônimo. Para isso, cada chave pública (pseudônimo) está associada a uma chave privada correspondente. Essa chave privada, por sua vez, é conhecida unicamente pelo dono do pseudônimo.

2.2.1 Criptografia de Chaves Públicas

A criptografia de chave pública também é conhecida como criptografia assimétrica. Essa técnica criptográfica denomina-se assimétrica porque a chave utilizada para cifrar uma

mensagem é diferente da chave utilizada para decifrá-la [Menezes et al. 1996]. Assim sendo, cada entidade deve possuir um par de chaves distintas: uma chave pública e uma chave privada. A chave pública é distribuída livremente para todas as entidades, enquanto que a chave privada deve ser conhecida apenas pelo seu dono e, possivelmente, por uma entidade gerenciadora de chaves.

Uma mensagem cifrada com a chave pública apenas pode ser decifrada por sua chave privada correspondente. Portanto, ao enviar seu pseudônimo publicamente em cada mensagem, cada veículo permite que outras entidades enviem-lhe mensagens que apenas ele poderá decifrar.

De modo semelhante à cifra realizada com a chave pública, uma mensagem cifrada com a chave privada pode somente ser decifrada pela chave pública correspondente. A partir desse princípio, os veículos assinam digitalmente as mensagens. Nesse caso, um *hash* da mensagem é cifrado com a chave privada, e os receptores verificam a autenticidade do emissor através da decifragem do *hash* com a chave pública.

2.3 APLICAÇÕES

De modo geral, as redes veiculares foram concebidas com o objetivo de prover melhores condições de trânsito. Dentre as diversas aplicações propostas na literatura estão soluções de busca de estabelecimentos, propagação de alertas de veículos com sirene, compartilhamento de multimídia, troca de informações sobre vagas de estacionamentos, etc. Contudo, as principais aplicações para as VANETs são aquelas que impactam diretamente na segurança e integridade física dos usuários. Assim sendo, a família de padrões IEEE 1609 é motivada principalmente por prover serviços às aplicações de segurança no trânsito e monitoração colaborativa, como citado no padrão IEEE 1609.2 [IEEE P1609.2 Working Group 2006]. Este trabalho também foca-se em tais grupos de aplicações, visto que essas possuem maiores desafios em relação aos problemas de rastreamentos em VANETs.

As aplicações de segurança no trânsito são focadas em evitar colisões entre os veículos. Elas podem ser utilizadas para auxílio em ultrapassagens, alertas para redução de velo-

cidade, indicação de riscos em cruzamentos, etc. De modo geral, tais aplicações baseiam-se na detecção de um risco de colisão em potencial entre veículos. Por outro lado, as aplicações de monitoração colaborativa atuam de forma mais abrangente, permitindo que os motoristas obtenham uma visão geral sobre as condições do tráfego nas rodovias. Assim sendo, o objetivo possibilitar a obtenção de informações sobre congestionamentos, acidentes ou quaisquer anormalidades no tráfego.

Cada aplicação possui necessidades específicas para que possa funcionar adequadamente. Assim sendo, os protocolos de segurança devem se adequar às aplicações. De acordo com os requisitos para o funcionamento de cada aplicação, descrito em [Hartenstein and Laberteaux 2008], qualquer veículo da rede deve: (1) obter as localizações exatas dos veículos em sua proximidade (segurança no trânsito) e (2) estimar as localizações dos veículos em seu raio de alcance (monitoramento colaborativo).

RESUMO

Os dispositivos comunicantes utilizados nas VANETs são: OBUs, RSUs e AC. As OBUs são dispositivos contidos em cada veículo, utilizados para se comunicar com outras OBUs e com RSUs. As RSUs são os dispositivos integrantes da infraestrutura e localizados às margens das rodovias e, por fim, a AC é uma entidade com permissões para autorizar e revogar a participação de dispositivos na rede.

Cada veículo possui um conjunto de chaves públicas homologadas pela AC, conhecidas como pseudônimos. Tais pseudônimos são diretrizes dos padrões IEEE 1609 para que os veículos não enviem em claro o seu ID real. Além disso, através dessas chaves públicas, outras entidades são capazes de enviar mensagens cifradas que apenas o receptor será capaz de decifrar, visto que ele possui a chave privada correspondente ao seu pseudônimo.

As principais aplicações das VANETs são voltadas para segurança e monitoração no trânsito. Para o funcionamento adequado de tais aplicações, é necessário que cada veículo obtenha as localizações exatas dos veículos em sua proximidade e possa estimar as localizações dos veículos em seu raio de alcance.

CAPÍTULO 3

TRABALHOS RELACIONADOS

A preocupação com privacidade em VANETs existe desde o início das pesquisas sobre essas redes. Diversos mecanismos foram propostos até então para mitigar problemas de rastreamentos. No entanto, os mecanismos já propostos apresentam limitações em alguns contextos, seja para prover privacidade aos veículos ou para atender às necessidades das aplicações de segurança no trânsito e monitoração. Este capítulo apresenta os principais trabalhos propostos no estado da arte, descrevendo suas característica e limitações.

3.1 GRUPOS

O conceito de grupos criptográficos é frequentemente utilizado em VANETs para lidar com o problema de rastreamentos [Sampigethaya et al. 2007, Freudiger et al. 2007, Wasef and Shen 2010, Song et al. 2010, Stübing et al. 2011]. Um grupo criptográfico é definido como um conjunto limitado de veículos que se comunicam de forma cifrada e que estão geograficamente próximos entre si. Em geral, eles são utilizados para impedir que um atacante obtenha informações trocadas entre os veículos internos aos grupos.

Na literatura, os mecanismos baseados em grupos focam em criar um ambiente seguro para dificultar que um atacante correlacione os pseudônimos. Portanto, a ideia é dificultar que um atacante identifique um dado veículo antes de ingressar no grupo como sendo o mesmo veículo após sair do grupo. Para isso, os veículos ingressam em um grupo, modificam seus pseudônimos enquanto estão internos e, posteriormente, saem do grupo. Como o atacante não sabe quais são os novos pseudônimos assumidos pelos veículos enquanto pertenciam aos grupos, dificulta-se a correlação. Contudo, os grupos são formados apenas em momentos estratégicos em que o mecanismo em questão define como sendo

adequados para substituição dos pseudônimos.

Em [Wiedersheim et al. 2010] e [Pan and Li 2012] são demonstradas as vulnerabilidades inerentes aos mecanismos focados em impedir correlações entre pseudônimos. Nos trabalhos, é demonstrado que as características de mobilidade dos veículos (direção, sentido, velocidade, etc) tendem-se a se manter durante o trajeto. Portanto, ao substituir o pseudônimo, as características de mobilidade de um dado veículo permitem que um atacante possa inferir que apenas o pseudônimo está modificado. Através de simulações, em [Wiedersheim et al. 2010] é mostrada uma capacidade de rastreamento de veículos superior a 900 segundos, mesmo que os veículos substituam seus pseudônimos em curtos intervalos de 4 segundos.

Como citado, até então os mecanismos baseados em grupos focam em evitar correlações de pseudônimos. Porém, as deficiências do uso de pseudônimos, demonstradas em [Wiedersheim et al. 2010] e [Pan and Li 2012], indicam que eles não geram a entropia necessária para impedir que atacantes rastreiem os veículos com sucesso. Além disso, o principal problema de tais abordagens é o fato de os veículos sempre enviarem suas localizações em claro enquanto estão fora dos grupos, que é a maior parte do tempo. Existem diferentes abordagens baseadas no uso de grupos criptográficos na literatura, sendo as principais delas: zonas mistas [Freudiger et al. 2007] e grupos móveis [Stübing et al. 2011, Wasef and Shen 2010].

3.1.1 Zonas Mistas (ZM)

As zonas mistas (ZMs) são regiões bem definidas no mapa onde os veículos tornam-se indistinguíveis entre si para um atacante. Nelas, os veículos estabelecem uma comunicação cifrada e restrita apenas às entidades internas à ZM. Assim sendo, um atacante externo fica impossibilitado de obter informações das entidades internas.

Para que o atacante possa rastrear os veículos de uma ZM, é necessário realizar correlações entre os eventos de entrada e saída na ZM. As regiões fora das ZM são denominadas região de aplicação. Portanto, um evento de entrada significa que o veículo sai da

zona de aplicação e entra na ZM, enquanto que um evento de saída significa a um veículo sai da ZM e entra na zona de aplicação. A Figura 3.1 ilustra os eventos de entrada (E_1 e E_2) de dois veículos em um instante T_x e os eventos de saída (S_1 e S_2) em um instante T_{x+1}. Um rastreamento bem sucedido em uma ZM é feito ao identificar que o veículo que gera o evento E_1 é o mesmo veículo que gera o evento S_2, por exemplo.

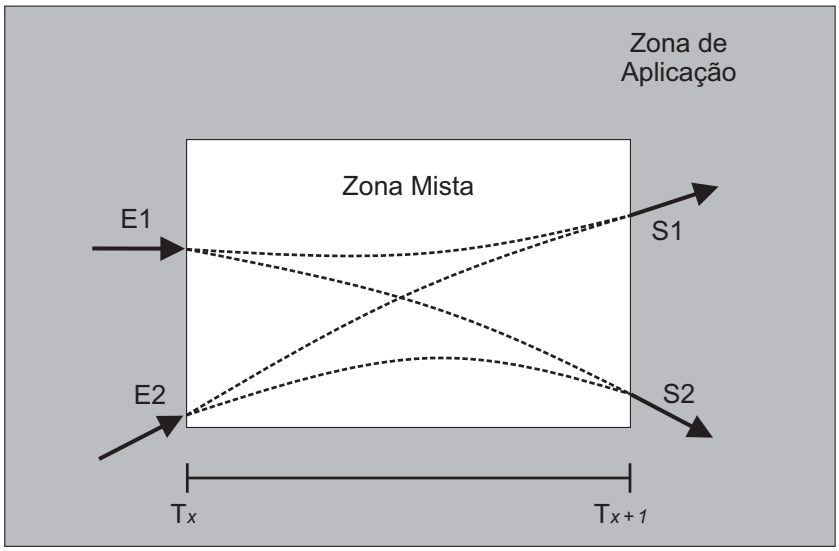

Figura 3.1 Zona Mista

Naturalmente, o atacante é capaz de utilizar as características de mobilidade obtidas sobre os veículos antes de entrar na ZM e verificar se são semelhantes às informações obtidas após a saída. Como os veículos tendem a manter a mesma direção, sentido e velocidade ao se moverem, essa inferência torna-se viável.

Em [Freudiger et al. 2007] são utilizadas zonas mistas situadas em regiões bem definidas do mapa. Ao ingressar em uma ZM, os veículos apenas se comunicam de forma cifrada, utilizando uma chave compartilhada entre eles. O gerenciamento de cada ZM é realizado por uma RSU, que é responsável por aceitar novos veículos, distribuir e atualizar a chave secreta do grupo. Ao se aproximarem de uma ZM, os veículos se comunicam com a RSU coordenadora do grupo para solicitar a chave secreta do grupo. Tal chave é enviada cifrada através de criptografia assimétrica com base na chave pública do requisitante.

A solução proposta em [Freudiger et al. 2007] define que os grupos estejam localiza-

dos em cruzamentos entre vias para dificultar correlações de pseudônimos, visto que os veículos tendem a mudar suas características de mobilidade nessas regiões. Assim sendo, os veículos se comunicam de forma cifrada nos locais onde há maior dificuldade de um atacante realizar uma correlação espacial e temporal sobre os movimentos realizados pelos veículos.

A dependência em relação à presença de RSUs em cada grupo é um forte limitante para a adoção em larga escala da solução proposta em [Freudiger et al. 2007]. Como citado, os veículos apenas protegem suas localizações enquanto pertencem aos grupos. Portanto, é necessária a uma alta densidade de RSUs para minimizar os problemas de rastreamentos. Além disso, o trabalho restringe que veículos internos aos grupos não possam informar suas localizações aos veículos externos, mesmo que eles estejam próximos entre si. Desse modo, as aplicações de segurança no trânsito ficam inviáveis.

3.1.2 Grupos Móveis

O mecanismo proposto em [Wasef and Shen 2010] não limita a formação de grupos em regiões específicas do mapa. Na proposta, sempre que um veículo deseje substituir seu pseudônimo em qualquer local do mapa, ele requisita a formação de um grupo. A ideia é permitir que os veículos se comuniquem de forma cifrada até que alguns dos veículos internos do grupo tenham realizado a substituição. Para permitir que veículos externos obtenham a localização dos internos, o trabalho propõe que todos os veículos da rede conheçam as chaves secretas utilizadas em todos os grupos. Além disso, para evitar que as informações de localizações possam ser obtidas indevidamente enquanto os veículos pertencem aos grupos, o trabalho supõe que os atacantes não conhecem tais chaves. Contudo, a suposição feita em relação às capacidades dos atacantes não é realística, pois as OBUs não são restritas aos veículos. Portanto, um atacante também conheceria as chaves secretas dos grupos, caso possuísse uma OBU [IEEE P1609.2 Working Group 2006].

O esquema apresentado em [Stübing et al. 2011] utiliza regiões pré-definidas no mapa,

denominadas células, para que sejam formados grupos criptográficos. Essas regiões são conhecidas previamente por todos os veículos da rede, isto é, cada veículo precisa saber todos os locais do mapa onde os grupos devem ser formados. Assim sendo, apesar de não haver a presença de RSUs, como em [Wasef and Shen 2010], os grupos são formados apenas em lugares específicos do mapa, como em [Freudiger et al. 2007]. No trabalho, os veículos podem continuar se comunicando em grupo, mesmo que saiam da região das células. No entanto, é definido que os grupos perdurem por um período de tempo pré-determinado.

Em [Stübing et al. 2011], as chaves dos grupos são definidas de forma colaborativa. Para isso, cada veículo envia uma mensagem contendo um fragmento de chave para todos os outros veículos contidos no local de formação do grupo. Todos os fragmentos de chaves dos veículos são utilizados para calcular a chave secreta do grupo. Assim sendo, este processo pode ser custoso, dado que é necessária a comunicação de cada veículo com todos os outros. Em relação ao raio das regiões das células, é preciso que eles sejam, no máximo, iguais à metade do alcance máximo das mensagens. Desse modo, todos os veículos dentro de uma mesma célula podem se alcançar, permitindo assim a comunicação necessária para o cálculo das chaves. Além da formação inicial do grupo, os veículos externos também podem solicitar o ingresso em grupos já formados.

3.2 PERÍODO DE SILÊNCIO ALEATÓRIO

Os períodos de silêncio aleatório ou RSPs (*Random Silent Period*) são intervalos de tempo com duração aleatória em que os veículos permanecem sem enviar mensagens. Essa técnica, utilizada em [Sampigethaya et al. 2005,Sampigethaya et al. 2007,Chen and Wei 2012], é adotada em conjunto com o processo de substituição de pseudônimos. Nessa abordagem, se os períodos de silêncio de dois ou mais veículos se sobrepuserem, torna-se mais difícil para um atacante identificar qual pseudônimo substituído pertence a cada veículo. Portanto, caso vários veículos fiquem em silêncio simultaneamente, o atacante terá maior dificuldade de identificar o emissor de cada mensagem quando eles voltarem

a enviá-las.

A técnica de RSP, no entanto, é apenas uma extensão ao processo de substituição de pseudônimos. Porém, o principal ponto negativo dessa abordagem é fazer com que os veículos passem um período de tempo significativo sem enviarem suas localizações. Em [Chen and Wei 2012], por exemplo, são utilizados períodos variando entre 0,3 segundos até 8 segundos de silêncio. Porém, esse intervalo é suficientemente grande para que dois veículos se aproximem, mas não detectem o risco de colisão entre eles. Assim sendo, a solução proposta neste trabalho desconsidera o uso de períodos de silêncio aleatório visando minimizar os riscos de colisões entre veículos.

3.3 OFUSCAÇÃO

As técnicas de ofuscação se baseiam na adulteração ou redução da precisão das informações com o intuito de proteger as entidades às quais essas informações pertencem. As informações são adulteradas para minimizar os danos caso elas sejam obtidas por entidades maliciosas. Em [Ma 2010], a técnica de ofuscação é definida como a redução da precisão da informação original, enquanto que a técnica de perturbação consiste na inserção de erros para impedir que o atacante obtenha a informação correta. Contudo, este trabalho trata qualquer modificação deliberada na informação original como sendo uma ofuscação.

Naturalmente, quanto maior for o grau de ofuscação das informações, maior será a privacidade provida. Isto é, quanto maior for a adulteração na informação ofuscada em relação à original, maior será a dificuldade de um atacante utilizar tal informação para rastrear os veículos. Porém, a ofuscação deve ser realizada de forma que os dados ofuscados ainda possam ser utilizados adequadamente pelas entidades íntegras. Essa técnica é frequentemente adotada em áreas de pesquisa como banco de dados [Narayanan and Shmatikov 2006] e redes de telefonia móvel [Quercia et al. 2011,Ardagna et al. 2011]. Em redes veiculares, porém, o seu uso tem sido pouco explorado.

A pouca utilização das técnicas de ofuscação em VANETs é decorrente do fato de

que as informações ofuscadas, se mal utilizadas, podem colocar os veículos em risco de colisão. Por exemplo, uma mensagem ofuscada pode passar a ideia de que o emissor da mensagem está distante do receptor, mesmo que as entidades estejam muito próximas entre si. Portanto, essa técnica pode ser útil para evitar rastreamentos, mas deve ser utilizada apenas quando isso não gere riscos à integridade física dos usuários.

Em [Chen and Wei 2012] é proposto um esquema de ofuscação adaptável com foco em VANETs. A ideia da proposta é ajustar o grau de ofuscação das informações de acordo com o risco de colisão entre os veículos. As localizações ofuscadas são enviadas nas *CAMs* através de uma área, isto é, uma região onde o veículo emissor se encontra. O trabalho também utiliza ofuscação de velocidade e direção. Desse modo, são informados um limite inferior e um limite superior para cada variável. Essa proposta se foca em mitigar os riscos de ocorrerem de colisões traseiras, isto é, a frente de um veículo colidindo com a traseira de outro. Além disso, o mecanismo também utiliza períodos de silêncio aleatório, abordagem citada na Seção 3.2.

Em [Chen and Wei 2012], à medida que os veículos se aproximam, o grau de ofuscação das mensagens é reduzido. Essa proximidade é calculada através da intensidade de sinal das mensagens recebidas. Além da redução do grau de ofuscação, se os veículos estiverem significativamente próximos, eles informam suas localizações exatas para permitir detecções de riscos de colisões de forma mais precisa. Porém, com as localizações exatas sendo enviadas em claro nesse contexto, os veículos ficam suscetíveis a rastreamentos. Ressalta-se que as situações de curtas distâncias entre os veículos são frequentes em vias de trânsito intenso, de modo que o mecanismo torna-se vulnerável a ataques.

RESUMO

Existem diversas propostas focadas em mitigar rastreamentos nas redes veiculares. Elas podem ser divididas em: soluções baseadas em grupo e soluções baseadas em ofuscação. De modo geral, nos trabalhos baseados em grupos, os veículos protegem suas localizações apenas enquanto pertencem aos grupos. Nos outros momentos, porém, os veículos en-

viam publicamente suas localizações exatas, possibilitando rastreamentos. Além disso, mesmo inseridos em grupos, os veículos ainda podem ser rastreados através de correlações espaciais e temporais [Wiedersheim et al. 2010, Pan and Li 2012].

As técnicas de ofuscação modificam a precisão das informações com o intuito de proteger as entidades. Porém, essa modificação pode impactar nas aplicações de segurança no trânsito, gerando situações de riscos de colisão não detectadas pelos veículos. Em [Chen and Wei 2012] é proposto que as informações sejam ofuscadas apenas enquanto os veículos não estão muito próximos entre si, minimizando as situações onde os veículos não detectaram riscos de colisão. Contudo, os veículos ficam vulneráveis a rastreamentos nas situações de proximidade.

CAPÍTULO 4

O MECANISMO PROPOSTO (HYBSEC)

Um problema comum a todos os trabalhos relacionados é a existência de contextos onde os atacantes podem obter as localizações exatas dos veículos. Diferentemente, a solução proposta nesse trabalho, denominada HybSec, impede o acesso indevido às localizações exatas dos veículos em qualquer contexto. Para isso, o HybSec utiliza simultaneamente novas técnicas de ofuscação e de grupos criptográficos. Através da união dos benefícios dessas duas técnicas, o HybSec garante que haja troca de mensagens contendo localizações exatas apenas entre veículos próximos entre si, dado que apenas estas entidades necessitam obter tais informações. Neste capítulo é apresentado o funcionamento detalhado do HybSec.

4.1 VISÃO GERAL

De modo geral, os veículos sempre propagam suas localizações ofuscadas para qualquer entidade, porém suas localizações exatas são enviadas apenas para os veículos em um mesmo grupo criptográfico. Portanto, cada veículo envia sua localização ofuscada independentemente de estar presente em um grupo. Deste modo, essas mensagens permitem que os veículos obtenham uma estimativa das condições do trânsito, provendo informações para as aplicações de monitoração colaborativa. Além disso, as localizações ofuscadas são utilizadas para que os veículos identifiquem a necessidade formar um grupo.

A formação de um grupo é realizada sempre que dois veículos encontram-se a uma distância que pode gerar riscos de colisão. Como citado, os veículos passam a trocar mensagens contendo suas localizações exatas ao formarem um grupo. Tais mensagens proveem as informações necessárias para o funcionamento adequado das aplicações de

segurança no trânsito. Além da formação inicial, é possível que haja o ingresso de novos veículos em um grupo existente. Diferentemente dos trabalhos relacionados, os grupos no HybSec não são utilizados para evitar a correlação de pseudônimos, mas para proteger a localização exata dos veículos.

O HybSec é uma solução independente da presença da infraestrutura. Portanto, não é necessária comunicação com RSUs para o funcionamento adequado da solução. Destaca-se que está fora do escopo desse trabalho definir a forma como os veículos obtêm os pseudônimos utilizados, bem como os momentos que os veículos realizam substituições de seus pseudônimos. Naturalmente, assume-se que esses procedimentos são realizados para evitar que as rotas dos veículos sejam reveladas através da simples verificação do emissor de *CAMs* consecutivas.

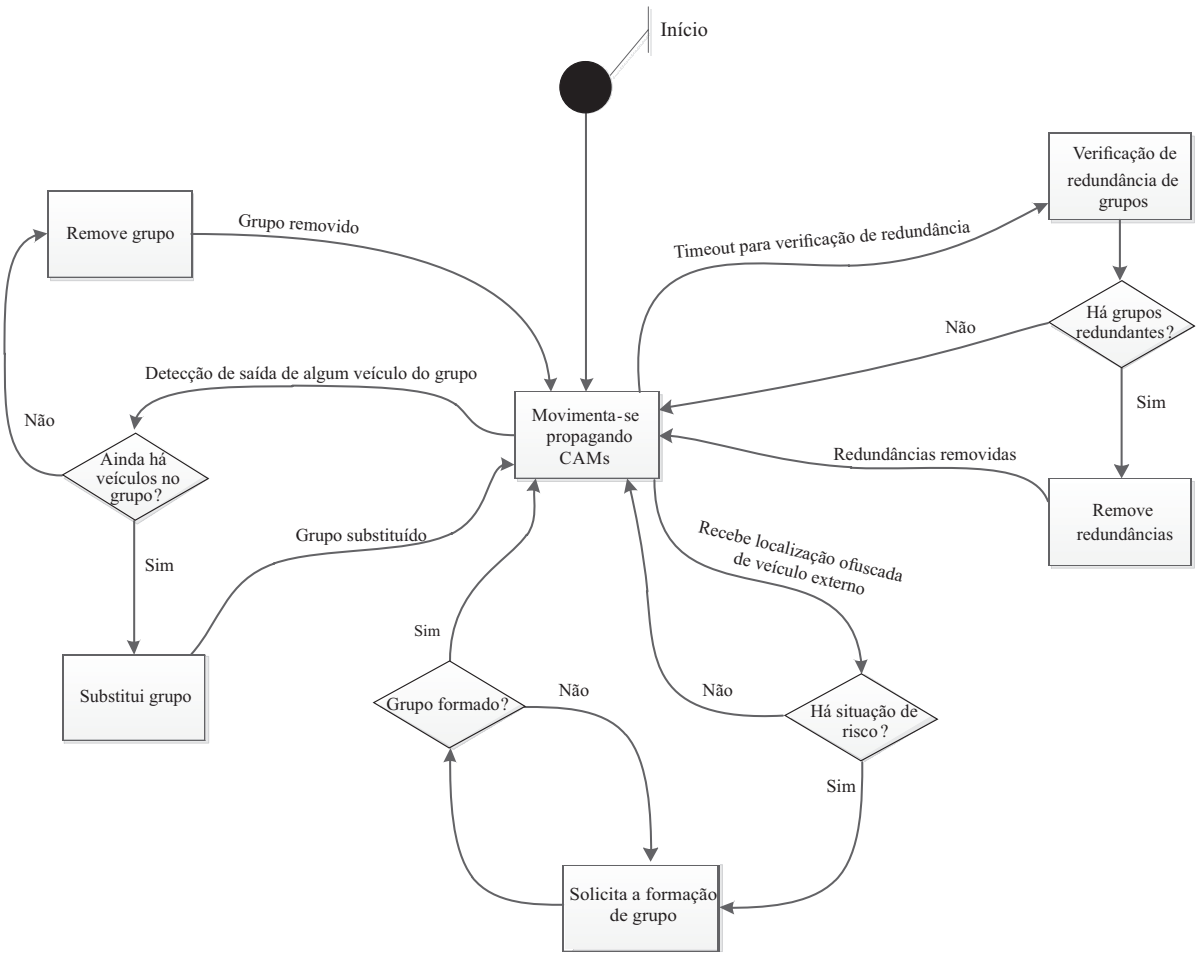

Figura 4.1 Visão geral do HybSec.

A Figura 4.1 apresenta um fluxograma contendo uma visão geral dos estados e ações do HybSec. De modo geral, ao iniciar o mecanismo para cada veículo (ex: o motorista liga o veículo), é iniciado o estado de *Movimenta-se propagando CAMs*. Nesse estado, os veículos permanecem enviando *CAMs* contendo suas localizações ofuscadas e, se pertencerem a grupos, enviando também suas localizações exatas. A partir desse estado, os veículos podem ingressar em grupos (parte inferior da Figura), terminar grupos existentes (parte esquerda da Figura) ou eliminar grupos redundantes (parte direita da Figura).

4.2 MODELO DE AMEAÇA

O modelo de ataque do HybSec considera um atacante global, autêntico e passivo. Ao considerar um atacante global, assume-se que ele é capaz de capturar simultaneamente todas as mensagens trocadas na rede. Naturalmente, o texto claro de cada mensagem só pode ser obtido se ela for transmitida sem criptografia ou se o atacante possuir a chave para decifrá-las. Na prática, um atacante global pode ser um conluio de dispositivos distribuídos ao longo das rodovias de uma cidade. Apesar de ser improvável obter uma cobertura completa de todo o mapa de rodovias, ao considerar um atacante global é possível lidar com o pior caso de ataques em conluio.

Um atacante autêntico é uma entidade que possui uma OBU. Portanto, ele é capaz de verificar a autenticidade das mensagens e receber mensagens enviadas pela AC. Assim sendo, não é possível realizar suposições sobre informações da rede conhecidas pelos veículos, porém desconhecidas pelos atacantes. Em [Wasef and Shen 2010], por exemplo, assume-se que todos veículos autênticos possuem uma chave que é utilizada para decifrar as mensagens de qualquer grupo, porém os atacantes não as possuem. Ao considerar um atacante autêntico, não se pode realizar tal suposição.

Um atacante passivo, por sua vez, é uma entidade que apenas realiza captura de mensagens. Portanto, ele é capaz de obter todas as mensagens contendo as localizações dos veículos da rede, desde que as informações sejam enviadas em texto claro. Contudo, tal atacante não envia mensagens na rede. Assim sendo, esse atacante ameaça apenas a

confidencialidade das informações, mas não a integridade ou autenticidade.

O modelo de ameaça baseado em atacantes passivos é utilizado tanto nesse trabalho como nos trabalhos relacionados. Atualmente, o modelo de ameaça considerando um atacante global, autêntico e ativo é um problema em aberto na literatura. Destaca-se que são considerados apenas rastreamentos feitos com base nas informações contidas nas mensagens enviadas pelos veículos. Portanto, este trabalho não trata de ataques que utilizem sensores, câmeras ou radares, por exemplo. Além disso, não são tratados atacantes que controlem indevidamente a comunicação de veículos autênticos, e os utilizem para realizar rastreamentos de outros veículos.

4.3 OFUSCAÇÃO

Todas as *CAMs* enviadas contêm a localização ofuscada de seu emissor. Através dessa informação, os veículos em proximidade são capazes de detectar uma aproximação em relação às outras entidades. A localização ofuscada um dado veículo não é informada através de um único ponto onde o veículo está posicionado, mas de uma região de circular onde o emissor está contido.

A região de ofuscação é calculada de forma pseudoaleatória. Portanto, a posição real do emissor pode ser qualquer ponto (x, y) contido em tal região. O ponto central (x', y') da região de ofuscação é calculado através da geração aleatória de dois valores: uma distância d em relação à posição real do veículo e um ângulo de inclinação α do segmento de reta entre (x, y) e (x', y') em relação ao eixo das abcissas do plano cartesiano. Seja r o raio da região de ofuscação, então $0 \leq d \leq r$; e $0 \leq \alpha < 2\pi$. A Figura 4.2 ilustra a geração do ponto central da região de ofuscação, onde x' e y' são definidos através da Equação (4.1) a seguir:

$$\begin{aligned} x' &= x + d \times cos(\alpha), \\ y' &= y + d \times sen(\alpha). \end{aligned} \tag{4.1}$$

Ao receber uma mensagem ofuscada, o receptor não é capaz de obter a localização

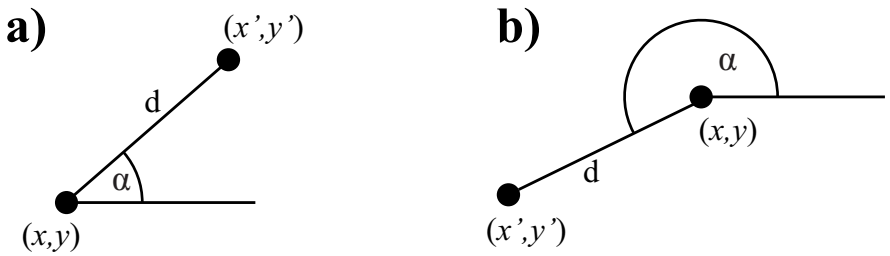

Figura 4.2 Geração de regiões de ofuscação. a) $0 < \alpha < \pi$; b) $\pi < \alpha < 2\pi$.

exata do emissor. Nesse caso, é possível apenas identificar que há um veículo localizado dentro de tal região. De mesma forma, essa limitação também é válida para um atacante que capture a mensagem. Como apresentado no Capítulo 5, a existência de dois ou mais veículos em proximidade enviando mensagens ofuscadas eleva a dificuldade de rastreamentos. Essa dificuldade também pode ser definida como a entropia da rede.

Além da ofuscação de localizações, os veículos também podem ofuscar outras informações sobre suas características de mobilidade. Por exemplo, podem ser ofuscadas a velocidade, a direção ou a aceleração dos veículos. Neste trabalho, a localização é única característica de mobilidade informada pelos veículos e, portanto, apenas essa informação é ofuscada. Quaisquer outras informações utilizadas pelas aplicações podem ser enviadas de forma ofuscada através campo *Informações Extras de Mobilidade*, contido nas *CAMs* (Seção 4.8.2). As ofuscações nesses casos são feitas de modo que os veículos informam uma faixa de valores em que a informação real está contida. Portanto, as mensagens devem conter os valores mínimo e máximo dessa faixa de valores.

4.4 SITUAÇÕES DE RISCO

A necessidade de comunicação em grupo surge através da percepção de um risco de colisão. Considere dois veículos A e B não pertencentes a um mesmo grupo. Caso B receba a *CAM* enviada por A, o veículo B verifica se existe uma situação de risco. A verificação da situação de risco é calculada através da sobreposição entre a região ofuscada, contida na mensagem recebida, e a região de guarda do veículo receptor. A região de guarda é

uma região centrada na posição real do receptor da mensagem e com raio maior ou igual ao raio de ofuscação (r).

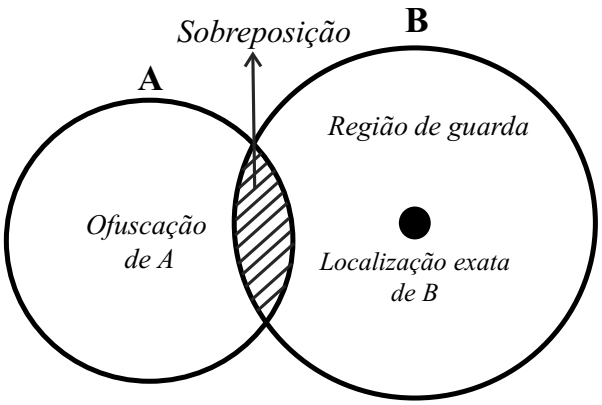

Figura 4.3 Situação de Risco detectada por B.

A Figura 4.3 ilustra a verificação de sobreposição realizada por B. No cenário ilustrado, caso B verifique que há sobreposição, uma mensagem *Group Request* é enviada solicitando a formação de um grupo. No entanto, esta mensagem não contém a localização real de B, mas apenas sua localização ofuscada, visto que os veículos ainda não formaram um grupo nesse momento. Nesse caso, o grupo apenas será estabelecido se A também detectar que há uma situação de risco entre as entidades.

O raio (r_g) da região de guarda é definido por $r_g = r \times f_g$, onde f_g é o fator de guarda. Através do fator de guarda é possível aumentar, quando necessário, o raio da região de guarda em relação ao raio de ofuscação. O f_g é utilizado para minimizar a ocorrência de diferentes interpretações sobre a necessidade de formação de grupos entre A e B. Assim sendo, minimizam-se as circunstâncias onde B detecta a situação de risco ao receber a *CAM*, porém A não detecta ao receber o *Group Request*. Para isso, o raio da região de guarda (r_g) é aumentado ($f_g > 1$) especificamente no recebimento do *Group Request* durante a requisição inicial de comunicação em grupo.

4.5 GRUPOS CRIPTOGRÁFICOS

O objetivo dos grupos criptográficos é garantir um canal de comunicação seguro contra um atacante global e passivo. Deste modo, os veículos podem trocar mensagens contendo suas localizações exatas e, ainda assim, não ficarem vulneráveis a rastreamentos em relação ao atacante. No HybSec, o gerenciamento dos grupos é realizado pelos próprios veículos e, portanto, independente de RSUs.

Ao ingressarem em um grupo, os veículos passam a enviar suas localizações exatas para as outras entidades do grupo através de um campo cifrado das *CAMs*. Desta forma, cada veículo do grupo é capaz de detectar aproximações, distanciamentos ou riscos de colisões de forma precisa. Contudo, ainda assim é possível que os veículos fiquem em situação de risco, mesmo pertencendo a um grupo. Isso ocorre porque os veículos fora do grupo podem se aproximar dos veículos pertencentes ao grupo. Assim sendo, é necessário que haja uma troca de informações entre os veículos internos e externos aos grupos, permitindo a detecção das situações de risco e o ingresso de veículos externos nos grupos.

Visando minimizar a sobrecarga na rede decorrente do envio de *CAMs* distintas para os veículos internos e externos, apenas uma mensagem é utilizada para propagar tanto a localização precisa quanto a ofuscada. Para isso, as localizações exatas são enviadas em campos cifrados, porém as localizações ofuscadas são enviadas em claro através de uma mesma mensagem.

Caso um veículo pertença a mais de um grupo simultaneamente, é necessário que *CAMs* distintas sejam enviadas para cada um dos grupos, visto que as chaves secretas, utilizadas para cifrar as mensagens, são diferentes em cada grupo. Nesse caso, a localização ofuscada do emissor é mantida constante ao enviar *CAMs* para grupos simultâneos, minimizando o problema de ofuscações sobrepostas, descrito em [Ardagna et al. 2011]. Esse problema ocorre quando um veículo envia duas ou mais mensagens contendo localizações ofuscadas diferentes, e um atacante captura essas informações. Através da interseção das regiões ofuscadas, o atacante é capaz de obter uma estimativa mais precisa sobre a localização do veículo, dado que o veículo está, necessariamente, localizado na interseção

de tais regiões.

4.6 FORMAÇÃO DE GRUPOS

O processo de formação de um novo grupo é realizado sempre entre dois veículos, apenas. A Figura 4.4 ilustra a formação de um grupo entre os veículos A e B. Imediatamente após B detectar a situação de risco, tal veículo envia para A uma mensagem *Group Request*. A localização ofuscada de B, contida na mensagem, é utilizada para que A também verifique a existência de situação de risco entre as entidades. Caso também seja verificada, A poderá criar um novo grupo ou aceitar B em um grupo pré-existente. Prioritariamente, a decisão tomada por A é utilizar um grupo pré-existente para a comunicação entre as entidades. Caso A pertença a mais de um grupo, ele aceitará B no grupo com maior número de veículos. Com isso, minimiza-se a quantidade de grupos simultâneos em que os veículos participam.

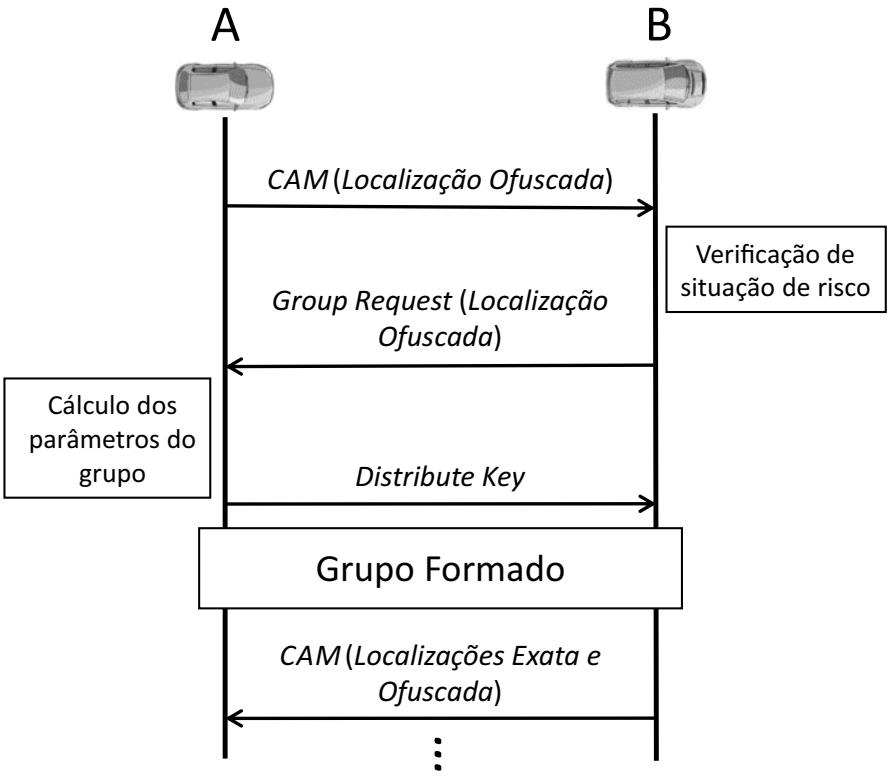

Figura 4.4 Formação de um novo grupo.

Na formação de um grupo, o veículo requisitado (A) torna-se o líder, isto é, o responsável por definir o ID do grupo e a chave simétrica a ser utilizada. Após verificar a situação de risco entre as entidades, o veículo A envia uma mensagem *Distribute Key* contendo os parâmetros do grupo. Caso A pertença a um grupo pré-existente, tais parâmetros não são recalculados, mas apenas enviados para B. Destaca-se que, em grupos pré-existentes, qualquer veículo do grupo pode aceitar a entrada de novas entidades. Os parâmetros privados contidos na *Distribute Key* são cifrados através da chave pública do receptor. Portanto, a chave secreta utilizada no grupo formado entre A e B é cifrada com o pseudônimo de B e enviada como parte da *Distribute Key*. O conteúdo de cada mensagem é detalhado na Seção 4.8.2.

4.7 PARÂMETROS DO GRUPO

Os campos de identificação de cada grupo, contidos nas mensagens internas, permitem que os receptores verifiquem se eles pertencem ao grupo ao qual a mensagem está endereçada. A identificação de um grupo é realizada através da *tupla* composta pelo ID do grupo ($group\_ID$) e a chave pública do líder ($lider\_pub\_key$). Tais informações são enviadas em claro e contidas em cada mensagem interna.

O ID do grupo é calculado pelo líder através de uma função de dispersão SHA–256, conforme a Equação (4.2) a seguir:

$$group\_ID = SHA\text{–}256(lider\_pub\_key \| contador\_de\_grupos).$$

Além da chave pública do líder, também é utilizado um contador de grupos como parâmetro para a geração do ID do grupo. Esse campo é incrementado pelo líder a cada novo grupo criado. Dessa forma, caso o líder crie mais de um grupo antes da substituição de sua chave pública, os IDs dos grupos criados serão diferentes. Assim como o ID do grupo, a chave simétrica (sim_k) é calculada através de uma função SHA-256, conforme:

$$sim\_k = SHA\text{–}256(lider\_ID \| lider\_pub\_key \| group\_ID), \tag{4.2}$$

onde $lider\_ID$ é ID real do líder do grupo, $lider\_pub\_key$ é a chave pública do líder e $group\_ID$ é o identificador do grupo. Ressalta-se que o ID real de cada veículo é uma informação privada e conhecida apenas pelo próprio e pela AC.

Naturalmente, é possível utilizar outras funções de dispersão, como SHA-512 ou SHA-3, para o cálculo da chave. É utilizada a SHA-256 devido ao tamanho de saída de 256 bits, compatível com o tamanho máximo da chave do AES. O AES, por sua vez, é o algoritmo de criptografia simétrica utilizado na comunicação em grupos. Destaca-se que a SHA–256 é uma função de dispersão resistente à colisão e recomendada pelo NIST (*National Institute of Standards and Technology*).

Um dos requisitos de segurança em VANETs é garantir que as mensagens sejam passíveis de auditorias. Em geral, os trabalhos que utilizam comunicação cifrada entre veículos não se preocupam em prover informações necessárias para que uma autoridade possa obter os textos claros das mensagens trocadas. Diferentemente, o esquema de cálculo das chaves utilizado no HybSec garante à AC a capacidade de obter as chaves simétricas de todos os grupos e, consequentemente, os textos claros das mensagens cifradas com tais chaves.

Para que a AC possa calcular a sim_k de um dado grupo, apenas é necessário que seja obtida uma mensagem interna do grupo. Dentre os três argumentos utilizados para o cálculo de sim_k, os campos $group\_ID$ e a $lider\_pub\_key$ são transmitidos em claro em cada mensagem. Naturalmente, a chave não pode ser obtida apenas a partir de tais argumentos, visto que o $lider\_ID$ é necessário para calculá-la. No entanto o $lider\_ID$ é trivialmente obtido pela AC, pois a AC possui um mapeamento entre o ID real dos veículos e todas as suas chaves públicas. Portanto, mesmo sem obter informações além das contidas nas mensagens, a AC é capaz de obter a chave utilizada para decifrá-las.

Em situações de auditoria, é necessário que seja submetido um conjunto de mensagens para a AC. Dependendo do protocolo definido para essas situações, as RSUs ou os próprios veículos podem submeter tais mensagens. Porém, vale ressaltar que quaisquer análises ou submissões de mensagens realizadas no processo de auditoria estão fora do escopo desse trabalho. Contudo, a solução proposta provê à AC a capacidade de realizar tais

auditorias.

4.8 SUBSTITUIÇÃO E TÉRMINO DE GRUPOS

A mobilidade dos veículos gera um alto dinamismo em relação aos eventos de entradas e saídas em grupos. Como os veículos possuem características de mobilidades diferentes, é natural que frequentemente alguns deles saiam do alcance do grupo. Como exemplo, haverá o estabelecimento de um grupo entre dois veículos caso eles se cruzem em sentidos opostos de uma rodovia. Porém, esse grupo se tornará desnecessário após o distanciamento dos veículos, dado que o grupo é composto apenas pelos dois. Portanto, é necessário que as entidades removam o grupo formado. Em grupos compostos por mais de dois veículos, a saída de algum deles implicará na substituição do grupo através do processo de RGP (*Replacement Group Procedure*).

Além da saída isolada de veículos, a diferença das características de mobilidade pode gerar segregações dos grupos ao longo do tempo. A detecção desses eventos é realizada através de um monitoramento individual de cada veículo, contabilizando o instante de recebimento das últimas mensagens enviadas pelas outras entidades do grupo. Assim sendo, não há sincronização entre os veículos, centralização de responsabilidades ou pontos únicos de falhas. Portanto, cada entidade possui uma visão particular sobre a presença dos outros elementos no grupo. O RGP permite que haja uma modificação no grupo de forma que este possa refletir a realidade corrente dos veículos. Assim sendo, o RGP é importante para (1) remoção de veículos que saem do grupo, (2) divisão do grupo em subgrupos, (3) eliminação de grupos desnecessários e (4) modificação da chave simétrica.

Como descrito na Seção 4.8.1, um dado veículo A considera o grupo G_1 como redundante caso verifique que todos os veículos de G_1 estão contidos em outro grupo no qual A pertence. Apenas se G_1 não for redundante, A informa a necessidade de substituição de G_1 aos outros veículos do grupo. A requisição para substituição do grupo é realizada através de uma mensagem *Replace Group Request*, que é enviada após um período aleatório de espera (*time_to_request*). Esse período de espera permite minimizar

as situações de requisições simultâneas enviadas por veículos distintos.

A mensagem *Replace Group Request* é responsável por indicar que houve um evento de saída e que o requisitante deseja substituir G_1. Caso a substituição do grupo seja confirmada pelos outros veículos do grupo, o requisitante se tornará o líder do novo grupo. Como só recebem requisições as entidades que estão ao alcance do emissor, então os veículos que saíram do grupo, mesmo que ainda não identificados, não as receberão.

A Figura 4.5 ilustra a comunicação entre dois veículos (A e B) durante o RGP. Caso o grupo seja composto por outros veículos além de A e B, todos eles receberão a requisição feita por A. Assim sendo, a troca de mensagens ilustrada na Figura será realizada entre A e todos os veículos receptores da requisição.

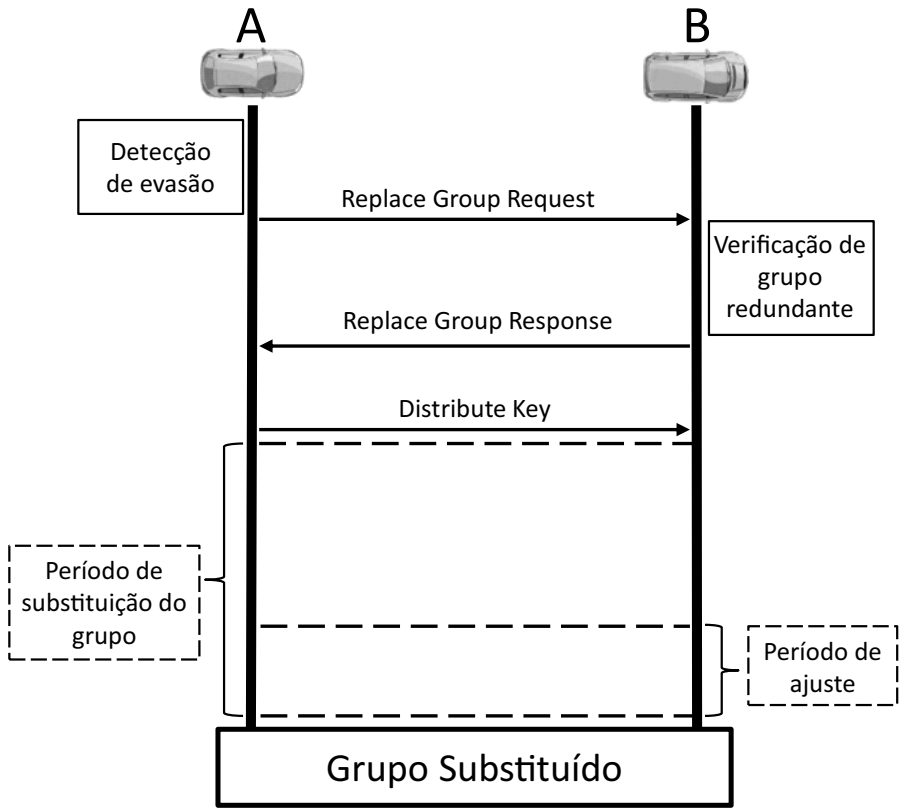

Figura 4.5 RGP - Troca de mensagens entre A e B para substituição de grupo.

Ao receber a *Replace Group Request*, B verifica se G_1 é um grupo redundante e, caso negativo, uma mensagem *Replace Group Response* é dada como resposta. O recebimento

da primeira resposta à requisição feita indica que A deve calcular os parâmetros do novo grupo (G_2). Caso A não receba respostas à *Replace Group Request*, uma nova requisição é enviada após um período aleatório de espera (*time_to_request*).

Após A calcular os parâmetros de G_2, a chave simétrica do novo grupo é enviada como conteúdo da mensagem *Distribute Key*. Essa chave simétrica é cifrada com a chave pública de B para garantir que apenas B será capaz de decifrá-la. Deste modo, inviabiliza-se que veículos que tenham saído do grupo, mesmo possuindo a chave simétrica de G_1, possam decifrá-la. Especificamente no processo de RGP, a *Distribute Key* contém os IDs de G_1 e G_2, permitindo que o receptor valide a substituição do grupo. Portanto, B verifica se o ID de G_1 corresponde ao grupo que A requisitou substituir.

Ao ser distribuída a chave simétrica de G_2 por A, inicia-se o *período de substituição do grupo* (Figura 4.5). Como não há sincronia sobre quais veículos estão presentes em cada grupo, este período é utilizado para que todos os veículos de G_1 tenham tempo hábil para substituí-lo. Após substituí-lo, cada veículo identifica G_1 como inativo. Desse modo, não é aceito o ingresso de novos veículos em G_1. Portanto, caso haja situação de risco em relação a veículos fora de G_1, será utilizado outro grupo (como G_2) para comunicação cifrada entre as entidades. A remoção de G_1 ocorre após o período de substituição.

A movimentação dos veículos, a perda de mensagens e outros fatores podem colaborar para que um ou mais veículos de G_1 não ingressem em G_2 durante o período de substituição. Portanto, tais veículos passarão a se comunicar de forma ofuscada após a substituição, mesmo estando em situação de risco entre si. Visando mitigar esse problema, o *período de ajuste* (Figura 4.5) é utilizado para que todos os veículos de G_1 verifiquem se o emissor de uma *CAM*: (1) está em situação de risco e (2) não está em outro grupo comum a ambos. Caso (1) e (2) sejam positivos, uma requisição direcionada de comunicação em grupo (*Group Request*) é enviada ao emissor da *CAM*. Neste momento, como ambos os veículos ainda pertencem a G_1, a mensagem *Group Request* contém a localização exata do veículo requisitante.

4.8.1 Redundância de Grupos

Como citado, é possível que alguns veículos permaneçam simultaneamente em mais de um grupo ativo. Por exemplo, se um veículo V_2 detecta um risco em relação aos veículos V_1 e V_3 em um momento T_1, então duas mensagens *Group Request* são enviadas por V_2, uma para cada um dos outros veículos. Nesse caso, se os receptores da requisição confirmarem a situação de risco através da *Distribute Key*, V_2 entrará em dois grupos distintos simultaneamente. Essa situação é ilustrada na letra *a*) da Figura 4.6.

Na letra *b*) da Figura 4.6 é apresentado, em um momento T_2, a aproximação entre os veículos V_1 e V_3. Essa aproximação gera a necessidade de comunicação em grupo entre as entidades. Considerando que V_1 envia o *Group Request*, então o veículo V_3 aceita V_1 em G_2. Ressalta-se que, prioritariamente, os veículos se comunicam através de grupos pré-existentes e, apenas se isso não for possível, um novo grupo é criado. Como ambas as entidades passam a pertencer ao grupo G_2, então G_1 torna-se redundante para V_1 e V_2. Portanto, tais veículos devem remover G_1 de suas listas de grupos.

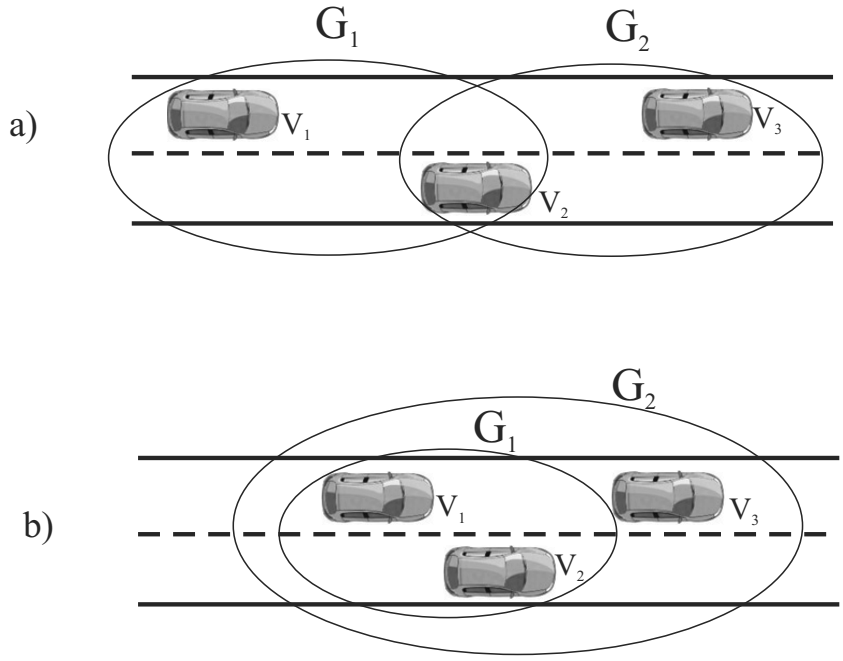

Figura 4.6 Grupos Redundantes.

Na prática, a verificação de redundância de grupos é feita frequentemente por cada

veículo para identificar se algum grupo está totalmente contido em outro. Está definido na Seção 5.2 a frequência com que esse procedimento é realizado nas simulações. Matematicamente, é feita a verificação de continência de um grupo em relação a outro. O custo máximo de cada verificação é $n * q$, onde n e q são os tamanhos dos grupos analisados.

4.8.2 Mensagens Utilizadas

Ao longo da descrição do HybSec, os tipos de mensagens trocadas entre os veículos foram citadas. A seguir é apresentado um detalhamento das informações que compõem cada uma dessas mensagens. Ressalta-se que não são apresentados os campos das mensagens não utilizados diretamente pelo mecanismo proposto. Portanto, campos como *timestamp* (carimbo de tempo) ou *symm_algorithm* (algoritmo de cifra simétrica utilizado), especificados pelo padrão IEEE 1602.2, não são descritos. Algumas das informações contidas nas mensagens são enviadas através de mais de um campo, como o par de coordenadas utilizado para informar a localização de um veículo.

Na descrição das mensagens, todas as informações enviadas cifradas através da chave secreta do grupo estão explicitamente indicadas através do símbolo $(*)$, enquanto que as informações cifradas com a chave pública do destinatário estão indicadas através do símbolo $(+)$. Portanto, subentende-se que as outras informações são enviadas em claro.

4.8.2.1 Informações Comuns a Todas as Mensagens - 109 bytes

A fim de evitar repetições nas descrições das mensagens, os campos comuns a todas elas estão apresentadas na Figura 4.7. As informações contidas em cada campo são apresentadas a seguir:

Pseudônimo do Emissor (*psd_em*) - 32 bytes

Identificador do emissor da mensagem. Como o pseudônimo também é a chave pública do veículo, essa chave é utilizada para cifra assimétrica de informações. O tamanho desse campo depende do algoritmo de criptografia assimétrica utilizado.

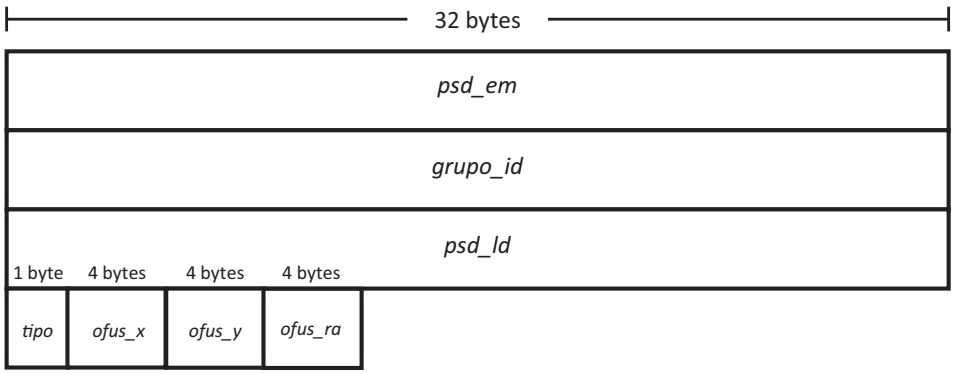

Figura 4.7 Campos comuns a todas as mensagens.

Neste trabalho, utiliza-se criptografia de curvas elípticas com chaves públicas de 32 bytes.

ID do Grupo (*grupo_id*) - 32 bytes

Identificador do grupo de destino da mensagem. Este campo permanece vazio se a mensagem não for destinada a um grupo.

Pseudônimo do Líder (*psd_ld*) - 32 bytes

Identificador do líder do grupo de destino da mensagem. Esse campo é utilizado para que o receptor identifique qual veículo definiu da chave do grupo. Através dele, a AC é capaz de recuperar a chave simétrica do grupo. Este campo permanece vazio se a mensagem não for destinada a um grupo.

Tipo da Mensagem (*tipo*) - 1 byte

Campo indicando o tipo da mensagem.

Localização Ofuscada ($ofus\_x$, $ofus\_y$ e $ofus\_ra$) - 12 bytes

Par de coordenadas indicando a localização ofuscada do emissor, juntamente com o raio de ofuscação utilizado

4.8.2.2 CAM - 141 bytes

A Figura 4.8 apresenta os campos contidos na *CAM*, além dos campos comuns a todas as mensagens.

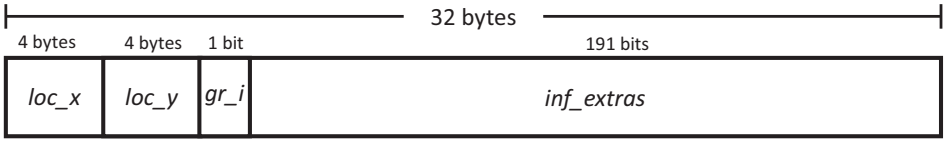

Figura 4.8 Estrutura da *CAM*.

Localização Exata (loc_x e loc_y) - 8 bytes ($*$)

Par de coordenadas da localização exata do emissor. Caso a mensagem não seja enviada para um grupo, este campo permanece vazio.

Grupo Inativo (gr_i) - 1 bit

Campo indicando se o grupo de destino está inativo. Esse campo é marcado como positivo caso a mensagem seja destinada a um grupo e se este grupo estiver durante o período de substituição.

Informações Extras de Mobilidade (inf_extras) - 191 bits

Campo utilizado para o envio de informações adicionais sobre a mobilidade dos veículos, como velocidade e aceleração. As informações enviadas são dependentes da aplicação que utiliza o HybSec. Neste trabalho, este campo não é utilizado.

4.8.2.3 Group Request - 109 bytes

As informações contidas no *Group Request* são apenas os campos comuns a todas as mensagens.

4.8.2.4 Distribute Key - 213 bytes

A Figura 4.9 apresenta os campos contidos na *Distribute Key*, além dos campos comuns a todas as mensagens.

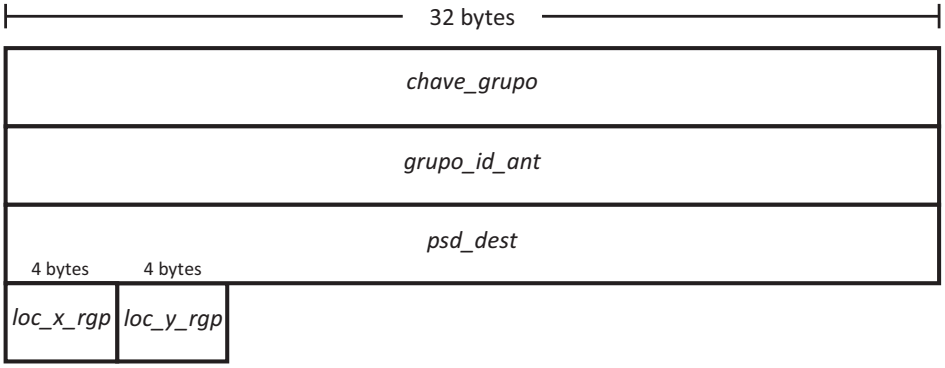

Figura 4.9 Estrutura da *Distribute Key*.

Chave do Grupo (*chave_grupo*) - 32 bytes (+)

Chave simétrica do grupo em que o destinatário irá ingressar.

ID do Grupo Antigo (*grupo_id_ant*) - 32 bytes (+)

Identificador do grupo que será substituído. Esse campo é utilizado apenas durante o RGP.

Pseudônimo do Destinatário (*psd_dest*) - 32 bytes

Identificador do destinatário da mensagem.

Localização Exata (*loc_x_rgp* e *loc_y_rgp*) - 8 bytes (+)

Par de coordenadas da localização exata do emissor. Essa localização exata não é enviada na formação inicial do grupo, mas apenas no processo RGP. Destaca-se que no RGP, o emissor e o destinatário já pertencem previamente a um mesmo grupo.

4.8.2.5 Replace Group Request - 109 bytes

As informações contidas nesta mensagem são apenas os campos comuns a todas as mensagens.

4.8.2.6 Replace Group Response - 141 bytes

A Figura 4.10 apresenta os campos contidos na *Replace Group Response*, além dos campos comuns a todas as mensagens.

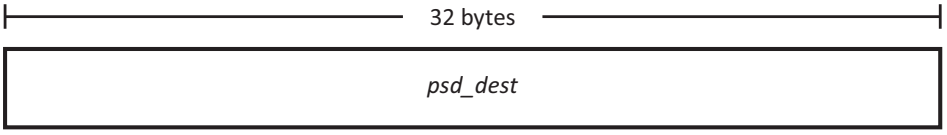

Figura 4.10 Estrutura da *Replace Group Response*.

Pseudônimo do Destinatário (*psd_dest*) - 32 bytes

Identificador do destinatário da mensagem.

RESUMO

O HybSec utiliza simultaneamente técnicas de ofuscação e de grupos criptográficos para mitigar rastreamentos em *VANETs*. Nele, os veículos sempre enviam mensagens contendo suas localizações ofuscadas. Contudo, ao se aproximarem de outras entidades, os veículos formam grupos criptográficos e passam a trocar mensagens contendo suas localizações exatas. Assim sendo, qualquer veículo é capaz de conhecer a localização estimada de todos os outros, mas apenas os veículos em proximidade são capazes de conhecer as localizações exatas. Desse modo, as necessidades das aplicações de segurança e monitoramento são atendidas pela solução.

Depois de formados, os grupos podem precisar ser reestruturados devido à sua segmentação ou saída de veículos. Para isso, é utilizado o processo de substituição de grupos

(RGP). Nesse processo, os veículos que saíram do grupo são eliminados e a chave simétrica é modificada. Como característica que diferencia o HybSec dos trabalhos relacionados, destaca-se que um atacante global e passivo não é capaz de obter a localização exata de qualquer veículo em nenhum contexto.

CAPÍTULO 5

AVALIAÇÃO DE DESEMPENHO

Com o intuito de avaliar o desempenho do mecanismo proposto, este capítulo apresenta a avaliação de desempenho realizada. São descritos os parâmetros e métricas utilizados, bem como os resultados obtidos através das simulações. Os mecanismos propostos em [Stübing et al. 2011] e [Chen and Wei 2012], considerados as melhores abordagens dentre os trabalhos relacionados, são analisados em comparação com a solução proposta neste trabalho. Nos gráficos e descrições apresentados, tais trabalhos são identificados como Stübing e SafeAnon, respectivamente.

O desempenho do HybSec foi avaliado através uma implementação com linguagem programação Java. Em tal implementação, as principais classes definidas são *Vehicle* e *Controller*. A primeira delas é responsável por realizar as rotinas de verificação de *timeouts* e envios e processamentos de mensagens para comunicação através de grupos e de mensagens ofuscadas. A segunda é responsável por intermediar a comunicação entre as entidades, isto é, entregar as mensagens enviadas pelos veículos. Além disso, foram definidas classes auxiliares para as rotinas de criptografia, assinaturas digitais, conversão das mensagens para formatos binários, dentre outras.

Os registros das movimentações dos veículos não são gerados pelo HybSec, mas pelo simulador de mobilidade VanetMobiSim [Härri et al. 2007]. Portanto, através do VanetMobiSim foram geradas as coordenadas de cada veículo ao longo da simulação. Na prática, as coordenadas dos veículos representam os movimentos realizados por eles, como ultrapassagens, curvas ou reduções de velocidades, por exemplo.

Através do VanetMobiSim, é definido o mapa de rodovias utilizado pelos veículos. Além disso, são definidos os parâmetros relativos às mobilidades, como tempo de movimentação dos veículos no mapa, velocidade e aceleração máximas. Depois de realizada a

geração da mobilidade, os registros são importados para as implementações do HybSec e dos trabalhos relacionados, permitindo uma comparação entre tais propostas.

5.1 CENÁRIO DE MOBILIDADE

As simulações de mobilidade foram realizadas em uma área de 2,56 km^2 (1,6 km X 1,6 km) da cidade de São Francisco - CA, nos Estados Unidos. A Figura 5.1 ilustra a região da cidade utilizada. O mapa das simulações foi obtido através do U.S. Census Bureau [U.S. Census Bureau 2013].

Figura 5.1 Região utilizada nas simulações. Cidade de São Francisco - CA.

Para a geração de mobilidade com o VanetMobiSim, são consideradas uma velocidade máxima de 110 km/h e aceleração máxima de 4,5 m/s^2. Naturalmente, ambos são limites superiores. Contudo a velocidade e a aceleração desenvolvidas nas simulações dependem de diversos fatores como a densidade de veículos na rodovia, a quantidade de sinais de trânsito e o número de faixas. A velocidade mínima considerada é de 15 km/h. Esse parâmetro indica a menor velocidade que um veículo pode trafegar em condições mobilidade normais. A desaceleração padrão, considerada 2 m/s^2, é a desaceleração confortável para o motorista em uma frenagem. Além disso, foi utilizado 1 m/s^2 para o limiar de aceleração lateral, que especifica a aceleração máxima que um veículo exerce lateralmente ao mudar de faixa. A distância de segurança (*space headway*) entre os veículos é de 2 metros, isto é, em situações de congestionamento e trânsito parado, os veículos mantêm uma distância mínima de 2 metros entre si. O tempo de segurança (*time headway*) indica o intervalo de tempo entre um veículo V_1 alcançar um ponto P da rodovia e o veículo V_2, localizado logo atrás de V_1, também alcançar o ponto P. O tempo de segurança utilizado é de 2 segundos. A Tabela 5.1 apresenta os parâmetros de mobilidade utilizados.

Tabela 5.1 Parâmetros de mobilidade.

Velocidade máxima	110 km/h
Velocidade mínima	15 km/h
Aceleração máxima	4,5 m/s^2
Limiar de aceleração lateral	1 m/s^2
Desaceleração padrão	2 m/s^2
Space headway	2 metros
Time headway	2 segundos

Cada simulação reflete em trinta minutos de movimentação real dos veículos ao longo do mapa. Além disso, são realizadas vinte simulações para cada ponto dos gráficos e os resultados são apresentados com intervalo de confiança de 99%. Foram analisadas den-

sidades de veículos variando entre 50 veículos/km^2 e 800 veículos/km^2, refletindo desde um trânsito pouco denso até um cenário de trânsito intenso e forte congestionamento.

5.2 PARÂMETROS DE SIMULAÇÃO

Conforme orientações da família de padrões IEEE 1609, o alcance máximo das mensagens utilizado é de 300 metros, dado que a simulação é realizada em ambientes urbanos. Além disso, o período médio de envios de *CAMs* é de 200 milissegundos. Contudo, os veículos enviam essas mensagens de forma probabilística, com intervalo mínimo de 150 milissegundos e máximo de 300 milissegundos entre duas *CAMs* consecutivas.

A alta mobilidade dos veículos, a densidade da rede e as interferências no meio de comunicação são alguns dos fatores que podem afetar negativamente a entrega de mensagens. Naturalmente, os ambientes com maior densidade ou com veículos se movendo em velocidades elevadas tendem a aumentar a taxa de perda de mensagens na rede. Além disso, a interferência com o meio, a falta de visada entre os veículos e outros fatores podem ser relevantes para definir taxa de perda de mensagens em um ambiente real. Está fora do escopo desse trabalho a análise dos fatores que tornam os veículos mais propensos a perderem mensagens durante a comunicação. Contudo, visando prover uma melhor percepção sobre os impactos que a perda de mensagens pode causar aos trabalhos comparados, todos os cenários foram simulados com três diferentes taxas de perda. As taxas de perda (Tp) utilizadas foram: 2% (baixa), 8% (média) e 16% (alta), conforme a análise feita em [Bai et al. 2010].

Os períodos estáticos utilizados para a simulação do HybSec são: 9 segundos para *período de substituição do grupo*, 3 segundos para *período de ajuste*, 3 segundos para *período de remoção de redundância* e 0,6 segundos para o *time_to_request máximo*. O fator de guarda utilizado é $f_g = 1 + 1/3$ para o caso de recepção de *Group Requests*. A Tabela 5.2 apresenta os parâmetros utilizados.

No HybSec, todas as simulações foram feitas com dois raios de ofuscações (r) de 80 metros e 160 metros. Como citado, no SafeAnon os veículos suspendem a ofuscação de

Tabela 5.2 Parâmetros de simulação.

Período de substituição do grupo	9 segundos
Período de ajuste	3 segundos
Período de remoção de redundância	3 segundos
Time_to_request máximo	0,6 segundos
Intervalo mínimo para envio de *CAM*	150 milissegundos
Intervalo máximo para envio de *CAM*	300 milissegundos
Fator de guarda padrão	1
Fator de guarda para Group Requests	1+1/3

informações ao atingirem uma distância mínima. Nas simulações, tal trabalho é analisado com duas distâncias mínimas de comunicação ofuscada (LO): 15 e 30 metros. Em Stübing, a distância entre as células (CD) define indiretamente a frequência com que os veículos criam novos grupos. Tal mecanismo foi simulado com distâncias de 1100 metros e de 1600 metros entre as bordas das células. Esse distanciamento é recomendado para evitar interferências entre os grupos, dado que os veículos continuam se movendo após entrar nas células [Stübing et al. 2011]. Segundo recomendações do trabalho, o raio das células utilizado é de 150 metros e o tempo de vida útil dos grupos é de 40 segundos.

5.3 MÉTRICAS

As métricas para avaliar o desempenho dos trabalhos comparados são: a *entropia*, o *período de rastreamento*, o *percentual de situações de colisão em potencial* e o *tempo na situação de colisão em potencial*. A *entropia* indica a dificuldade de rastreamento de um dado veículo para o atacante. O *período de rastreamento* indica o maior período contínuo que o atacante consegue rastrear um veículo. Por fim, o *percentual de situações de colisão em potencial* e o *tempo na situação de colisão em potencial* indicam os momentos em que os veículos ficam próximos entre si e sem trocarem mensagens contendo suas localizações exatas.

5.3.1 Entropia

A dificuldade de rastreamento (*entropia*) de um veículo pode ser calculada através do tamanho de seu conjunto de anonimato [Serjantov and Danezis 2003]. De modo geral, a entropia indica a quantidade de informação, em bits, que um atacante precisa para distinguir entre o veículo rastreado e os outros veículos da rede. Para isso, os veículos contidos em um mesmo conjunto de anonimato são simultaneamente indistinguíveis para um atacante global e passivo, dado que os elementos de um conjunto são considerados em distribuição uniforme.

Para que o atacante possa realizar rastreamentos deterministicamente, é necessário que ele possa distinguir o veículo alvo de todos os outros veículos da rede. Portanto, o veículo alvo precisa possuir entropia zero. Assim sendo, as entropias dos veículos indicam, de forma abstrata, o grau de dificuldade que um dado cenário oferece para que um atacante realize rastreamentos com sucesso. Desse modo, quanto menor for a entropia da rede, maior é a eficiência do atacante em realizar rastreamentos.

A entropia de um dado veículo é maior que zero apenas se a localização que o atacante obtém não possa ser deterministicamente correlacionada com o veículo alvo. Como o atacante não possui acesso às localizações exatas dos veículos em nenhum momento no HybSec, os tamanhos dos seus conjuntos de anonimato são computados apenas com base nas ofuscações. Apesar de os grupos permitirem que os veículos troquem mensagens contendo localizações exatas, tal fato é indiferente no cálculo da entropia no HybSec, visto que o atacante não obtém as informações trocadas internamente nos grupos.

Em SafeAnon, os veículos enviam mensagens ofuscadas na maior parte do tempo, contudo as localizações exatas dos veículos são enviadas caso a distância mínima de ofuscação seja atingida. Assim sendo, ao enviar uma mensagem contendo sua localização exata, o veículo emissor torna-se rastreável para um atacante global. No caso das mensagens ofuscadas, assim como no HybSec, a entropia dos veículos é maior que zero caso haja sobreposições entre as ofuscações.

Em Stübing, o atacante não obtém informações de localização dos veículos enquanto

estes pertencem a um grupo. Assim sendo, a entropia dos veículos é maior que zero enquanto estes pertencem a um grupo. Contudo, o fato de os veículos enviarem suas localizações exatas sempre que estão fora dos grupos faz com que a entropia dos veículos seja zero nesses casos, tornando-os trivialmente rastreáveis.

Naturalmente, as entropias dos veículos variam ao longo das rotas percorridas por eles. Portanto, o grau de vulnerabilidade deles também muda. Para tornar evidente as vulnerabilidades de cada mecanismo em relação ao atacante, foram considerados apenas os piores casos da *entropia* de cada veículo para obtenção do resultado dessa métrica.

5.3.1.1 Cálculo da Entropia

A amostragem da entropia da rede é realizada em intervalos fixos de 200 milissegundos de mobilidade dos veículos. Em um intervalo de amostragem, os veículos que estiverem indistinguíveis entre si são considerados em um mesmo conjunto de anonimato. Em HybSec e SafeAnon, é necessário que as áreas ofuscadas das *CAMs* enviadas pelos veículos possuam sobreposições simultâneas para que os veículos sejam considerados indistinguíveis. Por outro lado, em Stübing, os veículos precisam estar contidos em um mesmo grupo para que essa condição seja satisfeita.

Para o cálculo da entropia da rede, não são consideradas as substituições de pseudônimos realizadas pelos veículos. Dessa forma, é possível avaliar as entropias geradas especificamente por cada mecanismo comparado para dificultar os rastreamentos realizados pelo atacante.

A Equação (5.1) apresenta o cálculo da entropia $H(n)$ que é realizado para cada veículo n. A probabilidade n ser rastreado com sucesso é p_n, S_n é o conjunto de anonimato ao qual n pertence e $|S_n|$ é o tamanho de S_n. Como os veículos pertencentes a um mesmo conjunto de anonimato são considerados em distribuição uniforme, então $p_n = 1/|S_n|$.

$$H(n) = -\sum_{n=1}^{|S_n|} p_n \log_2 p_n, \text{ onde } \sum_{n=1}^{|S_n|} p_n = 1. \tag{5.1}$$

Além de n, caso nenhum outro veículo pertença ao conjunto S_n, então $H(n)$ será igual

a zero. Nesse caso, n é trivialmente rastreável por um atacante. Naturalmente, em SafeAnon a entropia é zero sempre que os veículos estiverem a uma distância inferior à distância mínima de ofuscação. Em Stübing, a entropia de um dado veículo é zero sempre que ele não pertença a nenhum grupo.

Para o resultado da métrica *entropia*, foram consideradas apenas as menores entropias de cada veículo da rede. Para isso, foi utilizado apenas as 25% entropias mais baixas de cada veículo durante a simulação. Com essa taxa de amostragem, os resultados apresentam o desempenho de cada mecanismo nos casos em que os veículos encontram-se mais vulneráveis.

A Equação (5.2) apresenta a média das entropia mais baixas dos N veículos da rede ao longo de uma simulação. O conjunto das menores entropias de um veículo n é representado por Q_n, e $q_{n,p}$ é o *p-ésimo* elemento de Q_n.

$$H(N) = \frac{\sum_{n=1}^{N} \sum_{p=1}^{|Q_n|} q_{n,p}}{|Q_1| \times N}. \tag{5.2}$$

5.3.2 Período de Rastreamento

No contexto de rastreabilidade, que é o foco desse trabalho, a métrica *período de rastreamento* apresenta-se como o principal indicador de eficiência. Essa métrica é capaz de demonstrar qual é o maior tempo que o mecanismo analisado torna os veículos vulneráveis diante de um atacante.

A captura das localizações exatas dos veículos apenas possibilita um rastreamento efetivo se essas informações forem capturadas continuamente. Por exemplo, não é relevante para um atacante realizar dois rastreamentos de um mesmo veículo com períodos de trinta segundos cada, caso esses rastreamentos sejam feitos em um intervalo de cinco minutos de diferença. Para analisar um rastreamento, é necessário verificar quanto tempo sem interrupções o atacante é capaz de conhecer o a localização de um veículo alvo. Essa necessidade decorre do fato de que os veículos realizam modificações em seus pseudônimos. Apesar de estar fora do escopo deste trabalho a definição dos momentos em que tais

pseudônimos são modificados, os padrões IEEE 1609.3 e 1609.4 [IEEE P1609.3 Working Group 2010, IEEE P1609.4 Working Group 2010] citam que os veículos precisam realizar tais modificações.

Considere que um veículo V possua o pseudônimo p_0 no instante t_0 e que possua pseudônimo p_y no instante t_y. Considere também que V seja rastreado entre os instantes t_0 e t_{y-x}, onde $y > x + 1$ e $x > 0$. Então, se V for rastreado a partir do instante t_y, o atacante não será capaz de inferir que p_0 é o mesmo veículo que p_y. Ou seja, se um veículo é rastreado em dois períodos não contínuos, o atacante não será capaz de correlacionar que o rastreamento foi realizado sobre o mesmo veículo, dado que o veículo alvo modificou seu pseudônimo. Portanto, fica clara a necessidade de se analisar a continuidade dos períodos de rastreamento dos veículos. Assim sendo, foram considerados para o cálculo da métrica *período de rastreamento* apenas os maiores períodos contínuos que cada veículo permanece rastreado.

5.3.2.1 Cálculo do Período de Rastreamento

A métrica *período de rastreamento* é calculada com base na entropia $H(n)$ dos veículos. Um veículo é considerado rastreado em um dado instante se a sua entropia for zero. Portanto, o período de rastreamento de um dado veículo (n) corresponde ao maior intervalo consecutivo que ele permanece com *entropia* igual a zero $(H(n) = 0)$ durante a simulação.

Para evidenciar as vulnerabilidades de cada mecanismo comparado, a métrica *período de rastreamento* é composta apenas pelos veículos com piores tempos de rastreamentos. Portanto, o cálculo dessa métrica é uma média aritmética entre os 25% maiores tempos de rastreamentos da rede.

5.3.2.2 Análise Demonstrativa

Como citado, os veículos em conjuntos de anonimato de tamanho 1 são rastreáveis, visto que a *entropia* gerada para o atacante é 0. Em Stübing, os veículos participam de conjun-

tos de anonimato com tamanho maior que 1 apenas enquanto pertencem a algum grupo, visto que este é o único momento que o atacante não obtém a localização dos veículos. Em todos os outros momentos, porém, o envio de mensagens contendo localizações exatas permite que os veículos sejam rastreados. Portanto, para que um veículo não possa ser rastreado em Stübing, é preciso que: (1) pelo menos dois veículos estejam próximos entre si e (2) um grupo seja formado entre as entidades. No entanto, o HybSec também garante que a *entropia* será maior que 0, caso (1) e (2) sejam verdadeiros. Portanto, o período de vulnerabilidades a rastreamentos de Stübing é maior ou igual ao período de vulnerabilidades do HybSec.

Na solução proposta em SafeAnon, o tamanho de um conjunto de anonimato é maior que 1 apenas se: (3) os veículos estiverem a uma distância superior à distância mínima de ofuscação e (4) houver sobreposição entre as localizações ofuscadas de tais veículos. Porém, o HybSec garante que os tamanhos dos conjuntos de anonimato serão maiores que 1, caso (3) e (4) sejam verdadeiros. Portanto, o período de vulnerabilidades a rastreamentos de SafeAnon também é maior ou igual ao período de vulnerabilidades do HybSec.

5.3.3 Colisões em Potencial

Para garantir segurança física aos usuários, é necessário que qualquer mecanismo utilizado nas VANETs minimize as situações de risco de colisão entre veículos. Visando medir o grau de segurança provido pelos mecanismos comparados, as métricas de *colisões em potencial* são definidas.

As métricas de *percentual de situações de colisão em potencial* e *tempo na situação de colisão em potencial* são indicadores complementares para medir as situações de colisão em potencial. Uma *colisão em potencial*, por sua vez, é uma situação onde os veículos não identificam que estão em risco de colisão. Portanto, através dessas métricas, é possível verificar se o mecanismo proposto se adequa às aplicações de segurança no trânsito.

Cada trabalho analisado difere no contexto que as mensagens contendo as localizações

exatas são enviadas. Em HybSec, tais mensagens são cifradas e enviadas apenas através grupos criptográficos. Em SafeAnon, o envio é feito em claro na rede, desde haja proximidade entre os veículos. Em Stübing, o envio é feito em claro enquanto os veículos não pertencem aos grupos e cifrado enquanto pertencem. Contudo, independentemente do método utilizado, essa métrica analisa se tais mensagens são trocadas nos momentos adequados.

5.3.3.1 Cálculo das Colisões em Potencial

O *percentual de situações de colisão em potencial* e o *tempo na situação de colisão em potencial* indicam, respectivamente, a frequência e o tempo que os veículos ficam em situações de *colisão em potencial*. Dois veículos são considerados em uma situação de *colisão em potencial* se eles estiverem a uma *distância de risco* e sem trocar informações exatas de localização.

Nas simulações, a *distância de risco* utilizada é de 50 metros ou menos. Considere que os veículos não excedem a velocidade de 60 km/h (∼16,7 m/s) em ambientes urbanos e que os veículos estejam distanciados de 50 metros, conforme a *distância de risco* utilizada. Naturalmente, o pior caso de aproximação entre as entidades é quando dois veículos se movem em sentidos opostos de uma mesma rodovia. Nesse caso, tais veículos desempenham uma velocidade relativa máxima de 120 km/h (33,3 m/s). Através dessa velocidade relativa, os motoristas teriam 1,5 segundos para realizarem uma ação que evitasse a colisão, caso eles apenas percebam que há uma situação de risco após o alerta dos veículos. De acordo com o estudo apresentado em [Drews et al. 2009], o intervalo de 1,5 segundos é o mínimo suficiente para que a grande maioria dos motoristas, independente da faixa etária, reajam diante uma situação de risco. Desse modo, foi adotada a distância de 50 metros como o limiar para a *distância de risco* nas simulações.

No cálculo do *percentual de situações de colisão em potencial*, $Cp(n)$ indica a quantidade de *CAMs* recebidas pelo veículo n, dado que n estava em uma *colisão em potencial* com o emissor no momento do recebimento. Além disso, $Tr(n)$ é o total de *CAMs* re-

cebidas por n e que foram enviadas por veículos em *distância de risco* em relação a n. Considerando uma rede composta por N veículos, o *percentual de situações de colisão em potencial* ($P_{cp}(N)$) pode ser calculado através da Equação (5.3) a seguir:

$$P_{cp}(N) = \frac{\sum_{n=1}^{N} Cp(n)}{Tr(n)}. \tag{5.3}$$

De forma complementar, o *tempo na situação de colisão em potencial* é uma média dos tempos que os veículos permanecem em situações de *colisão em potencial*. Para isso, é calculada a razão entre os períodos contínuos de tempo que os veículos permanecem em uma *colisão em potencial* e o número de vezes que tais situações ocorrem. Ressalta-se que os cálculos das métricas de *colisões em potencial* consideram 100% das amostras obtidas ao longo da simulação, diferente das métricas *entropia* e *período de rastreamento*.

5.4 VALIDAÇÕES

As implementações dos mecanismos Stübing e SafeAnon foram validadas com os resultados dos trabalhos originais. Foram utilizados os cenários e parâmetros descritos em tais trabalhos para replicar os resultados obtidos neles. Nas validações, cada cenário foi simulado cem vezes e os resultados foram apresentados com intervalo de confiança de 99%. A mobilidade dos veículos foi gerada pelo VanetMobiSim.

Os trabalhos comparados não descrevem detalhadamente os parâmetros utilizados na geração de mobilidade. Parâmetros como a velocidade máxima, o tempo de segurança ou os detalhes do mapa das rodovias não são apresentados. Assim sendo, foram utilizados os parâmetros apresentados na Tabela 5.1. Portanto, é natural que ocorram diferenças entre os registros do VanetMobiSim neste trabalho e os registros dos geradores de mobilidade dos trabalhos relacionados. Contudo, essas diferenças geram pouco impacto nas validações realizadas.

5.4.1 Validação de Stübing

Em Stübing foi realizada uma análise do percentual de veículos que permanecem rastreáveis durante um intervalo de um minuto. Ou seja, mede-se o tempo contínuo que o atacante consegue permanecer rastreando cada veículo da rede a partir do início das simulações. Em tal trabalho, a simulação é feita apenas em uma única rodovia em linha reta, sem sinais de trânsito, e com todos os veículos se movimentando no mesmo sentido. Deste modo, os veículos não sofrem de diversas situações que impactam as simulações que utilizam mapas de rodovias, por exemplo: a troca de mensagens em cruzamentos, a comunicação com veículos localizados em ruas paralelas e a saída de veículos dos grupos devido às curvas nas pistas. Além disso, em um cenário com uma única rodovia, garante-se que os veículos sempre passarão pelos locais das células de formação dos grupos, diferente de um mapa de rodovias.

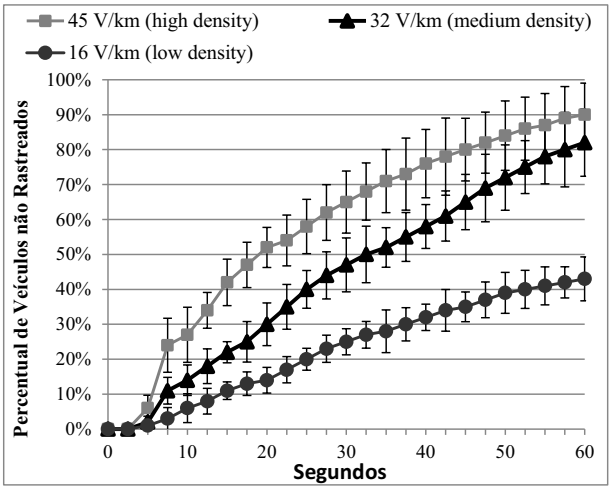

Figura 5.2 Validação do percentual de rastreamentos em Stübing.

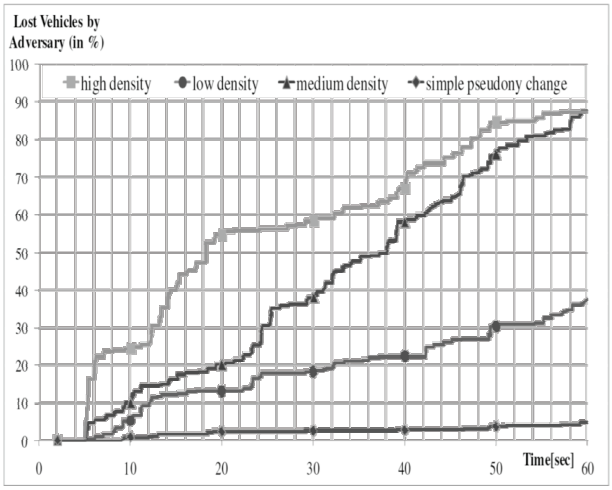

Figura 5.3 Percentual de rastreamentos em Stübing. Fonte: [Stübing et al. 2011].

A Figura 5.2 apresenta a validação da simulação feita em Stübing, apresentada na Figura 5.3. As curvas relativas ao mecanismo proposto em Stübing estão legendadas como *high density*, *medium density* e *low density*. Essas três curvas são relativas aos cenários, com 45 veículos/km, 32 veículos/km e 16 veículos/km, respectivamente.

5.4.2 Validação de SafeAnon

Em SafeAnon foi medida a entropia média dos veículos na rede. Destaca-se, diferentemente da fórmula de cálculo da entropia descrita na Seção 5.3.1.1, a validação do SafeAnon não utilizou apenas as menores entropias dos veículos para obtenção dos resultados dessa métrica. Porém, foi realizada a média de todas as amostras de entropias feitas ao longo da simulação, conforme realizado em tal trabalho.

Como citado na Seção 5.3.1.1, os veículos precisam ser indistinguíveis a um atacante para que possam ser considerados em um mesmo conjunto de anonimato. Contudo, em SafeAnon, considera-se que se não houverem veículos contidos dentro do raio de ofuscação de uma entidade, então tal entidade pertence a um conjunto de anonimato composto por todos os veículos dentro de seu raio de alcance de transmissão de mensagens. Deste modo, o conjunto de anonimato de um veículo distante das outras entidades pode ter tamanho superior a 1. Apesar de essa consideração não refletir a dificuldade real de rastreamento gerada para um atacante, foi utilizado o mesmo cálculo de entropia definido em SafeAnon para fins de validação.

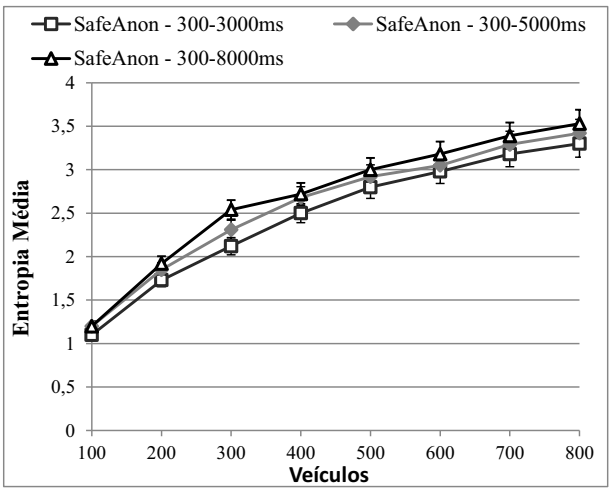

Figura 5.4 Validação da entropia média da rede em SafeAnon.

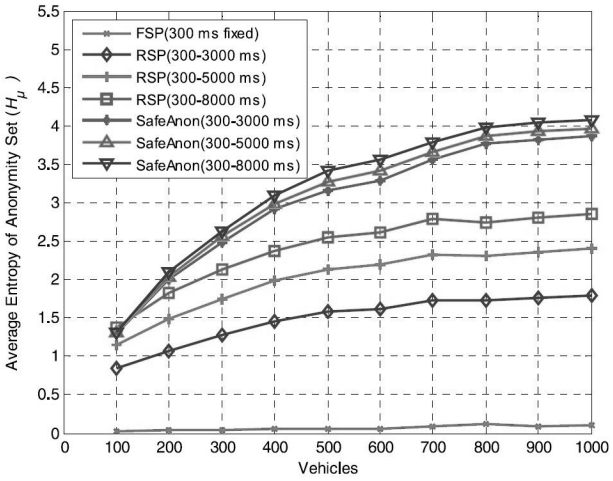

Figura 5.5 Entropia média da rede em SafeAnon. Fonte: [Chen and Wei 2012].

Na geração de mobilidade de SafeAnon é utilizado um mapa da região de Manhattan-NY. A Figura 5.4 apresenta a validação da simulação feita em SafeAnon, apresentada

na Figura 5.5. As curvas relativas ao SafeAnon estão legendadas como *SafeAnon (300-3000 ms)*, *SafeAnon (300-5000 ms)* e *SafeAnon (300-8000 ms)*. Como o trabalho utiliza períodos de silêncio aleatório (Seção 3.2), os períodos citados entre parênteses nas legendas representam o mínimo e o máximo de tempo que os veículos permanecem sem enviar *CAMs* durante os períodos de silêncio aleatório. Nas validações realizadas (Figura 5.4) foram simuladas redes de até 800 veículos, enquanto que no SafeAnon (Figura 5.5) é apresentado um cenário de até 1000 veículos.

5.4.3 Considerações sobre as Validações

Como apresentado nas Figuras, os gráficos de validação de ambos os trabalhos apresentam-se significativamente semelhantes aos gráficos originais. Ressalta-se que ambos os trabalhos relacionados não utilizam intervalo de confiança nos gráficos, de modo que os resultados apresentados neles tornam-se estimados.

5.5 RESULTADOS

A seguir são apresentados os resultados de cada uma das métricas avaliadas. Nos gráficos, a distância entre as células em Stübing é identificada por CD, a distância mínima de comunicação ofuscada em SafeAnon é identificada por LO e o raio de ofuscação em HybSec é identificado por r. As taxas de perda de mensagens são indicadas nas legendas de cada figura através da sigla Tp.

5.5.1 Entropia

As Figuras 5.6, 5.7 e 5.8 apresentam as entropias dos mecanismos comparados para as taxas de perda de 2%, 8% e 16%, respectivamente. Percebe-se que os resultados de Stübing são iguais a zero em todos os cenários avaliados. Em tal trabalho, os veículos ficam com entropia zero caso eles não pertençam a nenhum grupo, visto que não há indistinguibilidade para o atacante nesses casos. Como os gráficos apresentam o resultado

das 25% menores entropias, e todos os veículo em Stübing permanecerem fora dos grupos em mais de 25% de seu tempo de mobilidade, então o resultado da métrica *entropia* torna-se zero.

O resultado no Hybsec foi superior aos trabalhos relacionados em todos os cenários. Nele, os aumentos do raio de ofuscação e da densidade de veículos da rede impactam positivamente na elevação da entropia. Isso ocorre porque a elevação de ambos os fatores geram um maior número de sobreposições entre as ofuscações, ocasionando em maiores conjuntos de anonimato e, consequentemente, maiores entropias. Em HybSec, a *entropia* varia entre 0,26 e 1,38, considerando todos os cenários avaliados.

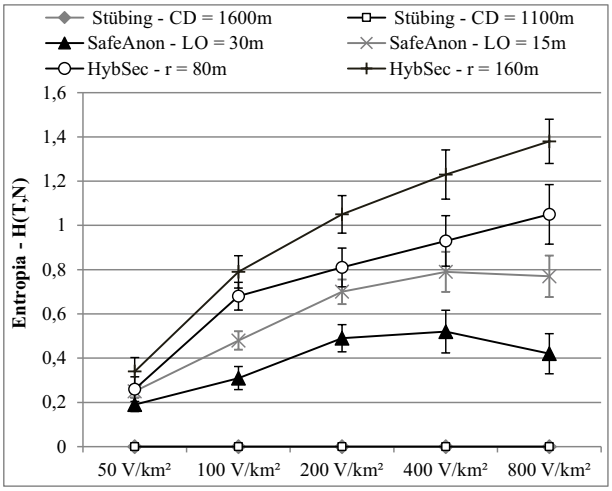

Figura 5.6 Entropia. Tp = 2%.

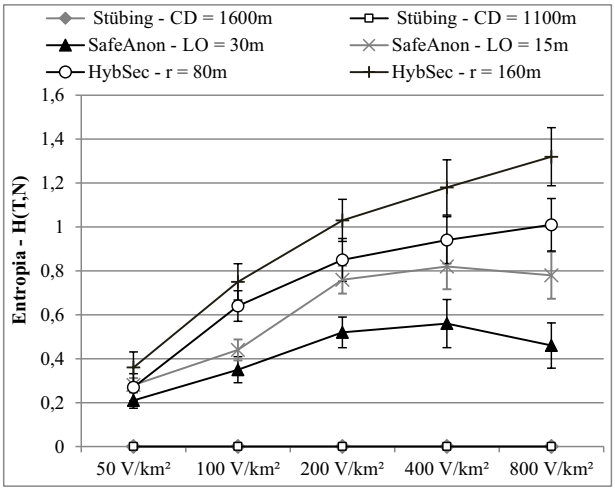

Figura 5.7 Entropia. Tp = 8%.

As sobreposições de ofuscações no SafeAnon também são responsáveis pela entropia da rede. Tal mecanismo, porém, possui desvantagens em cenários de congestionamento intenso, como em redes de 800 veículos/km^2. Como os veículos tendem a ficar muito próximos entre si em rodovias congestionada, isso ocasiona na redução e eliminação das ofuscações realizada pelo SafeAnon. Desse modo, há uma queda na entropia do mecanismo em redes densas. Naturalmente, o limiar de ofuscação (LO) de 15 metros garante uma maior entropia em relação ao LO de 30 metros, visto que os veículos precisam estar mais próximos para que as ofuscações de mensagens sejam eliminadas. Deste modo, os veículos permanecem por mais tempo em conjuntos de anonimato com tamanhos supe-

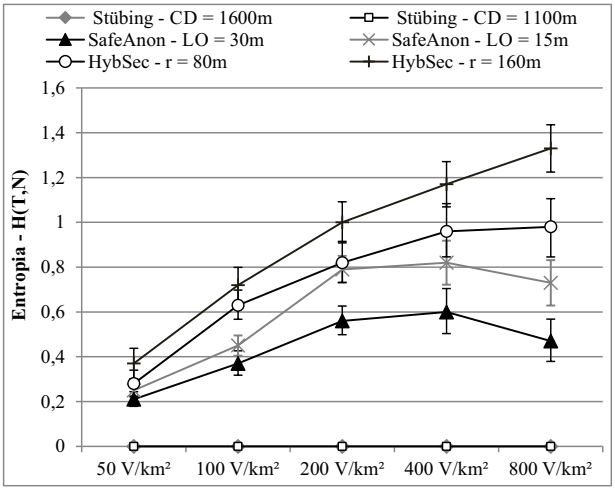

Figura 5.8 Entropia. Tp = 16%.

riores a um. O resultado da entropia em SafeAnon varia entre 0,19 e 0,82, considerando todos os cenários avaliados.

5.5.2 Período de Rastreamento

As Figuras 5.9, 5.10 e 5.11 apresentam os resultados do período de rastreamento em cada proposta para as taxas de perda de 2%, 8% e 16%, respectivamente. Assim como na entropia, os períodos de rastreamentos em HybSec e SafeAnon são pouco afetados pela taxa de perda de mensagens. Em Stübing, contudo, são gerados atrasos no processo de formação dos grupos devido às mensagens perdidas na definição colaborativa das chaves. Nesse caso, os veículos atrasam o ingresso nos grupos, aumentando o período de vulnerabilidade.

O HybSec apresenta um período de rastreamento inferior aos trabalhos relacionados em todos os cenários. Os gráficos apresentados comprovam a análise feita na Seção 5.3.2.2, demonstrando que os períodos máximos de rastreamento de Stübing e SafeAnon são sempre maiores que na solução proposta neste trabalho.

O período de rastreamento do HybSec varia entre 2 e 34,9 segundos, dependendo do raio de ofuscação utilizado, da taxa de perda de mensagens e da densidade da rede. Nos cenários com 400 e 800 veículos/km^2, e raio de ofuscação de 160 metros, os resultados são

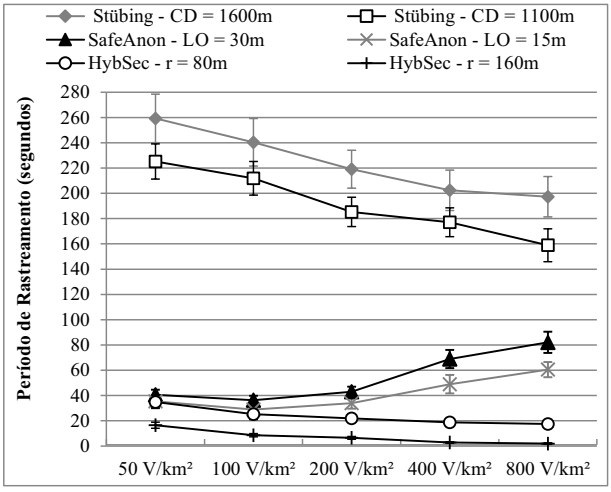

Figura 5.9 Período de rastreamento. Tp = 2%.

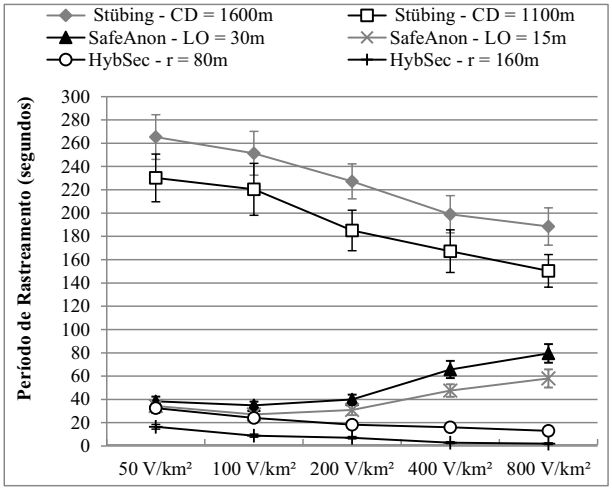

Figura 5.10 Período de rastreamento. Tp = 8%.

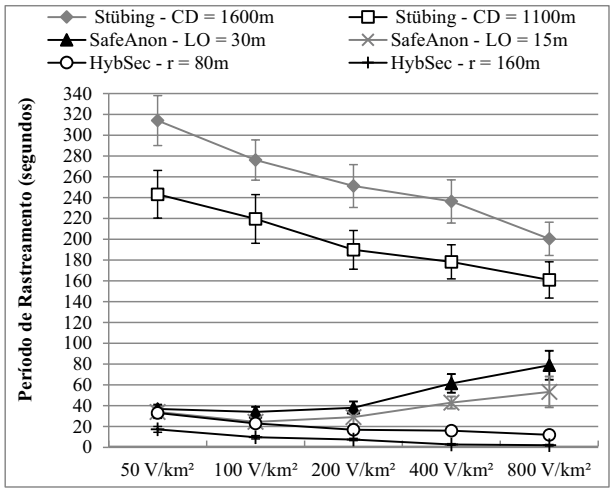

Figura 5.11 Período de rastreamento. Tp = 16%.

sempre inferiores a 3 segundos, demonstrando a maior eficiência do mecanismo em redes com densidades média e alta. Naturalmente, em redes com baixa densidade, os veículos trafegam longas distâncias sem se aproximarem de outros veículos. Nesse caso, há poucas sobreposições entre áreas de ofuscação, tornando-os mais vulneráveis a rastreamentos.

Não há grandes diferenças entre os resultados do HybSec e do SafeAnon nos cenários de redes pouco densas. Contudo, há uma sensível piora nos resultados do SafeAnon nas redes com densidades médias e altas. Diferentemente do HybSec, em que os resultados

são melhores à medida que a rede fica mais densa, em SafeAnon os resultados tornam-se piores. Em SafeAnon, o *período de rastreamento* tem seu melhor resultado igual a 29 segundos e pior resultado igual a 82,1 segundos, considerando todos os cenários avaliados. Como esperado, os veículos tendem a ficar muito próximos entre si em redes densas, de modo que a ofuscação é eliminada no SafeAnon. Em tal trabalho, a diminuição do limiar de ofuscação (LO) permite a redução dos períodos de rastreamento, pois os veículos trocam localizações exatas apenas quando estão mais próximos entre si.

Em Stübing, o *período de rastreamento* é significativamente superior ao HybSec e ao SafeAnon. Em tal trabalho, esse resultado negativo é decorrente de os veículos apenas protegerem suas localizações enquanto pertencem aos grupos. Os resultados obtidos variam entre 150,4 e 314,2 segundos, considerando todos os cenários avaliados.

5.5.3 Colisões em Potencial

As Figuras 5.12, 5.13 e 5.14 apresentam os *percentuais de colisões em potencial* para as taxas de perda de 2%, 8% e 16%, respectivamente. Como resultado complementar, as Figuras 5.18, 5.19 e 5.20 apresentam os *tempos de colisões em potencial*. Em tais métricas, os resultados do HybSec e Stübing são significativamente próximos entre si, enquanto que o SafeAnon apresenta resultados notoriamente piores.

Em todas as abordagens, o aumento da taxa de perda de mensagens impactou na elevação do percentual e tempo na situação de colisão em potencial. No HybSec, a perda de mensagens ofuscadas eleva as situações em que os veículos não percebem as situações de risco, postergando a comunicação através grupos. De modo semelhante, a perda de mensagens ofuscadas em SafeAnon atrasa a detecção de risco e a eliminação da comunicação ofuscada. Em Stübing, como não há troca de mensagens ofuscadas, esse problema de atraso na percepção das situações de risco ocorre com menos frequência que no HybSec e SafeAnon. Contudo, o cálculo das chaves de grupos em Stübing depende de que cada veículo do grupo envie um fragmento de chave para todos os outros. Portanto, a perda de mensagens nesse momento gera atrasos na formação inicial dos grupos e eleva

as situações de colisão em potencial.

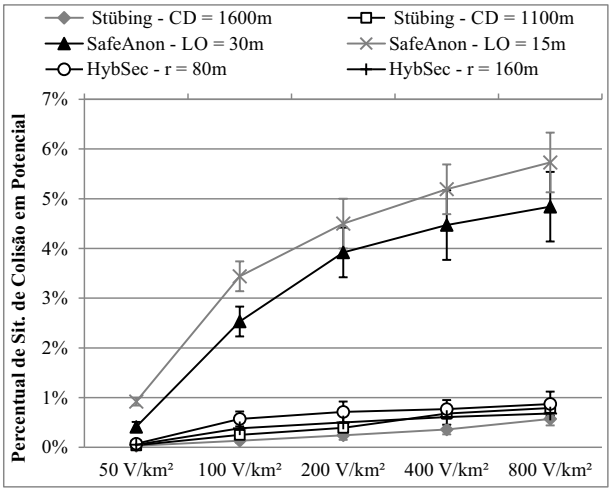

Figura 5.12 Percentual de situações de colisão em potencial. Tp = 2%.

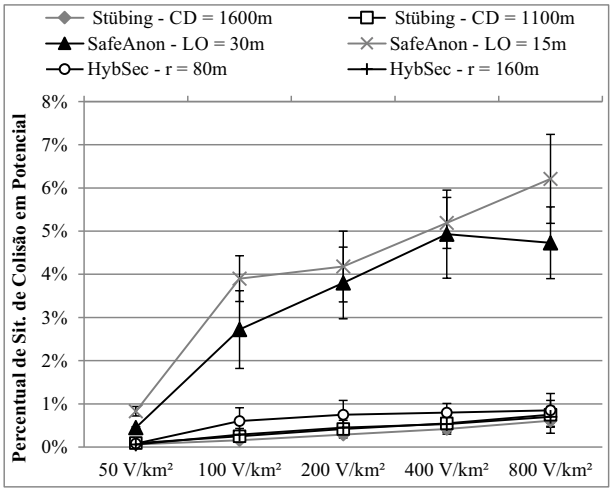

Figura 5.13 Percentual de situações de colisão em potencial. Tp = 8%.

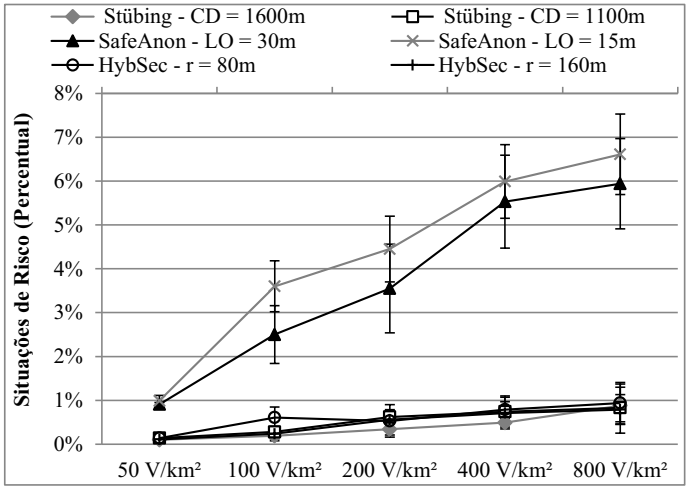

Figura 5.14 Percentual de situações de colisão em potencial. Tp = 16%.

Em SafeAnon, os veículos ficam em colisão em potencial se estiverem na distância de risco (50 metros ou menos) e continuarem informando localizações ofuscadas entre si. Portanto, o limiar de ofuscação (LO) influencia no período que os veículos permanecem em potencial de colisão após eles entrarem na região de *distância de risco*. Como apresentado nos gráficos, o LO de 30 metros apresenta um resultado superior ao LO de 15 metros.

Contudo, em ambos os casos, o SafeAnon apresenta resultados piores que nas outras abordagens. O percentual de situações de colisão em potencial no SafeAnon varia entre 0,41% e 6,6%, considerando todos os cenários avaliados.

Dada a dificuldade de comparação entre os resultados de HybSec e de Stübing devido à proximidade de suas curvas, as Figuras 5.15, 5.16 e 5.17 apresentam os percentuais de colisões em potencial apenas dessas duas abordagens para as taxas de perda de 2%, 8% e 16%, respectivamente.

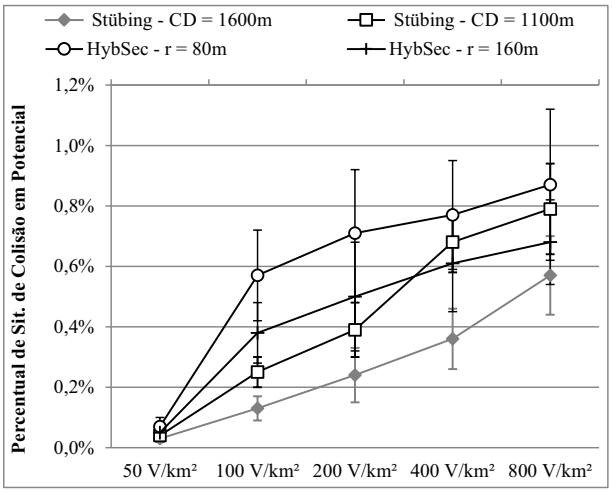

Figura 5.15 Percentual de situações de colisão em potencial de HybSec e Stübing. Tp = 2%.

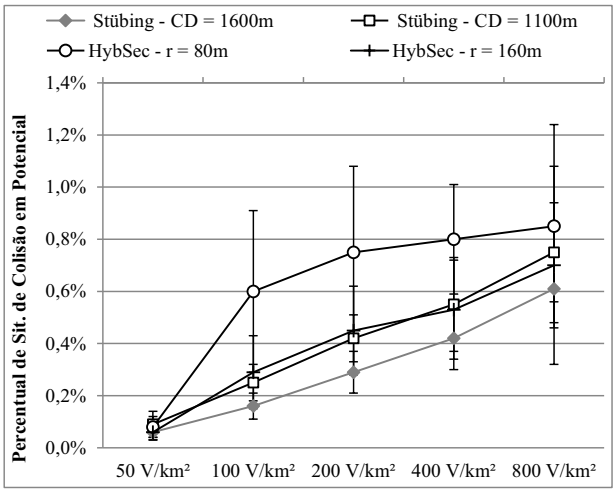

Figura 5.16 Percentual de situações de colisão em potencial de HybSec e Stübing. Tp = 8%.

Na maior parte dos cenários, o percentual de situações de colisão em potencial em Stübing é um pouco inferior ao resultado em HybSec. Porém, há cenários onde o resultado do HybSec é inferior e, além disso, há sobreposições entre os intervalos de confiança dos resultados dos dois mecanismos. Portanto, tais abordagens podem ser consideradas equivalentes nessa métrica. Os pontos médios dos intervalos de confiança de ambas as propostas sempre é inferior a 1%, considerando todos os cenários avaliados, evidenciando a baixa frequência com que os veículos ficam em risco.

Os resultados dos tempos de colisões em potencial são complementares aos resultados dos percentuais de colisões em potencial. No SafeAnon, esses tempos variam entre 1,3

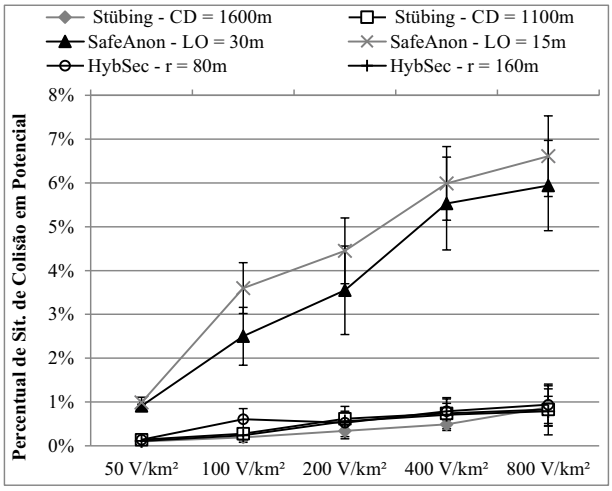

Figura 5.17 Percentual de situações de colisão em potencial de HybSec e Stübing. Tp = 16%.

e 4,5 segundos, sendo significantemente maior que nas outras abordagens. Além disso, percebe-se um expressivo aumento desse tempo nas redes com maior densidade de veículos em tal mecanismo. Em HybSec e Stübing, todos os resultados são inferiores a 0,8 segundo, mesmo em redes com alta densidade de veículos e taxa de perda de mensagens elevada.

Assim como na métrica *percentual de situações de colisão em potencial*, as Figuras 5.21, 5.22 e 5.23 apresentam uma comparação apenas entre os *tempos de colisões em potencial* de HybSec e Stübing para as taxas de perda de 2%, 8% e 16%, respectivamente. Destaca-se a proximidade entre os resultados das duas abordagens nessa métrica.

Como apresentado, o tempo médio de colisões em potencial é inferior a 0,8 segundos no HybSec. Portanto, os veículos permanecem sem o auxílio dos grupos para indicar potenciais riscos de colisão apenas em curtos intervalos de tempo. Ressalta-se que essas situações ocorrem em menos de 1% dos momentos que os veículos precisam se comunicar em grupos, segundo os resultados do *percentual de situações de colisão em potencial*.

5.5.4 Considerações sobre Consumo de Banda

Neste trabalho, não foram realizadas análises detalhadas sobre o consumo de banda dos mecanismos comparados. Porém, devido à troca de mensagens entre os veículos para formação e término dos grupos no HybSec, é natural esse mecanismo possua maior con-

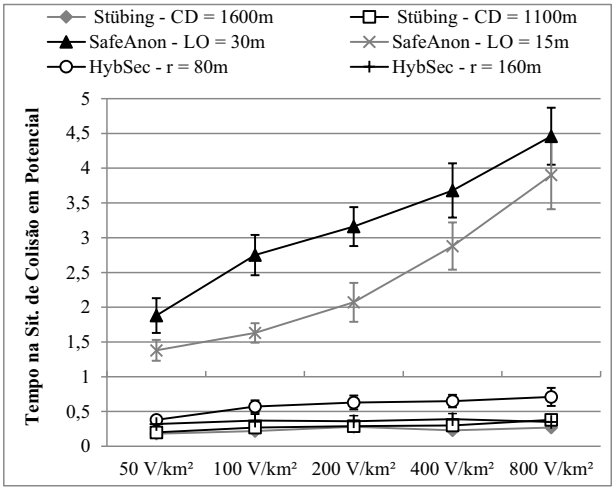

Figura 5.18 Tempo na situação de colisão em potencial. Tp = 2%.

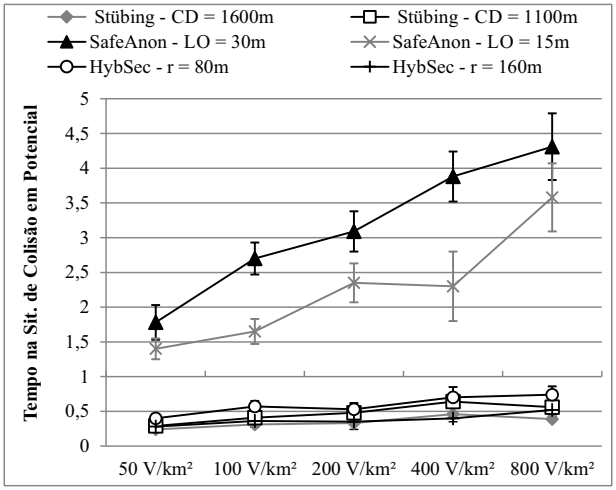

Figura 5.19 Tempo na situação de colisão em potencial. Tp = 8%.

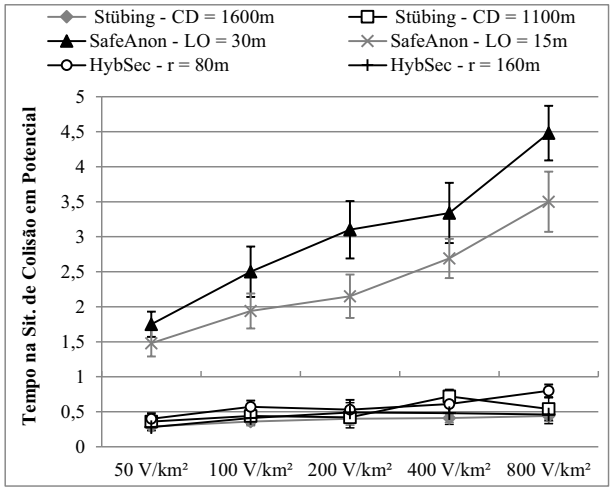

Figura 5.20 Tempo na situação de colisão em potencial. Tp = 16%.

sumo em relação aos trabalhos relacionados. Diferentemente do HybSec, a formação de grupos em Stübing ocorre com menor frequência, dado que esse processo é realizado apenas se os veículos estiverem presentes em uma célula. Portanto, são trocadas uma menor quantidade de mensagens de formação de grupos em relação ao HybSec. Em SafeAnon, por sua vez, não há comunicação em grupos e, além disso, os veículos precisam apenas enviar *CAMs* para o funcionamento do mecanismo.

Em todos os trabalhos, a maior parte das mensagens trocadas na rede são *CAMs*. Isso

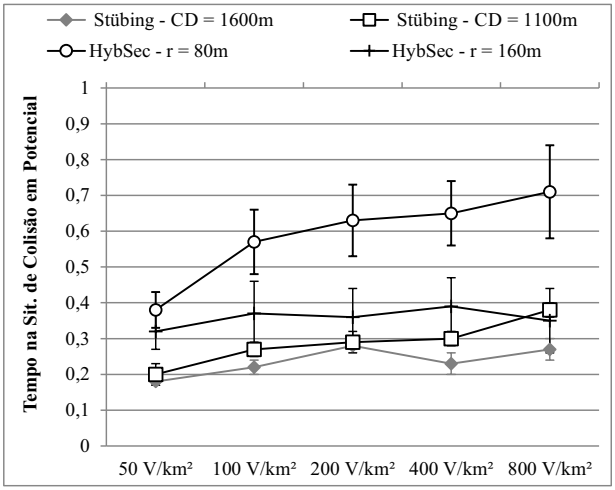

Figura 5.21 Tempo médio de colisões em potencial de HybSec e Stübing. Tp = 2%.

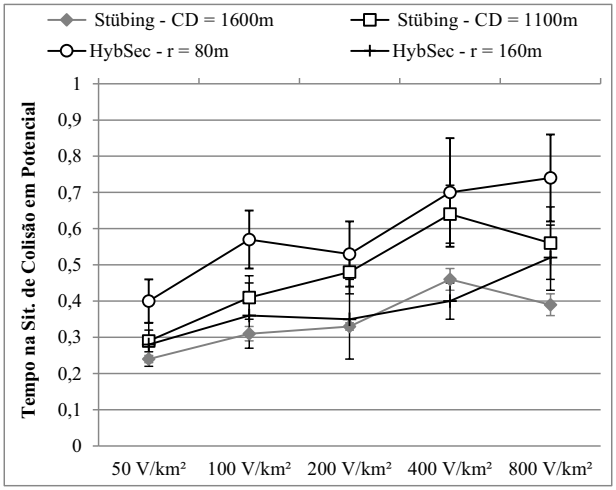

Figura 5.22 Tempo médio de colisões em potencial de HybSec e Stübing. Tp = 8%.

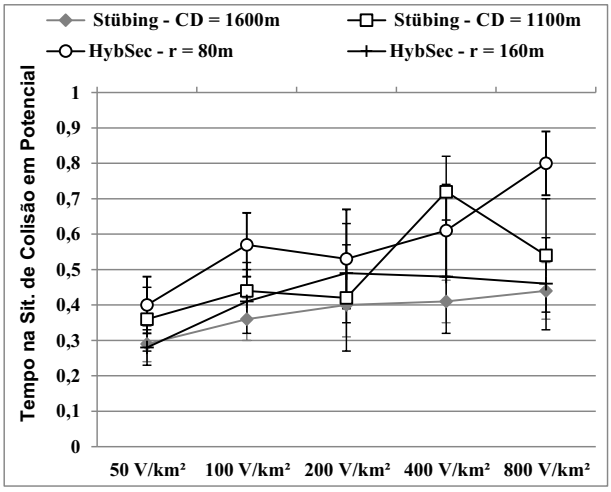

Figura 5.23 Tempo médio de colisões em potencial de HybSec e Stübing. Tp = 16%.

ocorre devido à alta frequência de envio dessas mensagens, dado que elas são enviadas, aproximadamente, a cada 200 milissegundos por cada veículo, segundo as recomendações da família de padrões IEEE 1609. Assim sendo, apesar de o HybSec necessitar de uma maior troca de mensagens devido à frequente formação de grupos, a maioria dessas mensagens são *CAMs* e independem do mecanismo utilizado.

RESUMO

Os resultados do HybSec foram analisados em comparação com as soluções propostas em Stübing e SafeAnon. Os registros das movimentações dos veículos são gerados pelo simulador VanetMobiSim. As métricas utilizadas para avaliar o desempenho dos trabalhos comparados são: a *entropia*, o *período de rastreamento*, o *percentual de situações de colisão em potencial* e o *tempo na situação de colisão em potencial*.

Nos resultados das simulações, a taxa de perda de mensagens gera poucos impactos na *entropia* e no *período de rastreamento* em HybSec e SafeAnon. Em Stübing, contudo, há uma sensível piora em ambas as métricas devido à perda de mensagens. Nas métricas de colisão em potencial, todos os trabalhos são afetados negativamente pelo aumento na perda de mensagens. Porém, mesmo com a piora dos resultados, no HybSec e SafeAnon não são criadas situações onde os veículos permanecem longos períodos em uma colisão em potencial.

O resultado da *entropia* do HybSec é superior aos trabalhos relacionados em todos os cenários. Na solução proposta, o aumento na densidade de veículos impacta positivamente na elevação da entropia, enquanto que SafeAnon há uma piora nos resultados dessa métrica. Em Stübing foi obtida a menor entropia dentre os trabalhos comparados, visto que os veículos ficam fora dos grupos na maior parte do tempo.

No contexto de rastreabilidade, que é o foco desse trabalho, a métrica *período de rastreamento* apresenta-se como o principal indicador de eficiência. Nessa métrica, o HybSec apresenta melhores resultados em relação aos trabalhos relacionados em todos os cenários.

Nas métricas de *percentual de colisões em potencial* e *tempo na situação de colisão em potencial*, os resultados do HybSec e Stübing são significativamente próximos entre si, enquanto que o SafeAnon apresenta resultados notoriamente piores. Em HybSec e Stübing, o tempo na situação de colisão em potencial é inferior a 0,8 segundos em todos os cenários. Além disso, as situações de colisões em potencial ocorrem em menos de 1% dos momentos que os veículos precisam trocar suas localizações exatas.

CAPÍTULO 6

CONSIDERAÇÕES FINAIS

Existem diversas propostas para mitigar os problemas de rastreamentos em VANETs. As principais dessas propostas, apresentadas em Stübing [Stübing et al. 2011] e SafeAnon [Chen and Wei 2012], utilizam respectivamente abordagens baseadas em grupos criptográficos ou ofuscação de localizações. Contudo, isoladamente essas abordagens possuem vulnerabilidades que permitem que os veículos sejam rastreados em alguns contextos.

A solução proposta neste trabalho, denominada HybSec, impede o acesso indevido às localizações exatas dos veículos e, com isso, evita a possibilidade de rastreamentos serem realizados por entidades maliciosas. O objetivo geral do trabalho foi atingido ao serem explorados simultaneamente no HybSec os benefícios das abordagens de grupos criptográficos e ofuscação para minimizar o tempo máximo de rastreamentos dos veículos.

No HybSec foi utilizada a ofuscação de localizações para que os veículos não informem suas localizações exatas, mas apenas uma região onde eles se encontram. Contudo, os veículos em proximidade nas VANETs precisam trocar mensagens contendo suas localizações exatas para atender às aplicações de segurança no trânsito. Dada essa necessidade, o HybSec propõe que apenas os veículos próximos entre si estabeleçam grupos criptográficos para informar suas localizações exatas.

Em todos os cenários, os resultados da *entropia* e *período de rastreamento* do HybSec são melhores que nos trabalhos relacionados, indicando a maior dificuldade de um atacante realizar rastreamentos. A permanência dos veículos em situações de colisão em potencial também foi analisada. Essa análise permitiu verificar a frequência com que os veículos não detectam, erroneamente, um risco de colisão. Os mecanismos HybSec e Stübing apresentam uma baixa frequência com que os veículos permanecem nessas situações. Portanto, além de o HybSec garantir uma maior segurança contra rastreamentos,

a solução também mantém a capacidade dos veículos detectarem riscos de colisão.

A característica de autogerenciamento do HybSec é um motivador para a implantação dessa solução em redes reais, dado que a independência de intervenção da infraestrutura reduz os custos de implantação. Outro fator relevante para a sua implantação é que a solução se adequa às principais aplicações propostas para as VANETs, como segurança no trânsito e monitoração colaborativa.

Como trabalhos futuros, podem ser listados os seguintes pontos:

- Implementar o HybSec em um simulador que considere interferências do meio de comunicação e colisões entre mensagens. Em seguida, verificar os impactos desses fatores nos processos de formação e substituição de grupos.

- Realizar uma análise comparativa sobre o consumo de processamento e banda do HybSec em relação aos trabalhos relacionados.

- Desenvolver um algoritmo para definição dinâmica dos raios de ofuscação, visando maximizar a entropia e as detecções de riscos, porém evitando o ingresso dos veículos em grupos desnecessários.

Este trabalho gerou uma publicação no 31º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, promovido pela Sociedade Brasileira de Computação e realizado em Maio de 2013 [Souza and Gonçalves 2013].

REFERÊNCIAS BIBLIOGRÁFICAS

[Alomair et al. 2012] Alomair, B., Clark, A., Cuellar, J., and Poovendran, R. (2012). Scalable RFID Systems: A Privacy-Preserving Protocol with Constant-Time Identification. *IEEE Transactions on Parallel and Distributed Systems*, 23(8):84–90.

[Ardagna et al. 2011] Ardagna, C. A., Cremonini, M., di Vimercati, S. D. C., and Samarati, P. (2011). An Obfuscation-Based Approach for Protecting Location Privacy. *IEEE Transactions on Dependable and Secure Computing*, 8(1):13–27.

[Bai et al. 2010] Bai, F., Stancil, D. D., and Krishna, H. (2010). Toward Understanding Characteristics of Dedicated Short Range Communications (DSRC) From a Perspective of Vehicular Network Engineers. In *Proceedings of the International Conference on Mobile computing and networking (MobiCom)*, pages 329–340, New York, NY, USA.

[Chaum 1981] Chaum, D. L. (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, 24(2):84–90.

[Chen and Wei 2012] Chen, Y.-M. and Wei, Y.-C. (2012). SafeAnon: a Safe Location Privacy Scheme for Vehicular Networks. *Telecommunication Systems*, 50(4):339–354.

[Drews et al. 2009] Drews, F. A., Yazdani, H., Godfrey, C. N., Cooper, J. M., and Strayer, D. L. (2009). Text Messaging During Simulated Driving. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 51(5):762–770.

[Freudiger et al. 2007] Freudiger, J., Raya, M., Félegyházi, M., Papadimitratos, P., and Hubaux, J.-P. (2007). Mix-Zones for Location Privacy in Vehicular Networks. In

Proceedings of ACM Workshop on Wireless Networking for Intelligent Transportation System, Vancouver, Canada.

[Härri et al. 2007] Härri, J., Fiore, M., Filali, F., and Bonnet, C. (2007). Vehicular Mobility Simulation for VANETs. In *Proceedings of IEEE Annual Simulation Symposium*, pages 301–309, Norfolk, VA, USA.

[Hartenstein and Laberteaux 2008] Hartenstein, H. and Laberteaux, K. P. (2008). A Tutorial Survey on Vehicular Ad Hoc Networks. *IEEE Communications Magazine*, 46(8):164–171.

[IEEE 802.11p Task Group 2010] IEEE 802.11p Task Group (2010). IEEE Standard for Information technology – Telecommunications and information exchange between systems – 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 P1609.1 Working Group 2006] IEEE P1609.1 Working Group (2006). IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager.

[IEEE P1609.2 Working Group 2006] IEEE P1609.2 Working Group (2006). IEEE Trial-Use Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages.

[IEEE P1609.3 Working Group 2010] IEEE P1609.3 Working Group (2010). IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services.

[IEEE P1609.4 Working Group 2010] IEEE P1609.4 Working Group (2010). IEEE Standard for Wireless Access in Vehicular Environments (WAVE)– Multi-channel Operation.

[Lu et al. 2012] Lu, R., Lin, X., Luan, T. H., Liang, X., and Shen, X. (2012). Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs. *IEEE Transactions on Vehicular Technology*, 61(1):41–53.

[Ma 2010] Ma, Z. (2010). *Location Privacy in Vehicular Communication Systems: a Measurement Approach*. PhD thesis, University of Ulm.

[Menezes et al. 1996] Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press. ISBN 0-8493-8523-7.

[Narayanan and Shmatikov 2006] Narayanan, A. and Shmatikov, V. (2006). Obfuscated Databases and Group Privacy. In *Proceedings of ACM Conference on Computer and Communications Security (CCS)*, pages 102–111, New York, NY, USA.

[Pan and Li 2012] Pan, Y. and Li, J. (2012). An Analysis of Anonymity for Cooperative Pseudonym Change Scheme in One-dimensional VANETs. In *Proceedings of IEEE International Conference on Computer Supported Cooperative Work in Design*, pages 251–257.

[Peng et al. 2011] Peng, H., Lu, S., Li, J., Zhang, A., and Zhao, D. (2011). An Anonymity Scheme Based on Pseudonym in P2P Networks. *Forensics in Telecommunications, Information, and Multimedia*, 56:287–293.

[Quercia et al. 2011] Quercia, D., Leontiadis, I., McNamara, L., Mascolo, C., and Crowcroft, J. (2011). SpotME If You Can: Randomized Responses for Location Obfuscation on Mobile Phones. In *Proceedings of International Conference on Distributed Computing Systems (ICDCS)*, pages 102–111, Minneapolis, MN, USA.

[Sampigethaya et al. 2005] Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., and Sezaki, K. (2005). CARAVAN: Providing Location Privacy for VANET. In *Proceedings of Embedded Security in Cars (ESCAR)*.

[Sampigethaya et al. 2007] Sampigethaya, K., Li, M., Huang, L., and Poovendran, R. (2007). AMOEBA: Robust Location Privacy Scheme for VANET. *IEEE Journal on Selected Areas in Communications*, 25:1569–1589.

[Serjantov and Danezis 2003] Serjantov, A. and Danezis, G. (2003). Towards an information theoretic metricfor anonymity. *Lecture Notes in Computer Science*, 2482:41–53.

[Song et al. 2010] Song, J.-H., Wong, V. W. S., and Leung, V. C. M. (2010). Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks. *Mobile Networks and Applications*, 15(1):160–171.

[Souza and Gonçalves 2013] Souza, E. F. and Gonçalves, P. A. S. (2013). Mitigação de Rastreamentos em VANETs Através de Grupos Criptográficos e Ofuscação de Localizações. In *Proceedings of Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 849–862, Brasília.

[Stübing et al. 2011] Stübing, H., Pfalzgraf, M., and Huss, S. A. (2011). A Decentralized Group Privacy Protocol for Vehicular Networks. In *Proceedings of Third IEEE International Conference on Social Computing / International Conference on Privacy, Security, Risk and Trust*, pages 1147–1154, Boston, MA, USA.

[U.S. Census Bureau 2013] U.S. Census Bureau (2013). Topologically Integrated Geographic Encoding and Referencing. `http://www.census.gov/geo/maps-data/data/tiger.html`.

[Wasef and Shen 2010] Wasef, A. and Shen, X. (2010). REP: Location Privacy for VANETs using Random Encryption Periods. *ACM Mobile Networks and Applications*, 15:172–185.

[Wiedersheim et al. 2010] Wiedersheim, B., Ma, Z., Kargl, F., and Papadimitratos, P. (2010). Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough. In *Proceedings of Wireless On-demand Network Systems and Services*, pages 176–183.

[Yin et al. 2004] Yin, J., ElBatt, T., Yeung, G., Ryu, B., Habermas, S., Krishnan, H., and Talty, T. (2004). Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, pages 1–9, New York, NY, USA.

[Zhang and Delgrossi 2012] Zhang, T. and Delgrossi, L. (2012). *Vehicle Safety Communications: Protocols, Security, and Privacy.* John Wiley and Sons. ISBN 1118132726.