Mitigação de Rastreamentos em VANETs Através de Grupos Criptográficos e Ofuscação de Localizações

Eduardo Ferreira de Souza, Paulo André da S. Gonçalves

Centro de Informática (CIn)
Universidade Federal de Pernambuco (UFPE)
50.740-560 – Recife – PE – Brasil

{efs, pasg}@cin.ufpe.br

Abstract. *Each vehicle in VANETs periodically broadcast messages with its current location. However, these messages allow attackers to improperly track any vehicle. The main mechanisms proposed to mitigate this problem are based either on cryptographic groups or obfuscations. The first approach allows attackers to easily track vehicles that are not in any group. The trace facility also occurs with the second approach, but when the vehicles are close together. This paper proposes a hybrid mechanism based on location obfuscation and cryptographic groups, which mitigates these tracking problems.*

Resumo. *Cada veículo nas VANETs transmite periodicamente mensagens contendo sua localização geográfica atual. Contudo, tais mensagens permitem que atacantes rastreiem indevidamente os veículos. Os principais mecanismos propostos para mitigar esse problema se baseiam ou no uso de grupos criptográficos ou no uso de ofuscações. A primeira abordagem permite que os veículos que não estejam em nenhum grupo possam ser facilmente rastreados. A facilidade de rastreamento também ocorre com a segunda abordagem, porém quando os veículos estiverem próximos entre si. Este artigo propõe um mecanismo híbrido, baseado em grupos criptográficos e ofuscação de localizações, que mitiga esses problemas de rastreamento.*

1. Introdução

As redes veiculares ad-hoc (VANETs) provêem um ambiente colaborativo para troca de informações entre os veículos. Em geral, as VANETs se baseiam na família de padrões IEEE 1609 para comunicação V2V (*vehicle to vehicle*) e V2I (*vehicle to infrastructure*). A família de padrões IEEE 1609 é motivada, principalmente, pelas aplicações de segurança no trânsito, isto é, pelas aplicações que informam os motoristas sobre situações de risco em potencial a fim de evitar colisões entre os veículos [IEEE P1609.2 Working Group 2006].

As principais aplicações voltadas para segurança no trânsito utilizam mensagens conhecidas como *CAMs* (*Cooperative Awareness Messages*), as quais são enviadas periodicamente por cada veículo e contêm a localização do emissor da mensagem. Através de tais mensagens, os veículos são capazes de monitorar a situação do trânsito, permitindo que sejam evitados acidentes. Apesar dos benefícios obtidos pela troca de informações de localização, essa comunicação em claro permite que qualquer veículo seja indevidamente rastreado através da captura de sucessivas *CAMs*. Dada essa vulnerabilidade, o

desafio é garantir a não rastreabilidade dos veículos, porém permitindo que sejam trocadas informações de localizações para viabilizar as aplicações de monitoração e segurança no trânsito.

Existem diversos esforços para padronizar a comunicação em redes veiculares [IEEE P1609.2 Working Group 2006, IEEE 802.11p Task Group 2010]. No entanto, o uso de múltiplos pseudônimos por cada veículo é a única diretriz estabelecida para que os ataques de rastreamentos não sejam sempre eficazes. Para isso, cada pseudônimo é utilizado apenas por um período de tempo limitado e, posteriormente, substituído. Grande parte dos mecanismos para mitigar os problemas de rastreamentos propõem que os veículos formem grupos criptográficos para a substituição de pseudônimos de forma coletiva [Freudiger et al. 2007, Stübing et al. 2011, Wasef and Shen 2010].

Um grupo criptográfico é formado por um conjunto de veículos e pode contar ou não com a presença de RSUs[1]. Esses grupos são utilizados para que os veículos troquem informações sigilosas de forma criptografada. A principal dessas informações é a localização de cada veículo. Nesse caso, um atacante não é capaz de obter tais informações com base nas mensagens trocadas internamente nos grupos. Contudo, os mecanismos baseados puramente em grupos apenas protegem as localizações enquanto os veículos pertencem a algum grupo.

Em [Chen and Wei 2012] é proposto um mecanismo baseado em técnicas de ofuscação para mitigar rastreamentos em VANETs. A ofuscação é a adulteração deliberada da precisão das localizações enviadas. Com isso, impede-se que os receptores identifiquem a localização exata 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. Assim sendo, os veículos tornam-se suscetíveis a rastreamentos nesses contextos.

Como citado, isoladamente as técnicas de grupos criptográficos e ofuscação utilizadas nos trabalhos relacionados apresentam vulnerabilidades de rastreamentos. Porém, através da união dos benefícios das duas técnicas, este artigo apresenta um mecanismo híbrido que mitiga os problemas de rastreamento. Desse modo, a solução proposta permite que todas as informações de localizações enviadas sejam protegidas ou por grupos criptográficos ou por ofuscações. O modelo de ataque utilizado considera um atacante global e passivo, isto é, o atacante é capaz de capturar simultaneamente todas as mensagens trocadas na rede, mas não envia mensagens.

O restante deste artigo está organizado da seguinte forma: A Seção 2 apresenta os trabalhos relacionados e como os mesmos se diferenciam da solução proposta neste artigo. Na Seção 3 é descrito o mecanismo proposto para mitigação de rastreamentos em VANETs. A Seção 4 avalia o desempenho da solução proposta em termos da entropia gerada, tempo máximo de rastreamento e colisões em potencial. Finalmente, a Seção 5 apresenta as conclusões.

[1] *Roadside Units* (RSUs): Dispositivos integrantes da infraestrutura e localizados às margens das rodovias.

2. Trabalhos Relacionados

As principais aplicações suportadas pela família de padrões IEEE 1609 são voltadas para segurança no trânsito e monitoração colaborativa [IEEE P1609.2 Working Group 2006]. A monitoração colaborativa permite que os usuários obtenham uma visão geral sobre as condições do tráfego nas rodovias. Por outro lado, as aplicações de segurança no trânsito atuam de forma mais específica, informando aos usuários sobre potenciais riscos de colisão. De acordo com os requisitos para o funcionamento de cada aplicação, descrito em [Hartenstein and Laberteaux 2008], é preciso que qualquer veículo da rede: (1) obtenha as localizações exatas dos veículos em sua proximidade (segurança no trânsito) e (2) possa estimar as localizações dos veículos em seu raio de alcance (monitoração colaborativa). Alguns trabalhos relacionados, no entanto, não se adequam a tais necessidades.

Atualmente, existem diversas propostas para mitigar os problemas de rastreamentos em VANETs [Freudiger et al. 2007, Stübing et al. 2011, Wasef and Shen 2010, Chen and Wei 2012]. Todas essas, exceto [Chen and Wei 2012], utilizam técnicas baseadas em grupos criptográficos. Em tais trabalhos, os grupos são utilizados apenas com foco em substituição de pseudônimos. Isto é, os grupos são finalizados após os pseudônimos serem substituídos. Como o atacante não sabe quais são os novos pseudônimos assumidos pelos veículos enquanto pertenciam aos grupos, dificulta-se que ele correlacione um dado veículo antes de ingressar no grupo como sendo o mesmo veículo após sair do grupo.

Em [Wiedersheim et al. 2010] e [Pan and Li 2012] são demonstradas as vulnerabilidades inerentes aos mecanismos que se propõem a impedir correlações entre pseudônimos. Através de simulações, em [Wiedersheim et al. 2010] é mostrada uma capacidade de rastreamento superior a 900 segundos, mesmo que os veículos substituam seus pseudônimos em curtos intervalos de 4 segundos. Isso ocorre porque as características de mobilidade de um dado veículo (localização, direção, sentido, velocidade, etc) permanecem após a substituição, sendo possível um atacante inferir que apenas o pseudônimo está modificado.

Na proposta apresentada em [Freudiger et al. 2007] são utilizados grupos situados em regiões fixas do mapa e gerenciados por RSUs. O mecanismo define que os grupos estejam localizados em cruzamentos entre vias para dificultar correlações de pseudônimos, visto que nessas regiões os veículos tendem a mudar suas características de mobilidade. Como os veículos protegem suas localizações apenas enquanto pertencentes aos grupos, em todos os outros contextos eles ficam suscetíveis a 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.

O esquema proposto em [Stübing et al. 2011] utiliza regiões pré-definidas no mapa, conhecidas por todos os veículos da rede, para que sejam formados grupos criptográficos. No mecanismo, é desnecessária a utilização de RSUs para gerenciar as chaves do grupo, visto que as chaves são definidas de forma colaborativa pelos veículos. Porém, assim como em [Freudiger et al. 2007], os veículos ficam vulneráveis a rastreamentos quando não pertencem aos grupos e, além disso, não é possível a comunicação entre veículos internos e externos aos grupos.

Diferentemente dos outros trabalhos citados até então, o mecanismo proposto em [Wasef and Shen 2010] não limita a formação de grupos a regiões fixas do mapa.

Nesse caso, quando um veículo precisa substituir seu pseudônimo, ele requisita a formação de um grupo. 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, é assumido que os atacantes não conhecem tais chaves. Desse modo, pode-se evitar que as informações de localizações possam ser obtidas indevidamente enquanto os veículos pertencem aos grupos. Contudo, a suposição feita em relação às capacidades dos atacantes não é realística, pois as OBUs[2] não são restritas aos veículos. Portanto, um atacante também conheceria as chaves secretas dos grupos assim como qualquer veículo, caso possuísse uma OBU [IEEE P1609.2 Working Group 2006].

Sumarizando os trabalhos baseados em grupos analisados: os veículos protegem suas localizações apenas enquanto pertencem aos grupos. Nos outros momentos, porém, os veículos enviam publicamente suas localizações exatas, possibilitando rastreamentos. Além disso, em [Freudiger et al. 2007] e [Stübing et al. 2011] não é possível que veículos externos aos grupos detectem a proximidade em relação aos veículos internos, dado que não há troca de mensagens entre tais entidades.

As técnicas de ofuscação são frequentemente adotadas em redes de telefonia móvel [Ardagna et al. 2011], porém essa abordagem tem sido pouco explorada em VANETs. Em [Chen and Wei 2012] é proposto um esquema de ofuscação adaptável com foco em VANETs. Nele, o emissor das mensagens reduz a área das regiões de ofuscação ao detectar a proximidade com outro veículo. Nesse caso, se os veículos estiverem significativamente próximos, eles informam suas localizações exatas para permitir detecções de riscos de colisões. Porém, como há 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.

Um problema comum a todos os trabalhos relacionados é a existência de contextos em que os atacantes podem obter as localizações exatas dos veículos. Para evitar rastreamentos de forma eficaz, é preciso assegurar que apenas veículos que realmente necessitam obter informações sobre localizações exatas o façam. A solução proposta neste trabalho impede o acesso inadequado às localizações exatas dos veículos através da união das técnicas de grupos criptográficos e ofuscação de localizações.

3. O Mecanismo Proposto

Este trabalho propõe simultaneamente novas técnicas de ofuscação e de grupos criptográficos. A ofuscação de localizações é realizada tanto para que as entidades obtenham estimativas das condições do trânsito quanto para que sejam detectadas as necessidades de formação de grupos. Para isso, os veículos sempre propagam suas localizações ofuscadas, independentemente de estarem presentes ou não em grupos. A comunicação através de grupos é estabelecida sempre que dois ou mais veículos encontram-se a uma distância que pode gerar riscos de colisão. Ao se comunicarem em grupos, os veículos passam a informar suas localizações exatas aos veículos internos ao grupo.

[2] *On-Board Units* (OBUs): Dispositivos que operam em movimento e suportam comunicação com outras OBUs e com as RSUs. Todos os veículos possuem OBUs embutidos, porém estes dispositivos não são restritos aos veículos, visto que OBUs podem ser utilizadas de forma portátil.

3.1. Ofuscação

A localização ofuscada é informada como uma região de circular onde o emissor está contido. Desse modo, um atacante não é capaz de obter a localização exata do veículo. Além disso, a sobreposição entre regiões de ofuscação de diferentes veículos eleva a dificuldade de rastreamentos. Essa dificuldade também pode ser definida como a entropia da rede.

A posição real do emissor pode ser qualquer ponto (x, y) contido na região de ofuscação, visto que tal região é calculada de forma pseudoaleatória. Para calcular o ponto central (x', y') da região de ofuscação, são gerados aleatoriamente 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'). Seja r o raio da região de ofuscação, então $0 \leq d \leq r$; e $0 \leq \alpha < 2\pi$. Assim sendo, x' e y' são definidos através da Equação (1):

$$\begin{aligned} x' &= x + d \times cos(\alpha), \\ y' &= y + d \times sen(\alpha). \end{aligned} \tag{1}$$

Ao receber uma mensagem contendo uma região ofuscada, o receptor não é capaz de obter a localização exata do emissor. Portanto, é possível apenas identificar que há algum veículo localizado dentro de tal região.

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

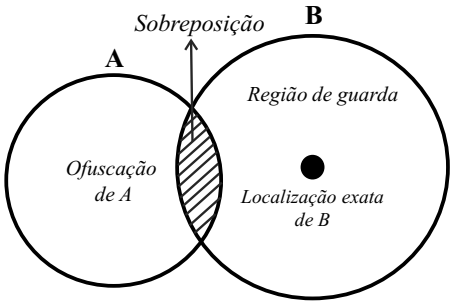

Figura 1. Situação de Risco detectada por *B*.

A Figura 1 ilustra a verificação de sobreposição realizada por B. No cenário ilustrado, caso B verifique que há sobreposição, uma mensagem de *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, pois os veículos ainda não pertencem a um mesmo grupo nesse momento. O grupo apenas será estabelecido caso

A também detecte a situação de risco através da localização ofuscada de B, contida no *Group Request*.

O raio da região de guarda (r_g) 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, minimiza-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.

3.2. Grupos Criptográficos

Os grupos criptográficos provêem um canal de comunicação seguro para a troca de localizações exatas, impedindo que um atacante global e passivo as obtenha. O gerenciamento de grupos proposto é realizado pelos próprios veículos e, portanto, independente de RSUs. Ao ingressarem em grupos, os veículos passam a enviar suas localizações exatas em um campo cifrado das *CAMs*. Porém, as mensagens podem conter simultaneamente informações de conhecimento público e informações restritas. Informações como número de identificação (ID) do grupo, pseudônimo e localização ofuscada do emissor são exemplos de informações enviadas em claro. Desta forma é possível que os veículos externos detectem situações de risco e ingressem em grupos pré-existentes. Destaca-se que, na prática, os pseudônimos são as chaves públicas utilizadas pelos veículos. Tais chaves são conhecidas e homologadas por uma Autoridade Certificadora[3] (AC) [IEEE P1609.2 Working Group 2006].

Visando minimizar a sobrecarga na rede decorrente do envio de *CAMs* distintas para os veículos internos e externos, apenas uma *CAM* é enviada contendo tanto a localização exata quanto a ofuscada. Porém, caso o veículo pertença a mais de um grupo, *CAMs* distintas são enviadas para cada um dos grupos. Nesse caso, a localização ofuscada do emissor é mantida constante ao enviá-las para grupos simultâneos, evitando o problema de ofuscações sobrepostas, descrito em [Ardagna et al. 2011].

3.2.1. Formação de Grupos

A Figura 2 ilustra a formação de grupo entre os veículos A e B. Os pontos nos centros das regiões de guarda representam a posição exata do receptor da mensagem. Imediatamente após A detectar a situação de risco, tal veículo envia para B um *Group Request*. A localização ofuscada de A, contida em tal mensagem, é utilizada para que B também verifique a existência de situação de risco entre as entidades. Caso também seja verificado, B poderá aceitar A em um grupo pré-existente ou criar um novo grupo para comunicação entre as entidades. Prioritariamente, a decisão tomada por *B* é aceitar A em um grupo pré-existente. Caso B pertença a mais de um grupo, ele aceitará A no grupo com maior número de veículos. Desse modo é minimizada a quantidade de grupos simultâneos que os veículos participam, minimizando também o *overhead* de troca de mensagens.

[3]Autoridade Certificadora (AC): Entidades confiáveis com permissões para autorizar e revogar a participação de dispositivos na rede.

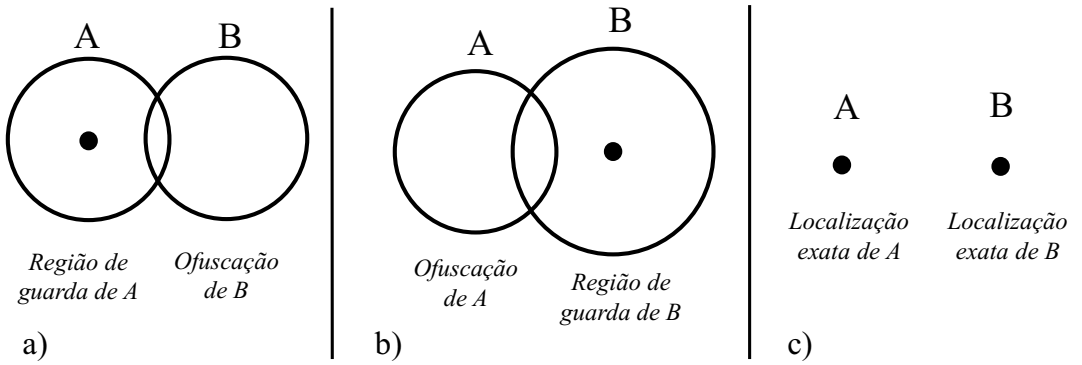

Figura 2. Exemplo de formação de Grupo. a) *B* envia um *CAM* e *A* detecta o risco; b) *A* envia a *Group Request* contendo sua localização ofuscada, e *B* detecta o risco; c) *B* envia a confirmação de formação de grupo, e os veículos passam a informar as localizações exatas.

A criação de um novo grupo é realizada apenas entre os dois veículos (A e B). Nesse processo, o veículo requisitado (B) torna-se o líder do grupo, 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, B envia uma mensagem *Distribute Key* contendo os parâmetros do grupo. Caso seja utilizado um grupo pré-existente, tais parâmetros não são recalculados, mas apenas enviados para A. Destaca-se que, em grupos pré-existentes, qualquer veículo do grupo pode aceitar a entrada de novas entidades. Os parâmetros contidos na *Distribute Key* são cifrados através da chave pública do receptor.

3.2.2. Parâmetros do Grupo

Os identificadores do grupo, contidos nas mensagens internas, permitem que os receptores verifiquem se pertencem ao grupo ao qual uma mensagem está endereçada. A identificação do 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 (2) a seguir:

$$group\_ID = SHA\text{–}256(lider\_pub\_key \| contador\_de\_grupos). \quad (2)$$

Além da chave pública do líder, também é utilizado um contador de grupos, que é incrementado pelo líder a cada novo grupo criado. Desta forma, caso o líder crie mais de um grupo antes da substituição de sua chave pública, os IDs dos grupos serão diferentes. Assim como o ID do grupo, a chave simétrica (sim_k) é calculada da seguinte forma:

$$sim\_k = SHA\text{–}256(lider\_ID \| lider\_pub\_key \| group\_ID), \quad (3)$$

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 veículo e pela AC.

Naturalmente, é possível utilizar outras funções de dispersão, como SHA-3, para o cálculo da chave. É utilizada a função 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 o *não-repúdio*, isto é, garantir que o emissor de uma mensagem não possa negar sua autoria. Desse modo, as mensagens tornam-se passíveis de auditorias. Através da assinatura digital contida em mensagens cifradas, uma autoridade certificadora é capaz de identificar seus emissores, porém não consegue obter os textos-planos para eventuais auditorias. Diferentemente dos trabalhos relacionados, o esquema de cálculo das chaves definido neste trabalho garante à AC a capacidade de obter as chaves de todos os grupos e, consequentemente, os textos-planos das mensagens cifradas com as chaves simétricas dos grupos.

Para que a AC possa calcular a sim_k de um dado grupo, é necessário que seja obtida apenas uma mensagem interna de tal grupo. Dentre os três argumentos utilizados para o cálculo de sim_k, os campos $group\_ID$ e a $lider\_pub\_key$ trafegam em claro. 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 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, em geral, é necessário que sejam reportadas um conjunto de mensagens para a AC. Dependendo do protocolo definido para essas situações, as RSUs ou os próprios veículos podem reportar tais mensagens. Porém, vale ressaltar que quaisquer análises ou reportações realizadas no processo de auditoria estão fora do escopo deste trabalho.

3.2.3. 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 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. Porém, esse grupo será desnecessário após o distanciamento dos veículos, dado que o grupo é composto apenas por eles. Portanto, é necessário que os veículos removam o grupo formado. Em grupos compostos por mais de dois elementos, a saída de veículos implicará substituição do grupo através do processo de RGP (*Replacement Group Procedure*).

Além da saída de veículos, as diferentes características mobilidade geram segregações do grupo ao longo do tempo. Para detectar tais eventos, todos os veículos do grupo realizam individualmente o monitoramento dos eventos de saída através do tempo de recebimento da última mensagem das outras entidades. Assim sendo, não há sincronização entre os veículos, centralização de responsabilidades ou pontos únicos de falhas. Portanto, cada elemento do grupo possui uma visão particular sobre a presença ou não 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 de saíram do grupo, (2) divisão do grupo em subgrupos, (3) eliminação de grupos desnecessários e (4) modificação da chave simétrica.

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 do grupo aos outros veículos através de uma mensagem de requisição (*Group Replace Request*). Essa requisição é enviada após um período aleatório de espera (*time_to_request*). Desse modo, é possível minimizar as situações de requisições simultâneas enviadas por veículos distintos. Tal mensagem é responsável por indicar que houve um evento de saída e que o requisitante deseja substituir o grupo. Nesse caso, o emissor se tornará o líder do novo grupo caso sua requisição seja aceita pelos outros veículos. 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 3 ilustra a comunicação entre dois veículos (A e B) durante o RGP. Caso o grupo seja composto por múltiplas entidades, outros veículos, além de B, 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.

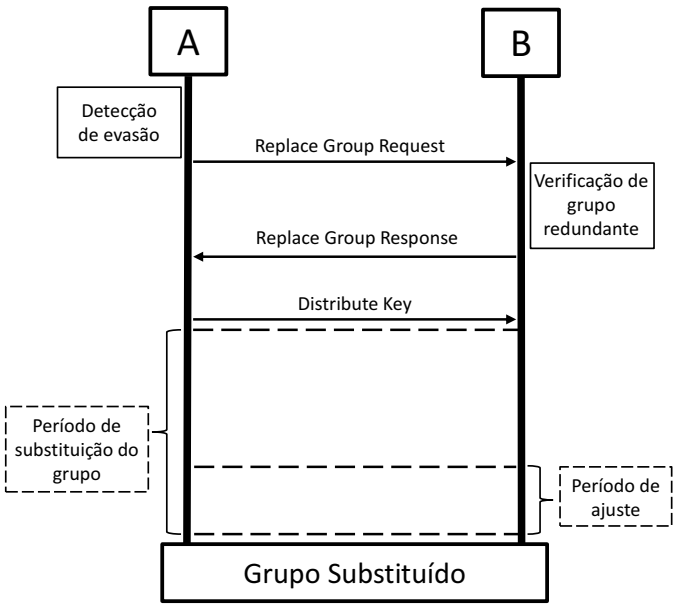

Figura 3. RGP - Troca de mensagens entre *A* e *B* para substituição de grupo.

Ao receber o *Group Replace Request*, B verifica se G_1 é um grupo redundante e, caso negativo, uma mensagem *Group Replace 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 ao *Group Replace Request*, uma nova requisição é enviada após um período aleatório (*time_to_request*). As assinaturas digitais do *Group Replace Request* e do *Group Replace Response* são cifradas através da chave simétrica do grupo. Portanto, apenas veículos pertencentes ao grupo podem enviá-las.

Após A calcular os parâmetros de G_2, a nova chave simétrica é cifrada através

da chave pública de B e é enviada como conteúdo da mensagem *Distribute Key*. Essa chave é cifrada com a chave pública de B, garantindo que apenas B seja capaz de 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, isto é, B verifica se o ID de G_1 corresponde ao grupo que A requisitou substituir.

Ao ser distribuída a sim_k de G_2 por A, inicia-se o *período de substituição do grupo* (Figura 3). 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. Assim sendo, 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. Nesse caso, tais veículos podem passar a se comunicar de forma ofuscada, mesmo estando em situação de risco. Para mitigar esse problema, o *período de ajuste* (Figura 3) é utilizado. Nesse período, todos os veículos de G_1 verificam se o emissor de cada *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*. Nesse momento, como ambos os veículos ainda pertencem a G_1, o *Group Request* contém a localização exata de seu emissor.

Como citado, é possível que alguns veículos permaneçam simultaneamente em mais de um grupo ativo. Como exemplo, considere que o veículo V_1 esteja em situação de risco em relação a dois veículos, V_2 e V_3, porém que V_2 e V_3 não estejam em situação de risco entre si. Considerando que V_1 envia duas mensagens de *Group Request*, uma para V_2 e outra para V_3, então V_1 irá participar de dois grupos simultaneamente. Os grupos formados serão G_{1_2}, composto por V_1 e V_2, e G_{1_3}, composto por V_1 e V_3. Posteriormente, se V_2 e V_3 ficarem em situação de risco entre si e V_2 entrar em G_{1_3}, então G_{1_2} torna-se desnecessário. Para mitigar a participação em grupos desnecessários, cada veículo frequentemente verifica se há grupos totalmente contidos em outros grupos aos quais ele pertença e, se identificados, estes são removidos.

4. Avaliação de Desempenho

O desempenho do mecanismo proposto é analisado através de um simulador de troca de mensagens desenvolvido neste trabalho. O trabalho adota a estrutura de quadros do padrão IEEE 802.11p [IEEE 802.11p Task Group 2010]. Conforme as orientações da família de padrões IEEE 1609 para ambientes urbanos, o alcance máximo das mensagens utilizado na comunicação entre os veículos é de 300 metros. Além disso, os veículos enviam *CAMs* com frequência média de 200 milissegundos.

O mapa utilizado para simular a mobilidade dos veículos é uma área de 1 km^2 do centro da cidade de São Francisco – CA, nos Estados Unidos. O mapa de rodovias foi obtido através do U.S. Census Bureau [U.S. Census Bureau 2012]. Os registros das movimentações são gerados pelo simulador VanetMobiSim [Harri et al. 2007] e, posteriormente, importados para o simulador de troca de mensagens desenvolvido no trabalho.

Em [Santa et al. 2009] é apresentado o resultado de um experimento de

comunicação de veículos em um ambiente real. No experimento, a taxa de perda de mensagens foi afetada por fatores como a velocidade dos veículos e a densidade da rede. Contudo, a taxa máxima de perda obtida foi de 1,16%, isto é, 98,84% de taxa de entrega de mensagens. Com base em tal experimento, as simulações realizadas neste trabalho utilizam uma taxa de perda fixa de 1,5%.

Para a geração de mobilidade dos veículos com o simulador VanetMobiSim, são considerados uma velocidade máxima de 110km/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. Cada simulação realizada reflete em trinta minutos de movimentação real dos veículos ao longo do mapa. Além disso, são realizadas vinte simulações e os resultados são medidos com intervalo de confiança de 99%. São analisadas densidades 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. Os períodos estáticos utilizados para a simulação são: 9 segundos para *período de substituição do grupo*, 3 segundos para *período de ajuste* e 3 segundos para *período de remoção de redundância*. O fator de guarda utilizado é $f_g = 1 + 1/3$ para o caso de recepção de *Group Request*.

As métricas para avaliar o desempenho deste trabalho são as seguintes: a *entropia média dos veículos*, o *tempo máximo de rastreamento* e a quantidade de *colisões em potencial* enfrentadas pelos veículos. A *entropia* indica a dificuldade de rastreamento de um dado veículo para o atacante. O *tempo máximo de rastreamento* indica o maior período contínuo que o atacante consegue rastrear um veículo. Por fim, as *colisões em potencial* indicam os momentos em que os veículos ficam próximos entre si e sem se comunicarem através de grupos. Nas simulações não há modificações de pseudônimos. Caso houvesse, isso elevaria, potencialmente, a dificuldade de rastreamentos.

A dificuldade de rastreamento (*entropia*) de um veículo pode ser medida através do tamanho de seu conjunto de anonimato [Serjantov and Danezis 2003]. A *entropia* mede 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. A *entropia* por si só apenas indica, de forma abstrata, quais cenários são mais difíceis para que um atacante realize rastreamentos. Porém, essa métrica é importante para que seja calculado o *tempo máximo de rastreamento* de um veículo.

Como o atacante não tem acesso às localizações exatas dos veículos, os tamanhos dos conjuntos de anonimato são computados apenas com base nas ofuscações. A análise realizada considera um conjunto de anonimato como um conjunto de veículos que enviam *CAMs* em uma amostra de tempo de 200 milissegundos, e que as áreas ofuscadas das mensagens possuem sobreposições simultâneas. A probabilidade do veículo n ser rastreado com sucesso é p_n, S_n é o conjunto de anonimato ao qual n pertence, $\|S_n\|$ é o tamanho de S_n e $H(n)$ é a *entropia* do veículo n, conforme a Equação (4) a seguir:

$$H(n) = -\sum_{n=1}^{\|S_n\|} p_n \log_2 p_n, \text{ onde } \sum_{n=1}^{\|S_n\|} p_n = 1. \tag{4}$$

Caso nenhum outro veículo além de n pertença ao conjunto de S_n, então $H(n)$ será 0 (zero). Nesse caso, n é trivialmente rastreável por um atacante. A Equação (5) apresenta a *entropia* média dos N veículos da rede ao longo de todo o tempo T de simulação.

$$H(T,N) = \frac{\sum_{t=1}^{T}\sum_{n=1}^{N} H(n)}{T \times N}. \quad (5)$$

A Figura 4 apresenta a *entropia* média para diferentes raios de ofuscação e densidades de veículos na rede. Percebe-se que ambas as variáveis impactam positivamente na *entropia* à medida que são incrementadas. Isso ocorre porque ambas geram um maior número de sobreposições entre as ofuscações, ocasionando em maior dificuldade de rastreamentos para um atacante.

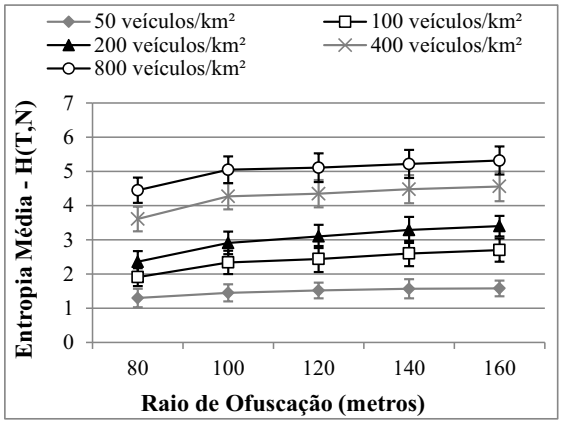

Figura 4. *Entropia* média da rede.

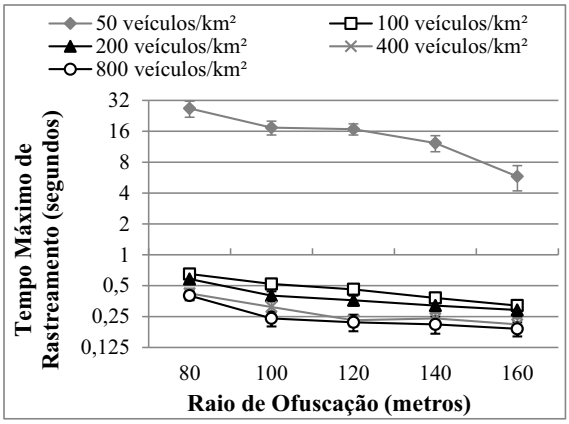

Figura 5. Média dos períodos máximos de rastreamento.

Como consequência da *entropia* $H(n)$, é avaliado o *tempo máximo de rastreamento* determinístico por um atacante global e passivo. Portanto, para que um atacante possa realizar o rastreamento com sucesso, é necessário que a *entropia* do veículo alvo seja zero. A Figura 5 apresenta a média do período máximo de rastreamento de todos os veículos da rede. Nota-se que no cenário com 50 veículos/km^2, onde a rede é pouco densa, o período de rastreamento varia entre 6 e 28 segundos, dependendo do raio de ofuscação utilizado. Naturalmente, como os veículos trafegam longas distâncias sem se aproximarem de outros veículos, não há sobreposição entre áreas de ofuscação, tornando-os vulneráveis a rastreamentos. Nos cenários com 100, 200, 400 e 800 veículos/km^2, os períodos de rastreamento máximos são inferiores a 1 segundo, demonstrando a maior eficiência do mecanismo em redes com densidades médias e altas.

Como citado, os veículos em conjuntos de anonimato de tamanho 1 são rastreáveis, visto que a *entropia* gerada para o atacante é 0. Em [Freudiger et al. 2007], [Stübing et al. 2011] e [Wasef and Shen 2010], os veículos participam de conjuntos de anonimato com tamanho maior que 1 apenas enquanto pertencem a grupos, pois este é o único momento que o atacante não obtém as localizações 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 tais mecanismos, é preciso que: (1) pelo menos dois veículos estejam próximos entre si e (2) um grupo seja formado entre as entidades. No entanto, a solução proposta neste trabalho

também garante que a *entropia* será maior que 0, caso (1) e (2) sejam verdadeiros. Assim sendo, o *tempo máximo de rastreamento* em [Freudiger et al. 2007], [Stübing et al. 2011] e [Wasef and Shen 2010] é, garantidamente, maior ou igual ao *tempo máximo de rastreamento* deste trabalho. De modo semelhante, em [Chen and Wei 2012] o tamanho de um conjunto de anonimato é maior que 1 apenas quando os veículos não estão próximos entre si. Porém, este trabalho garante a sobreposição de ofuscações de veículos próximos, de modo que o tamanho do conjunto de anonimato torna-se maior que 1 nessas situações. Desse modo, o *tempo máximo de rastreamento* em [Chen and Wei 2012] também é maior ou igual ao deste trabalho.

As métricas de *colisões em potencial* são utilizadas para medir a frequência e o tempo que os veículos ficam entre si em distâncias inferiores a 50% do raio de ofuscação quando eles não pertencem a um mesmo grupo. Na Figura 6 é mostrado que o percentual de *colisões em potencial* é inferior a 1% em todos os cenários. Além disso, o tempo médio em que essas situações perduram é inferior a 0,7 segundos, como apresentado na Figura 7. Portanto, os veículos permanecem sem o auxílio dos grupos para indicar potenciais riscos de colisão apenas em curtos intervalos de tempo. Considere o cenário de 800 veículos/km^2 e raio de ofuscação de 160 m: caso os veículos se aproximem a uma velocidade relativa de 80 km/h (22,2 m/s), então no intervalo de 0,7 segundos (Figura 7) eles se aproximam 15,6 m. Porém, como 50% do raio de ofuscação corresponde a 80 m, então os veículos detectam o risco a uma distância de 64,4 m, restando-lhes 2,9 segundos para realizarem manobras que evitem a colisão. Ressalta-se que essas situações ocorrem em menos de 1% dos momentos que os veículos precisam se comunicar em grupos, como apresentado no percentual de *colisões em potencial*.

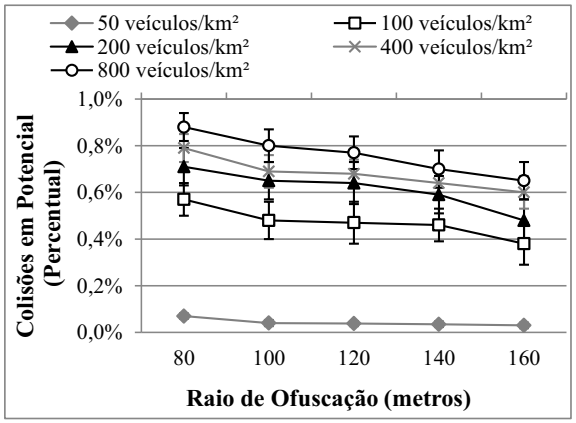

Figura 6. Percentual de *colisões em potencial*.

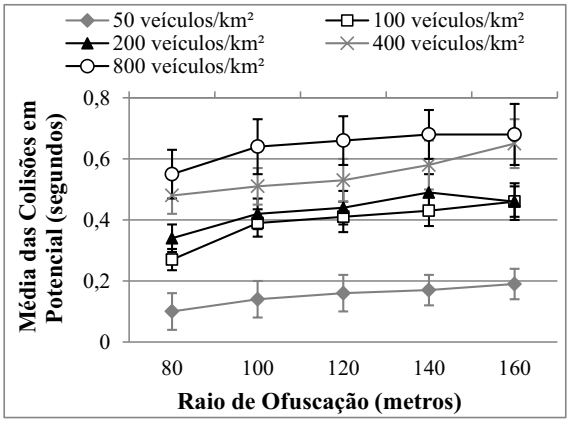

Figura 7. Duração média das *colisões em potencial*.

5. Conclusões

Neste trabalho foi proposto um mecanismo para mitigar o problema de rastreamento em redes veiculares. Foi utilizada uma abordagem híbrida, baseada em ofuscação de localizações e em grupos criptográficos. Tal abordagem se adequa às necessidades das aplicações de monitoração e segurança no trânsito. Diferentemente dos trabalhos relacionados, a localização exata dos veículos não trafega em claro na rede em nenhum momento. Foi demonstrado que a solução proposta garante um grau de *entropia* mais elevado que os trabalhos relacionados e, portanto, uma maior dificuldade de rastreamentos.

Através das simulações, foram analisadas as *colisões em potencial* sofridas pelos veículos. Em todos os cenários, o percentual de *colisões em potencial* foi inferior a 1%. Além disso, essas situações perduraram por menos de 0,7 segundos. Por outro lado, a principal métrica para avaliar o desempenho da solução foi o *tempo máximo de rastreamento* dos veículos. Em todos os cenários, essa métrica atingiu média inferior a 28 segundos, com destaque para os cenários com redes de médias e altas densidades, onde se obteve uma média inferior a 1 segundo. Portanto, o atacante não consegue rastrear os veículos durante períodos significativos de tempo.

Referências

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.

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

Freudiger, J., Raya, M., Félegyházi, M., Papadimitratos, P., and Hubaux, J.-P. (2007). Mix-Zones for Location Privacy in Vehicular Networks. In *Proc. of WSN4ITS*.

Harri, J., Fiore, M., Filali, F., and Bonnet, C. (2007). Vehicular Mobility Simulation for VANETs. In *Proc. of IEEE Annual Simulation Symposium*, pages 301–309.

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 - IEEE 802.11 - Amendment 6: Wireless Access in Vehicular Environments.

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

Pan, Y. and Li, J. (2012). An Analysis of Anonymity for Cooperative Pseudonym Change Scheme in One-dimensional VANETs. In *Proc. of IEEE CSCWD*, pages 251–257.

Santa, J., Tsukada, M., Ernst, T., Mehani, O., and Gómez-Skarmeta, A. F. (2009). Assessment of VANET multi-hop routing over an experimental platform. *Journal of Internet Protocol Technology*, 4(3):158–172.

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

Stübing, H., Pfalzgraf, M., and Huss, S. A. (2011). A Decentralized Group Privacy Protocol for Vehicular Networks. In *Proc. of IEEE International Conference on Privacy, Security, Risk and Trust / IEEE SocialCom*, pages 1147–1154.

U.S. Census Bureau (2012). Topologically Integrated Geographic Encoding and Referencing. `http://www.census.gov/geo/maps-data/data/tiger.html`.

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

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