Universidade Federal da Bahia
Instituto de Matemática
Programa de Pós-Graduação em Mecatrônica

ANTÔNIO MARCOS LOPEZ FERNANDEZ
CARIANHA

UMA ABORDAGEM PARA AUMENTAR A PRIVACIDADE DE LOCALIZAÇÃO ASSEGURADA POR MIX-ZONES EM REDES VEICULARES

DISSERTAÇÃO DE MESTRADO

Salvador
2011

ANTÔNIO MARCOS LOPEZ FERNANDEZ CARIANHA

UMA ABORDAGEM PARA AUMENTAR A PRIVACIDADE DE LOCALIZAÇÃO ASSEGURADA POR MIX-ZONES EM REDES VEICULARES

Dissertação apresentada ao Programa de Pós-Graduação em Mecatrônica da Escola Politécnica e do Instituto de Matemática, Universidade Federal da Bahia, como requisito para obtenção do grau de Mestre.

Orientador: *Prof. Dr. George Marconi de Araújo Lima*
Co-orientador: *Prof. Dr. Luciano Porto Barreto*

Salvador
2011

À glória de Deus, pela graça da vida, e aos meus pais,
Antônio e Josefa, pelo exemplo de como vivê-la.

AGRADECIMENTOS

A Deus, fonte de inspiração na elaboração deste trabalho.

A toda minha família, que colaborou com muito carinho e apoio para que eu concluísse esta etapa da minha vida, em especial, meus pais, Antônio Costa Carianha e Josefa Lopez Fernandez Carianha, meu irmão, Eduardo Lopez Fernandez Carianha, e minha avó, Digna Fernandez Benitez (*in memoriam*). Agradeço também a minha namorada Ayane de Souza Paiva, por sua paciência e apoio constante.

Ao professor Dr. George Marconi de Araújo Lima e ao professor Dr. Luciano Porto Barreto, pela paciência na orientação, disponibilidade, incentivo e reflexões ao longo do desenvolvimento deste trabalho.

A todos os professores do Programa de Pós-graduação em Mecatrônica da UFBA, que contribuíram para meu aperfeiçoamento acadêmico.

À CAPES, Governo Federal, pela bolsa de incentivo à pesquisa.

Aos colegas, amigos e a todos aqueles que, direta ou indiretamente, me incentivaram e apoiaram ao longo deste percurso. Expresso a todos os meus sinceros agradecimentos.

PUBLICAÇÕES

O presente trabalho deu origem a um artigo [1] publicado no workshop internacional HotWiSec (Hot Topics on Wireless Network Security and Privacy) que ocorreu na conferência IPCCC (International Performance Computing and Communications Conference) em Orlando, Estados Unidos, no dia 19 de Novembro de 2011.

RESUMO

As redes veiculares consistem em sistemas de comunicação que possibilitam que nós veiculares possam interagir entre si e com uma infraestrutura de suporte existente ao longo do caminho percorrido por estes. Exemplos de possíveis aplicações para estas redes incluem prevenção de colisões e difusão de informações sobre condições de tráfego e da pista. Um dos principais desafios para sua adoção em larga escala é garantir a privacidade de informações particulares dos seus usuários, tais como identidade do motorista, dinâmica de seus automóveis e percurso realizado rotineiramente. A ausência da garantia de privacidade pode inibir a participação dos usuários em redes veiculares, resultando no fracasso da implantação destas.

Para proteger a privacidade de localização do usuário, este deve permanecer anônimo e não-rastreável durante seu percurso. Soluções recentes asseguram privacidade de localização por meio de "*mix-zones*", regiões onde um nó veicular pode mudar sua identidade anônima temporária (pseudônimo) sem ser rastreado. Embora as *mix-zones* evitem ataques provindos de fora da rede de comunicação veicular, elas são vulneráveis a ataques internos, pois dentro de uma *mix-zone* as mensagens são codificadas por meio de uma chave secreta de grupo. Para tratar de tal vulnerabilidade, este trabalho propõe novos mecanismos, de modo a contribuir para aumentar o nível de privacidade de localização proporcionado por tais regiões. Através da realização de simulações minuciosas, a abordagem proposta é avaliada e comparada a soluções existentes. Os resultados mostram que a solução proposta é viável e fornece maior nível de privacidade de localização.

Palavras-chave: Redes Veiculares, Privacidade de Localização, *Mix-Zone*

ABSTRACT

Vehicular networks consist in communication systems that allow vehicles to interact with each other and with a support infrastructure along their path. Examples of possible applications for these networks include collision prevention and dissemination of information regarding traffic and road conditions. Ensuring users' information privacy such as driver's identity, dynamics of their vehicles and path performed in their journey is among the main challenges to the widespread adoption of such networks. The lack of privacy guarantee may inhibit the participation of users in vehicular networks, leading to the failure of its implementation.

A user must remain anonymous and not trackable during its journey in order to protect its privacy. Recent solutions address location privacy using cryptographic "mix-zones", which are regions where nodes change their temporary anonymous identity (pseudonym) without being tracked. Although mix-zones avoid attackers from outside the vehicular network, they are vulnerable to internal attacks since within a mix-zone messages are encrypted using a group secret key. In this work the location privacy offered by mix-zones is improved with mechanisms that address such a vulnerability. By carrying out extensive simulations, the proposed approach is evaluated and compared to existing solutions. The results show that the proposed solution is feasible and provides higher location privacy.

Keywords: Vehicular Networks; Location Privacy; Mix-Zone

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AES	Advanced Encryption Standard, 16
C2C-CC	Car 2 Car Communication Consortium, 13
CA	Certificate Authority, 21
CCM	Counter with CBC-MAC, 16
CMIX	Cryptographic MIX-zones, 27
DSRC	Dedicated Short Range Communications, 13
ECDSA	Elliptic Curve Digital Signature Algorithm, 21
FCC	Federal Communications Commission, 13
ITS	Intelligent Transportation Systems, 13
MANET	Mobile Ad-Hoc Network, 10
MD5	Message Digest 5, 20
NS-2	Network Simulator 2, 50
OBU	On-Board Unit, 9
OMNET++	Objective Modular Network Testbed in C++, 50
PKI	Public Key Infrastructure, 21
RSU	Road Side Unit, 9
SHA-1	Security Hash Algorithm, 20
STRAW	Street Random Waypoint, 49
TraNS	Traffic and Network Simulator, 50
VANETs	Vehicular Ad-Hoc Networks, 1
VeiNS	Vehicles in Network Simulation, 50
WAVE	Wireless Access in Vehicular Environments, 4

CONTEÚDO

CAPÍTULO 1

INTRODUÇÃO

Avanços tecnológicos vêm sendo incorporados a veículos automotivos para um maior conforto de condutor e passageiros no trânsito. Um destes avanços consiste em sistemas de comunicação que possibilitam interação entre veículos. As Redes *Ad Hoc* Veiculares (VANETs - *Vehicular Ad-Hoc Networks*) são formadas nestes sistemas pela comunicação entre veículos automotivos ou entre um veículo e a infraestrutura localizada nas margens das pistas, formada por unidades de comunicação dispostas em intervalos regulares e planejada para oferecer suporte a estas redes. Além de possibilitar a interação entre usuários móveis, estes sistemas têm como objetivo atender aplicações com requisitos diversos. Exemplos destas aplicações incluem prevenção de colisões e difusão de informações sobre condições de tráfego e da pista.

A redução de acidentes implica não apenas em redução de perda de vidas como também em um menor impacto econômico. Na União Europeia, ocorrem mais de 43.000 fatalidades anualmente, os gastos com estes acidentes chegam a €180 bilhões [6]. Os danos são igualmente devastadores nos Estados Unidos, onde ocorrem mais de 34.000 mortes por ano e o impacto econômico é de $164.2 bilhões [7, 8]. No Brasil, os acidentes de trânsito representam uma das principais causas externas (violências e acidentes) de morte no país, apenas não ultrapassam os homicídios. Em 2010, foram pagos, no Brasil, 50.780 sinistros de morte pelo seguro obrigatório [9], que implicaram em um custo de R$836 bilhões em indenizações e despesas [10].

Estas redes possuem uma série de desafios para sua adoção em larga escala. Dentre os principais desafios está o de garantir a segurança da comunicação veicular [11, 12, 13, 14]. Um significativo conjunto de ferramentas e possibilidades são oferecidos aos condutores e autoridades, mas um conjunto de abusos e ataques maliciosos se tornam possíveis, de modo que a falta de segurança facilitaria o comportamento antissocial e, possivelmente,

criminoso em tais redes.

Entre os diversos desafios para a segurança da informação em VANETs, a garantia de privacidade de localização é um dos requisitos mais importantes, segundo Laurendeau e Barbeau [15]. A preservação da privacidade dos usuários deve ser garantida em relação a informações particulares destes, como nome do condutor, número da placa, velocidade, posição, fabricante, modelo, número de identificação do veículo e percurso realizado rotineiramente. A ausência da garantia de privacidade pode inibir a participação dos usuários na comunicação veicular, resultando no fracasso de sua implantação, o que impossibilitaria os seus diversos benefícios.

Uma descrição de vulnerabilidades de segurança nestas redes e considerações sobre mecanismos necessários para solucioná-las são apresentadas na seção 1.1. A seção 1.2 apresenta as contribuições deste trabalho e a seção 1.3 descreve sua estrutura.

1.1 MOTIVAÇÃO

Surpreendentemente, as implicações de segurança e privacidade na comunicação sem fio das redes veiculares são geralmente subestimadas. Sistemas de comunicação veicular podem proporcionar segurança contra colisões e conforto aos condutores no trânsito, mas isto somente é possível se a segurança da comunicação contra ataques e atividades maliciosas for devidamente garantida.

Por exemplo, um veículo comprometido que forja mensagens para se mascarar como um veículo de emergência poderia enganar os demais veículos para fazê-los desacelerar ou encostar. Outra possibilidade é a transmissão de informações falsas sobre o fluxo de trânsito de um determinado local para induzir outros veículos ao uso de uma rota alternativa. É possível também que um atacante realize, na comunicação entre um nó veicular e uma unidade da infraestrutura, ataques do tipo “homem no meio”, em que um atacante estabelece conexões com seus alvos e espiona ou modifica as mensagens trocadas entre estes, os quais acreditam que estão se comunicando diretamente.

Assegurar a garantia de privacidade também é um desafio para a segurança da comunicação das redes veiculares. É interessante notar, primeiramente, que a proteção à privacidade está se tornando um problema de importância crescente na nossa sociedade digital. Mudanças na legislação estão em curso em vários países para a coleta e armazenamento de informações dos cidadãos, como a impressão digital e informações provindas de outros dispositivos biométricos. A questão vem ganhando também mais atenção do público devido a notícias recorrentes sobre vazamento de registros de dados pessoais por empresas e agências governamentais. Nas redes veiculares, uma consequência da ausência da garantia de privacidade é que um usuário pode tornar-se vítima de sequestradores se o crime organizado desvendar sua identidade através da análise da comunicação veicular e, em seguida, derivar informações sobre sua residência e rotina.

Nos sistemas veiculares, o monitoramento do tráfego já é possível devido ao aumento do número de câmeras e sensores na infraestrutura de trânsito. Entretanto, o monitoramento em larga escala de padrões de percurso de usuários específicos não é viável. Sistemas de vigilância modernos podem utilizar métodos para reconhecimento da numeração das placas, mas estes dependem de ângulos adequados para obtenção de visão desobstruída. O monitoramento das mensagens de comunicação veicular, por outro lado, pode ser conseguido com muito menos esforço em grande escala através da instalação de dispositivos de comunicação de baixo custo que registram as mensagens dos veículos ao longo das pistas. Reunindo mensagens da comunicação, é possível obter uma grande quantidade de dados, onde informações do percurso dos veículos podem ser encontradas.

Por meio destas informações, um atacante pode se beneficiar de diversas formas. Criminosos podem determinar o melhor momento para abordar suas vítimas no trânsito ou para realizar sequestros. O usuário pode ter sua privacidade invadida descobrindo-se os locais que este frequenta. Um atacante poderá agir como detetive e vender informações sobre usuários específicos ou para chantagear suas vítimas. Empresas de *marketing* podem comprar estas informações para descobrir as preferências dos usuários e importuná-los com ofertas de produtos para os quais eles sejam potenciais compradores. Deste modo, sem a garantia de privacidade de localização, os usuários podem se sentir bastante reti-

centes em utilizar tal tecnologia no trânsito, de modo a rejeita-la.

A primeira proposta para solução dos problemas de segurança da comunicação veio por meio da arquitetura WAVE (*Wireless Access in Vehicular Environments*)[16, 17], a qual estabelece um conjunto de padrões para a comunicação veicular. Um destes padrões [18] define o formato de mensagens seguras, as circunstâncias em que estas devem ser usadas e como devem ser processadas, de acordo com o nível de segurança desejado pelas aplicações.

Entretanto, a capacidade da arquitetura WAVE de garantir privacidade de localização é limitada, pois esta estabelece que as mensagens das aplicações de segurança do trânsito transmitidas periodicamente, por difusão, devem ser assinadas digitalmente. Infelizmente, neste caso, o uso de assinaturas digitais implica na transmissão do certificado digital do remetente, proporcionando os meios para que dispositivos, autorizados ou não, possam rastrear um determinado veículo por meio da identificação de tal assinatura e por meio das informações de localização difundidas em tais mensagens.

Deste modo, caso a comunicação veicular venha a ser considerada, pelos usuários, como um sistema de monitoramento em larga escala, a implantação das VANETs pode ser adiada por vários anos, ou mesmo falhar completamente, de modo que os usuários rejeitariam a tecnologia, apesar dos seus importantes benefícios para a segurança do trânsito. Visto que este é um sério problema, considerado de nível crítico, podemos concluir que a proteção da privacidade deve ser, obrigatoriamente, levada em conta nos projetos dos sistemas desenvolvidos para a comunicação veicular.

Para assegurar a privacidade de localização de um usuário, este deve permanecer anônimo e não-rastreável durante o seu percurso. Para isto, foi inicialmente proposto por Raya e Hubaux [19] o uso de pseudônimos (identidade temporária) com prazo de validade curto nas assinaturas digitais. Entretanto, mudar constantemente o pseudônimo em uso não é suficiente para garantia de não-rastreabilidade de um usuário, visto que pode-se facilmente correlacionar os pseudônimos utilizados por um mesmo nó veicular através das informações de estado (e.g., posição, velocidade, direção), disseminadas pe-

riodicamente por este [20]. Em seguida, foi proposto por Beresford [21] o uso de regiões chamadas de "*mix-zones*", as quais impedem que agentes externos à rede veicular possam utilizar dispositivos para espionagem da comunicação nestas regiões, de modo que estes não podem rastrear as mudanças de pseudônimos que nelas occorem. Entretanto, em uma abordagem proposta para implantação das *mix-zones* em VANETs, apresentada por Freudiger *et al.* [5], os nós veiculares se comunicam através de mensagens codificadas por meio de uma chave criptográfica de grupo conhecida apenas por nós autenticados que ocupam tal região, de modo que esta solução não impede um nó malicioso, capaz de se autenticar na rede, de realizar ataques à privacidade de localização dos usuários, visto que este nó tem acesso às chaves secretas usadas nestas regiões. Deste modo, faz-se necessário o desenvolvimento de uma abordagem que trate tal vulnerabilidade.

1.2 CONTRIBUIÇÕES

As principais contribuições deste trabalho podem ser assim pontuadas:

- De modo a aumentar o nível de privacidade de localização oferecido pelas *mix-zones*, este trabalho propõe uma abordagem para inibir ataques internos em tais regiões. A abordagem proposta utiliza as unidades da infraestrutura que gerenciam *mix-zones* para realizar a difusão periódica das informações de estado dos nós veiculares que ocupam estas regiões. Esta comunicação é codificada por uma chave secreta diferente para cada nó. Além disso, devido a sobrecargas na comunicação, resultante desta solução, mecanismos adicionais foram desenvolvidos para minimizar o impacto desta desvantagem. Uma avaliação experimental revelou que estes mecanismos são suficientes para viabilizar esta solução.

- Através da análise de possíveis ataques contra a privacidade dos usuários, um modelo analítico de ataque, baseado na correlação dos pseudônimos usados por usuários na entrada e saída de tais regiões, foi desenvolvido para possibilitar o estudo do nível de privacidade fornecido pela solução proposta. Por meio deste

modelo, constatou-se que o nível de privacidade de localização é satisfatório para VANETs. Em seguida, através da realização de simulações minuciosas, a solução proposta foi avaliada e comparada a outras existentes. Um dos cenários dos experimentos de avaliação foi construído de modo a representar um ambiente de comunicação veicular que se aproxima do comportamento veicular esperado para o trânsito. Para implementá-lo foi utilizado o mapa rodoviário da cidade de Colônia, Alemanha, e as trilhas dos pecursos de seus habitantes disponibilizadas pelo projeto TAPAS [22]. Até onde sabemos, este trabalho é o primeiro a demonstrar o uso de *mix-zones* neste contexto, outros trabalhos consideram apenas cenários pequenos e artificiais. Para fins de comparação, uma solução baseada no modelo "*mix-context*" encontrado na literatura foi também avaliada neste mesmo ambiente. Até onde sabemos, este trabalho é também o primeiro a avaliar o desempenho desta em relação ao nível de privacidade de localização por ela oferecido. Os resultados obtidos neste cenário mostraram que, durante o intervalo de simulação, o número de veículos rastreados foi mais que duas vezes menor quando utilizada a solução proposta

1.3 ESTRUTURA DESTE TRABALHO

Este trabalho está estruturado da seguinte forma:

- As soluções adotadas para os diversos desafios de segurança da comunicação veicular são apresentadas no capítulo 2. As soluções encontradas na literatura para garantia de privacidade dos usuários nas VANETs são também detalhadas neste capítulo.
- No capítulo 3, a solução proposta é apresentada. Uma análise de possíveis ataques a esta solução é realizada. O modelo analítico é considerado ao final deste capítulo. Este modelo é utilizado, em seguida, em experimentos que avaliam o nível de privacidade fornecido pela solução proposta.
- O ambiente utilizado para realização dos experimentos desenvolvidos é descrito no capítulo 4. A primeira avaliação apresenta um experimento controlado, enquanto

um outro experimento considera um cenário onde a movimentação veicular do projeto TAPAs é utilizada. Neste último cenário, a solução baseada no modelo "*mix-context*", um modelo alternativo ao da solução proposta, é também avaliada para fins de comparação em relação à capacidade de proteção dos usuários contra um atacante que é assumido presente em todos os locais.

- O capítulo 5 apresenta a conclusão deste trabalho e considera trabalhos futuros.

CAPÍTULO 2

SEGURANÇA DA COMUNICAÇÃO VEICULAR

Informação compreende tudo aquilo que possibilita a aquisição de conhecimento. A informação que pode ser armazenada computacionalmente e propagada na comunicação de dados deve ser protegida contra acesso não autorizado, uso, divulgação, interrupção, modificação, espionagem, gravação ou destruição. Garantir a segurança da informação em sistemas de comunicação veicular é um difícil desafio. Em parte, isto decorre de requisitos conflitantes, tais como anonimato versus irretratabilidade e nível de segurança versus eficiência. Outro fator significativo deve-se à comunicação aberta que ocorre por difusão de ondas de rádio, de modo a facilitar a espionagem desta.

Neste capítulo são analisados os requisitos de segurança necessários às redes veiculares para que estas sejam consideradas seguras e adequadas para implantação em larga escala. A seção 2.1 descreve as redes veiculares, de forma detalhada. A seção 2.2 trata dos principais serviços relacionados à segurança da informação e da aplicação destes em tais redes. A seção 2.3 apresenta soluções encontradas na literatura, desenvolvidas especificamente para assegurar privacidade de localização na comunicação veicular.

2.1 REDES AD-HOC VEICULARES

O avanço do desenvolvimento das tecnologias de comunicação tem revolucionado nosso estilo de vida por fornecer grande flexibilidade e conveniência para o acesso a serviços da Internet e várias outras aplicações de comunicação. Recentemente, fabricantes de veículos e indústrias de telecomunicações têm colaborado em um esforço para equipar veículos com tecnologia que permita a comunicação entre veículos. Tal como em redes móveis tradicionais, estas redes de comunicação se caracterizam pela movimentação e auto-organização dos nós, mas possuem como principal objetivo aumentar a segurança

nas rodovias e evitar acidentes de trânsito [23].

Através de um dispositivo de comunicação equipado nos veículos, chamado de unidade de bordo (OBU - *On-Board Unit*), veículos podem se comunicar com seus vizinhos e demais veículos durante o percurso, enquanto passageiros podem usar seus *laptops* para o acesso sem fio a serviços oferecidos por uma infraestruta de apoio presente ao longo de estradas e rodovias, constituída por dispositivos chamados de unidades de acostamento (RSU - *Road Side Unit*). Estas unidades podem estar distribuídas em intervalos regulares, conectadas diretamente ou indiretamente via uma rede de *backbones* ou através da Internet. O acesso à Internet possibilita às unidades de acostamento proverem acesso a servidores de aplicação que podem oferecer serviços diversos. Um exemplo ilustrativo de VANET é apresentado na figura 2.1.

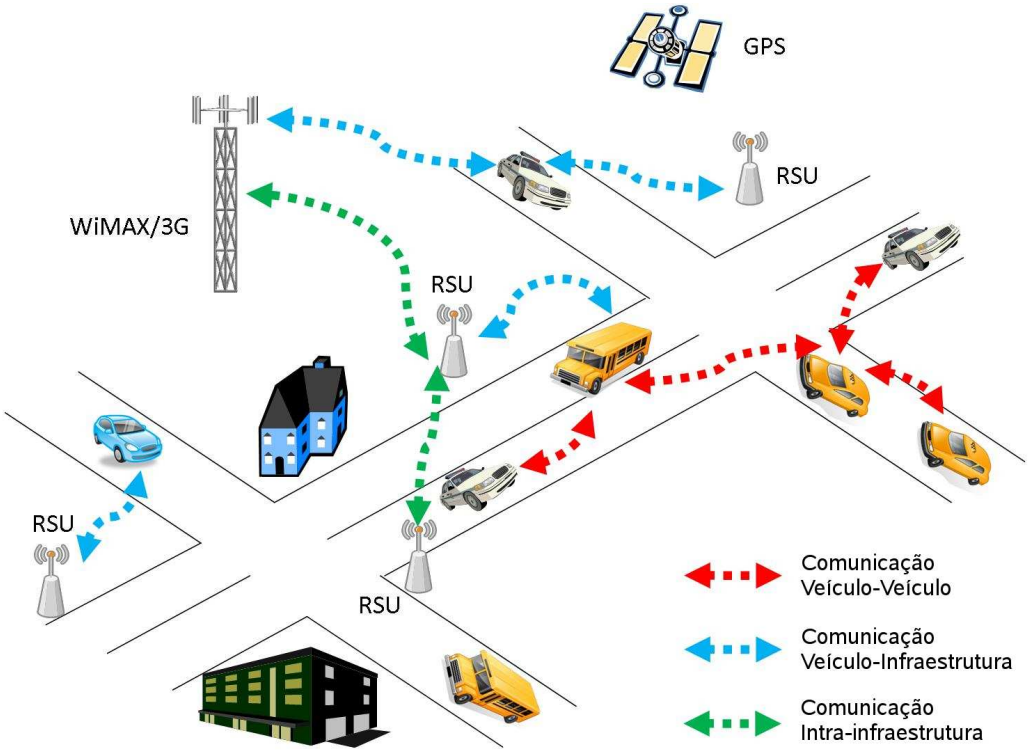


Figura 2.1: Exemplo de uma rede veicular.[2]

A comunicação veicular utiliza a tecnologia IEEE 802.11p [17] para o controle de acesso ao meio nas comunicações veículo-veículo e veículo-infraestrutura. Diversas outras tecnologias podem ser utilizadas nas VANETs, como WiMAX[24] ou redes sem fio de

terceira geração (3G). Serviços de localização por satélite, como o Sistema de Posicionamento Global (GPS) [25], desenvolvido pelos Estados Unidos, ou o sistema Galileo [26], da União Europeia, podem ser usados para determinação da localização dos veículos.

O processo de implantação destas redes ainda está em seu início, mas devido ao baixo custo e facilidade de implantação da tecnologia sem fio, espera-se que, nos próximos anos, cada vez mais veículos sejam produzidos equipados com unidades de bordo e que as margens das estradas sejam ocupadas pelas unidades de acostamento, as quais podem estar em semáforos, placas de trânsito, pedágios ou em dispositivos dedicados distribuídos em intervalos regulares.

As características que diferenciam as redes veiculares das redes móveis típicas são abordadas na subseção 2.1.1. A subseção 2.1.2 fornece detalhes sobre tipos de aplicações das VANETs. Aspectos mais detalhados da tecnologia sem fio de alcance curto são descritos na subseção 2.1.3.

2.1.1 Diferenças entre VANETs e MANETs

Tal como em uma Rede *Ad-Hoc* Móvel (MANET - *Mobile Ad-Hoc Network*), VANETs são capazes de se autoconfigurar por meio de dispositivos móveis que se comunicam através de conexão sem fio. Devido a esta similaridade, alguns princípios e conceitos aplicáveis a MANETs podem também ser aplicados ao cenário da comunicação veicular. Entretanto, as redes veiculares possuem características específicas que as diferem das redes móveis típicas, de modo que muitas das soluções para MANETs não satisfazem completamente às VANETs. Além da presença das unidades de acostamento, que formam uma infraestrutura de suporte para auxiliar nós veiculares ao longo do percurso destes, VANETs possuem as seguintes características específicas [13]:

- **Alta mobilidade e rápida mudança de topologia**: A rápida movimentação dos veículos implica que a comunicação entre eles ocorre durante poucos segundos, devido ao alcance limitado da comunicação, de modo que as conexões são estabele-

cidas e desfeitas rapidamente. Uma vez que muitos protocolos desenvolvidos para MANETs não consideram este fator, estes podem não se adequar às VANETs.

- **Restrições temporais e menor taxa de transferência**: Aplicações para VANETs, como avisos de colisão ou sensoriamento de proximidade, não requerem altas taxas de transferência de dados, como ocorre tipicamente em MANETs. Entretanto, VANETs possuem restrições temporais de atraso críticas.

- **Menor restrição de energia**: As baterias recarregáveis dos veículos representam uma alternativa para o problema do esgotamento da fonte energética que ocorre em redes móveis típicas. Deste modo, a influência da restrição de consumo de energia é muito menor em protocolos desenvolvidos para VANETs.

- **Características únicas de privacidade e segurança**: A autenticação rápida, a preservação da privacidade de forma condicional e a revogação de certificados em grande escala são alguns exemplos destas características.

- **Modelagem de mobilidade e de predição**: Visto que um nó veicular é geralmente limitado por rodovias, estradas e ruas, conhecendo-se a velocidade do veículo e o mapa do percurso, a futura posição do veículo pode ser estimada, de modo que se torna possível o desenvolvimento de modelos que permitem predizer mais facilmente a duração e o tamanho de determinadas rotas.

2.1.2 Aplicações

A disponibilização de informações sobre possíveis conflitos iminentes permite a prevenção de acidentes decorrentes da falta de cooperação entre os condutores. VANETs também facilitam a otimização do tráfego. De fato, os veículos podem coletar dados sobre engarrafamentos, condições meteorológicas, condições das pistas, zonas de construção, cruzamentos ferroviários etc. Podem, então, se tornar novas fontes de informação, enviando os dados para outros veículos ou alertas sobre situações que não podem ser detectadas no escopo de visão dos condutores. Por meio destas informações, perigos, em

potencial, podem ser detectados em seu estágio inicial e as contramedidas apropriadas podem ser providenciadas.

A atuação de aplicações relacionadas à segurança do trânsito depende de mensagens difundidas periodicamente, os chamados "*beacons*", que anunciam a presença de um veículo aos outros em sua proximidade. Estes *beacons* são mensagens curtas contendo a localização do veículo e outras informações de estado como velocidade e direção do movimento. Estas mensagens são transmitidas em períodos curtos (100 a 300 ms [19]) para que os vizinhos de um veículo obtenham atualizações do estado deste em tempo real.

As mensagens das aplicações de segurança podem ser classificadas em dois grupos: as mensagens de alerta e as mensagens de informações assistenciais [23, 27].

- **Mensagens de alerta**: Estas mensagens podem ser transmitidas, por exemplo, por uma RSU ao perceber que dois veículos se aproximam de um cruzamento de forma conflitante, de modo que estes devam providenciar alguma ação para evitar a colisão. Outro exemplo ocorre quando dois veículos estão em alta velocidade e o veículo da frente, de repente, freia bruscamente. Neste caso, o veículo da frente imediatamente transmite a mensagem de aviso de freio brusco para seus vizinhos. Deste modo, os condutores dos veículos que seguem atrás dele podem frear com antecedência ou, em último caso, uma aplicação de segurança pode decidir por frear automaticamente tal veículo.

- **Mensagens de informações assistenciais**: Uma RSU pode transmitir, por exemplo, mensagens informando sobre um fluxo de tráfego anormal devido a uma colisão de veículos, a qual incorra em uma enorme fila de trânsito. Neste caso, as unidades de acostamento espalham mensagens informando sobre tal congestionamento em um raio de alguns quilômetros para que os condutores possam escolher um caminho alternativo e evitar o engarrafamento. Outro exemplo ocorre quando veículos de emergência, como ambulâncias, carros de polícia e carros de bombeiro estão se aproximando. Neste caso, as unidades de acostamento podem notificar os

veículos que estão longe dos veículos de emergência para abrir caminho para estes com antecedência.

Além de oferecer aplicações para segurança do trânsito, VANETs também podem fornecer uma gama de outras aplicações. Algumas destas são descritas a seguir [28, 29]:

- RSUs podem servir como *gateways* para acesso à Internet ou para oferecer *uploads* / *downloads* de músicas e vídeos. Passageiros nos veículos também podem enviar / receber e-mails, navegar na Web e ter acesso a serviços diversos com diferentes qualidades de serviço, como voz sobre IP e videoconferência em tempo real.

- VANETs podem ser usadas para a disseminação de informações relativas ao ambiente. Os sensores nos veículos podem coletar dados como informações meteorológicas e umidade do ar. Os dados podem ser enviados para as RSUs, as quais podem atuar como coletores e servidores de dados.

- RSUs podem ser usadas para cobrança de pedágio ou para fins comerciais. Podem ajudar lojas a transmitir anúncios, tais como ofertas especiais de fim de semana, folhetos semanais e cupons de bilhetes de cinema. Condutores serão capazes de realizar compras diretamente através destas unidades.

- RSUs podem oferecer aos condutores serviços baseados em localização para ajudá-los na busca por locais como restaurantes, cafeterias ou postos de gasolina mais próximos. Caso uma destas unidades esteja localizada na entrada de um estacionamento, esta pode informar se este está lotado ou guiar um veículo até o local da vaga.

2.1.3 DSRC

Projetado especialmente para a comunicação em redes veiculares, o serviço DSRC [30] (*Dedicated Short Range Communications*) estabelece uma faixa de frequência para comunicação sem fio nestas redes e um conjunto de protocolos e padrões. O potencial desta

tecnologia tem sido reconhecido pelos fabricantes de automóveis, governos e instituições de pesquisa. Muitos projetos em escala nacional e internacional estão em andamento em todo o mundo e representam um esforço conjunto para o desenvolvimento das VANETs e para a definição de normas que possam garantir a interoperabilidade. Nos Estados Unidos, a *Federal Communications Commission* (FCC) reservou, em 1999, 75 MHz do espectro de frequência na faixa de 5.9 GHz para a comunicação veicular sem fio [31]. Em seguida, o DSRC foi estabelecido em 2003. Na Europa o Instituto de Padrões de Telecomunicações Europeu alocou parte do espectro de frequência na mesma faixa e o C2C-CC [32] (*Car 2 Car Communication Consortium*) desenvolve trabalhos de pesquisa nesta região. No Japão também foi reservado parte do espectro, mas para uma faixa de frequência de 5.8GHz. O ITS (*Intelligent Transportation Systems*) Consortium [33] tem desenvolvido projetos neste país. No Brasil existe a reserva do espectro para o DSRC, que já é utilizado em pedágios, mas há pouca pesquisa relacionada ao seu uso em redes veiculares [3].

Uma série de padrões foram desenvolvidos para o DRSC. Estes padrões formam a arquitetura WAVE [16, 30], ilustrada na figura 2.2. A escolha do uso da faixa de alta frequência em 5 GHz deve-se à alta taxa de transmissão de dados para distâncias apropriadas para a comunicação veicular, mesmo sob condições temporais desfavoráveis. O alcance máximo do DSRC foi estabelecido como 1000 metros [30]. Para as camadas física e de acesso ao meio, foi padronizado o uso da tecnologia IEEE 802.11p, com uma capacidade máxima de taxa de transferência de dados de até 27 Mb/s [34]. Para as camadas superiores, outros padrões desenvolvidos pelo IEEE definem um conjunto de camadas de rede semelhante ao modelo TCP/IP, que estão relacionados a aplicações, serviços de gerenciamento e a aspectos de segurança.

A arquitetura WAVE estabelece o uso do padrão IEEE P1609.2 [18] no que concerne à segurança da comunicação. Este padrão define, dentre outras coisas, os mecanismos que os diferentes tipos de aplicação podem utilizar para a garantia da segurança da informação na comunicação veicular. O padrão IEEE P1609.3 [35] define o *WAVE Short Message Protocol*, utilizado pelas aplicações de segurança do trânsito, e apresenta o *WAVE Ma-*

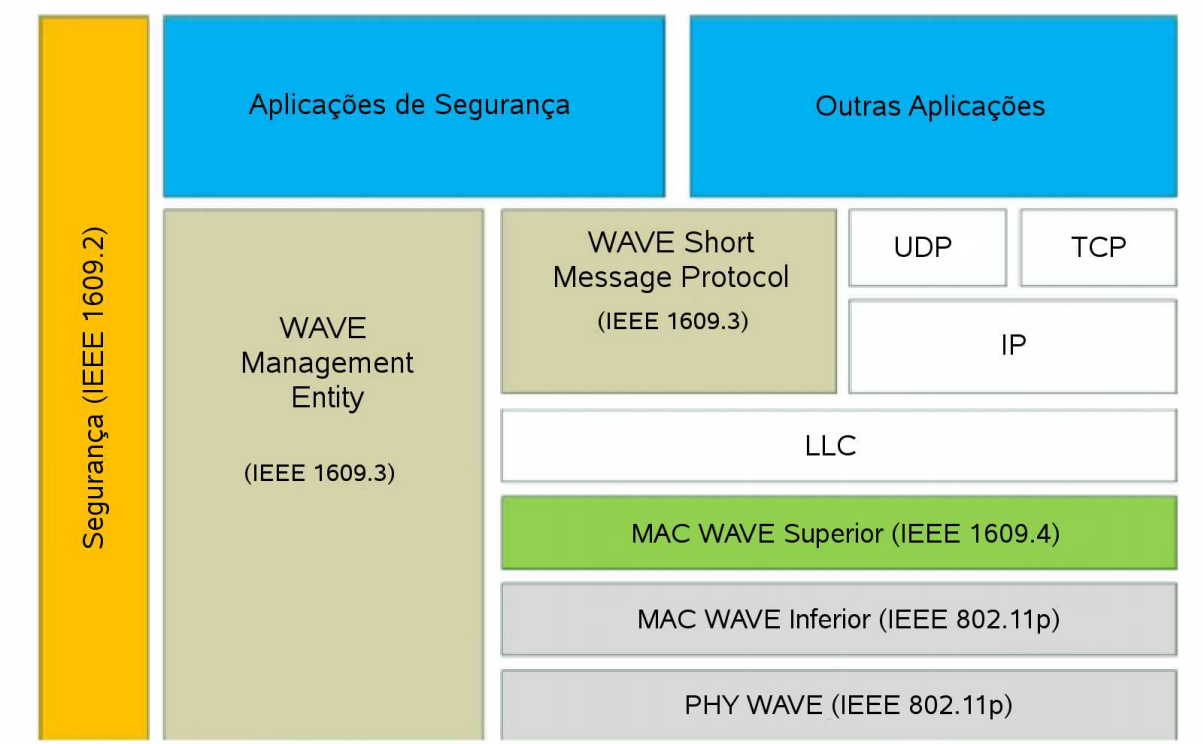


Figura 2.2: Arquitetura WAVE. [3]

nagement Entity, responsável por um conjunto de funções de gerenciamento dos serviços providos. O padrão IEEE P1609.4 [36] estende a camada MAC do padrão IEEE 802.11p para que esta possa oferecer suporte às operações da WAVE.

2.2 CONCEITOS BÁSICOS

A segurança da informação compreende um conjunto de medidas que visam a proteger e preservar a informação. Os principais serviços de segurança da informação e suas aplicações nas redes de comunicação veicular são apresentados a seguir.

2.2.1 Confidencialidade

A confidencialidade é a garantia do resguardo da informação e proteção contra sua revelação não autorizada [37]. Para isto, é preciso garantir que um atacante não seja capaz de deduzir, por meio de observação, o conteúdo das mensagens, sua origem, destino, tamanho, ou informações relacionadas ao fluxo de comunicação. A confidencialidade é essencial para as VANETs. Por exemplo, em requisições de serviços de localização, mapas e horários de voo, e em serviços de gerenciamento, como um registro perante autoridades rodoviárias, as mensagens incluem, por padrão, informações como local, horários, identificador do veículo, descrições técnicas e detalhes do percurso, os quais podem ser utilizados para identificar com precisão ações, preferências ou identidade do condutor.

A técnica que permite obter confidencialidade do conteúdo da informação na comunicação de dados é a criptografia, pela qual a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário por meio de uma chave secreta. Este é um ramo especializado da teoria da informação com muitas contribuições da matemática e de outras áreas do conhecimento. Um algoritmo criptográfico, também chamado de cifra, é uma função matemática usada para codificação e decodificação [38]. A operação do algoritmo costuma ter como parâmetro uma chave. A criptografia pode ser realizada por meio de chave simétrica ou assimétrica. Podemos compreender a diferença entre estas duas através de uma analogia com uma caixa que possui uma fechadura. Na criptografia assimétrica, ou de chave pública, a caixa aceita duas chaves diferentes: uma chave permite apenas trancar a caixa e a outra serve somente para abri-la. Qualquer um que tenha uma cópia da chave que tranca a caixa (a chave pública) pode colocar segredos nesta caixa e como há somente um possuidor da chave que abre a caixa (chave privada), este é o único que pode verificar os segredos nela guardados. Na criptografia simétrica, a mesma chave é usada tanto para trancar quanto para abrir a caixa.

Em um ambiente onde uma grande quantidade de participantes compartilha a mesma chave, caso o segredo da chave seja violado, faz-se necessário distribuir novamente uma

nova chave para todos os participantes. Esta é uma tarefa complicada, pois a distribuição deve ser realizada por um meio seguro. Para enfrentar este problema, a maior parte dos sistemas utiliza criptografia de chave pública para distribuir chaves únicas de sessão que, por sua vez, são empregadas em algoritmos de criptografia de chave simétrica. Este método também é empregado em VANETs. Na comunicação entre um nó veicular e uma RSU, uma chave é primeiramente negociada entre estes através de criptografia assimétrica, utilizando-se criptografia de chave pública sobre curvas elípticas [39, 18]. Em seguida, a comunicação passa a ser codificada por meio de criptografia simétrica, utilizando o padrão de criptografia AES (*Advanced Encryption Standard*) em modo CCM (*Counter with CBC-MAC*) [40, 41, 18].

Entretanto, tal método não é adequado, por ser custoso, para aplicações de segurança do trânsito, uma vez que estas aplicações possuem estritas restrições temporais na entrega de suas mensagens. Além disso, mensagens relacionadas às aplicações de segurança do trânsito são de interesse geral e, por este motivo, estas são difundidas abertamente, ou seja, não são codificadas. Isto implica que a coleta de informações de um nó veicular específico, por parte de um observador, é algo particularmente fácil. Inferências sobre dados pessoais de condutores poderiam violar a privacidade destes. Para isto, um observador pode utilizar-se do conteúdo destas mensagens, o qual possui informações que descrevem o estado do veículo (posição, velocidade, direção etc.) em um determinado instante. Estes dados podem ser usados para identificar o percurso realizado por um nó veicular, o qual, por sua vez, pode ser utilizado para derivar a identidade do condutor ou muitas informações particulares a respeito das atividades deste. Estas informações podem ser exploradas para disseminação de propagandas de forma impertinente, vigilância das atividades de empregados ou em atividades criminosas e atos terroristas. Soluções existentes na literatura para este desafio são descritas na subseção 2.3.

2.2.2 Integridade

A garantia de integridade objetiva combater ataques de modificação de mensagem, ou seja, cobre a violação da informação transferida, assegurando que as mensagens serão recebidas exatamente como foram enviadas, sem duplicação, inserção, modificação, reordenação ou repetição [37]. Na comunicação veicular, um nó malicioso ou defeituoso, agindo como encaminhador de mensagens de outros, pode interferir na comunicação destes, de modo a destruir, corromper ou modificar mensagens. Desta forma, notificações valiosas sobre condições de tráfego e mensagens de aviso de colisão podem ser manipuladas objetivando ataques que podem resultar em severos danos. Um atacante pode também tentar realizar ataques de repetição de mensagens para, por exemplo, obter serviços autorizados para determinados usuários. Nas VANETs, a garantia de integridade das mensagens decorre de uma das propriedades do mecanismo de assinatura digital, o qual será detalhado adiante, e do uso de um marcador temporal que garante a sua atualidade e evita ataques de repetição [12]. Para evitar que dados falsos sejam disseminados por toda a rede veicular, pode-se utilizar algum mecanismo que compare todos os dados coletados sobre um dado evento, de modo a possibilitar a classificação de dados recebidos relacionados ao evento como sendo confiáveis, pouco confiáveis ou maliciosos, antes de repassá-los aos veículos vizinhos [11]. Deste modo, por exemplo, caso apenas um veículo informe ter encontrado um acidente na pista, esta informação pode ser classificada como pouco confiável devido à ausência de confirmação deste evento por meio de outras fontes.

2.2.3 Autenticação

Por meio do serviço de autenticação, o destinatário de uma mensagem deve ser capaz de averiguar a origem desta, de modo que um atacante não deve ser capaz de assumir a identidade digital de um membro do sistema [38]. Na comunicação em uma rede veicular, as reações dos veículos a eventos devem ser baseadas em mensagens legítimas, isto é, geradas por uma origem legitimada por autenticação. A ausência da garantia de

autenticação permite, por exemplo, ataques de camuflagem de identidade.

Um nó veicular poderia falsificar sua identidade, por exemplo, mascarando-se como um veículo de emergência para induzir outros veículos a abrir caminho para sua passagem. Poderia também assumir a identidade de uma RSU e transmitir mensagens de anúncios de propaganda. Nas redes veiculares, o uso de uma assinatura digital e certificados assinados por uma terceira parte confiável são utilizados para provimento de autenticação e validação do originador de uma mensagem [11]. Existe também outro desafio relacionado à autenticação, decorrente do roubo da chave secreta que assegura a identidade única de um dispositivo de comunicação da rede veicular. Para resolver este problema, é assumido o uso de dispositivos de comunicação à prova de violações [12]. Uma desvantagem resultante desta abordagem é o encarecimento do custo para o usuário final. Entretanto, os danos evitados por ataques decorrentes da ausência deste pressuposto são muito relevantes, especialmente nos casos em que ocorra violação dos dispositivos de uma autoridade pública ou de uma RSU que fornece serviços. O atacante poderia fingir exercer o papel destas unidades para obter vantagens.

2.2.4 Irretratabilidade

Na segurança digital, irretratabilidade é a garantia que o emissor de uma mensagem não poderá, posteriormente, negar sua autoria [38]. Este também é um requisito fundamental para a comunicação veicular, pois esta pode servir como uma fonte de dados não refutáveis para ajudar em investigações legais, como no caso de acidentes. Isto implica na necessidade de identificação inequívoca dos veículos originadores das mensagens, o que vai de encontro ao requisito da privacidade. Outro exemplo que evidencia a necessidade de irretratabilidade é caso, por exemplo, um atacate finja ser um veículo de emergência ou policial para enganar os outros a sua volta, de modo a passar por estes com maior facilidade, ou fingir ser uma unidade de acostamento que transmite propagandas, de modo a forçar os veículos à receber estas informações, as quais podem ser indesejáveis para os usuários.

Nas VANETs, a propriedade da irretratabilidade é satisfeita por uma assinatura digital nas mensagens transmitidas. Entretanto, o desafio do provimento de privacidade, neste caso, requer uma solução mais complexa. A subseção 2.3 apresenta soluções desenvolvidas para VANETs que abordam esta questão.

2.2.5 Assinatura Digital

A autenticidade de documentos legais, financeiros ou de outros documentos costuma ser determinada pela presença de uma assinatura autorizada. Do mesmo modo, a assinatura digital consiste em um mecanismo de autenticação que possibilita ao criador de uma mensagem gerar um código que serve como assinatura em documentos digitais. Uma assinatura digital deve prover as seguintes propriedades [37]:

1) Autenticação de origem - o receptor deve poder confirmar que a assinatura foi feita pelo emissor declarado no campo origem;

2) Integridade - qualquer alteração na mensagem, devido a ataques ou falhas, faz com que a assinatura não corresponda mais ao documento;

3) Irretratabilidade - o emissor não pode negar sua autoria;

Tipicamente, uma assinatura envolve dois processos: a produção do *hash* e a codificação deste [38]. Em um primeiro momento é gerado o *hash*, um resumo da mensagem , através de algoritmos como MD5 [42](*Message Digest*) ou SHA-1 [43] (*Security Hash Algorithm*), que reduzem mensagens de qualquer tamanho a um resumo de tamanho fixo. Visto que o tamanho do *hash* é fixo e as mensagens possíveis são infinitas, é inevitável que mensagens diferentes levem a um *hash* idêntico. Porém, para comprometer a assinatura digital de uma mensagem original, seria necessário obter uma mensagem adulterada que resulte no mesmo resumo, o que a função *hash* garante ser um problema computacionalmente intratável[37], de modo que a probabilidade de ocorrência é desprezível.

Quando um receptor utiliza a mesma função *hash* na mensagem, o código produzido é comparado ao código enviado pelo emissor. Se o mesmo código é gerado, então a integridade da mensagem está assegurada. Para garantir também a autenticação e a irretratabilidade, o *hash* gerado pelo emissor deve ser codificado por ele utilizando um sistema de codificação assimétrica. Através de sua chave privada, o autor realiza a codificação do *hash* e o transmite anexo à mensagem. Quando o receptor decodifica o *hash* com sucesso, utilizando a chave pública do emissor, a autenticação do autor da mensagem é automaticamente assegurada. A propriedade da irretratabilidade decorre deste mesmo processo, uma vez que somente o originador possui a chave secreta que codificou o *hash* decodificado por meio da correspondente chave pública.

Nas redes veiculares, a camada de segurança IEEE P1609.2 da arquitetura WAVE recomenda o uso do Algoritmo de Assinatura Digital sobre Curvas Elípticas (ECDSA - *Elliptic Curve Digital Signature Algorithm*) [44] sobre a curva NIST p224 na assinatura das mensagens periódicas relacionadas à segurança do trânsito. O uso deste parâmetro resulta em uma assinatura de 56 bytes [18].

2.2.6 Certificado Digital

Um certificado digital é um documento eletrônico que possui dados como nome da entidade autora (pessoa ou instituição), entidade emissora do certificado, a qual funciona como uma terceira parte confiável, prazo de validade, chave pública da entidade autora e assinatura digital da entidade emissora do certificado [37]. Na comunicação de dados, pode-se usar um certificado digital para garantir à entidade que recebe uma assinatura digital a certeza de que a entidade responsável pela chave pública que valida a assinatura, declarada no certificado, é uma entidade validada por uma terceira parte confiável.

Deste modo, um certificado digital normalmente é usado para relacionar univocamente uma entidade a uma chave pública e assegurar que esta entidade é um membro válido da rede de comunicação. Em uma Infraestrutura de Chaves Públicas (PKI - *Public Key Infrastructure*), o certificado é assinado pela Autoridade Certificadora (CA - *Certificate*

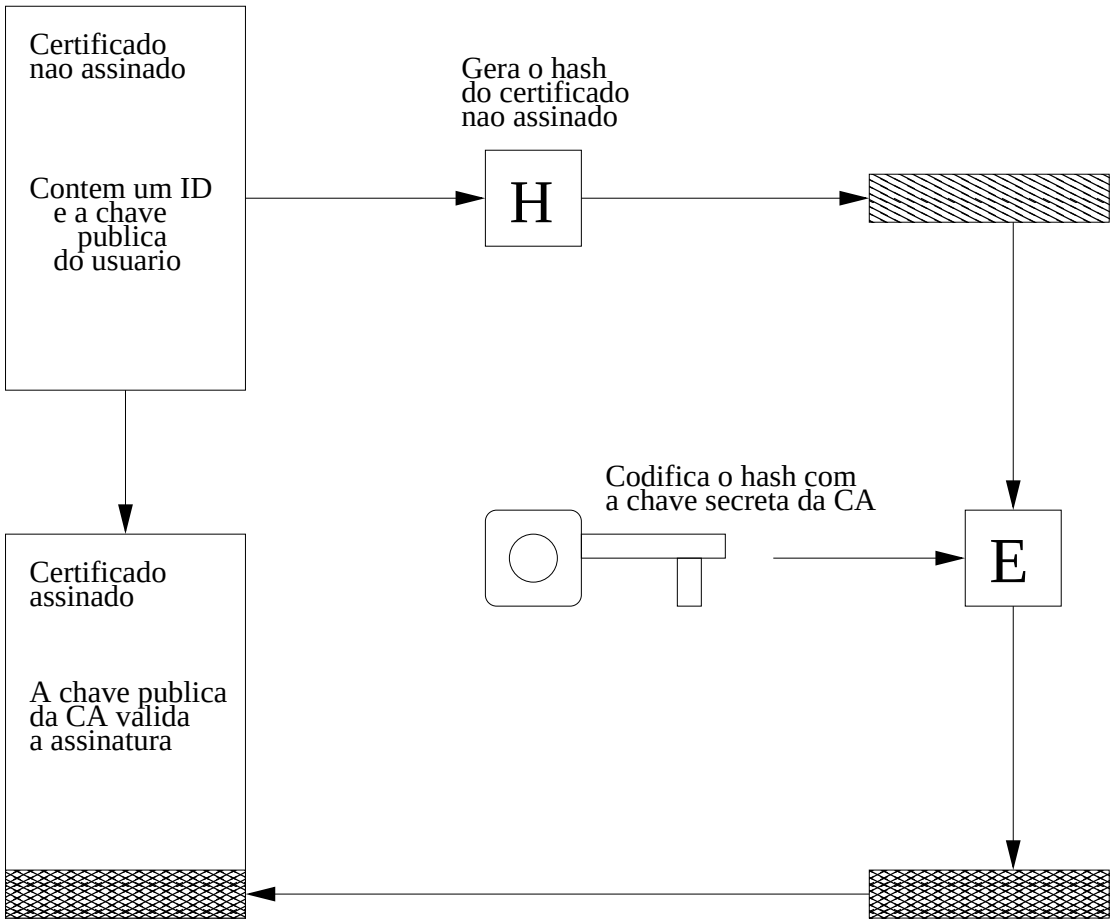


Figura 2.3: Emissão de um certificado

Authority) que o emitiu a pedido de um usuário. A figura 2.3 ilustra a construção de um certificado. Nas redes veiculares, cada veículo produzido é registrado por uma CA, de modo a receber uma identidade única, ou seja, um par de chaves público/privada. Para revogar certificados, de modo a excluir um dado usuário da rede veicular, listas de certificados revogados podem ser usadas. Estas listas podem ser difundidas pela infraestrutura ao longo das pistas.

Uma entidade, como um nó veicular, quando recebe uma mensagem assinada e com um certificado digital em anexo a esta, adota o seguinte procedimento. De posse da chave pública da CA, que é conhecida por todos os membros da comunicação, ocorre, primeiramente, a validação do certificado recebido. Uma vez que o certificado tenha sido validado, tem-se a certeza de que a entidade autora declarada neste é um membro válido

da comunicação. O passo seguinte é verificar se a chave pública deste membro faz parte de uma lista de certificados revogados [45]. Em seguida, caso a chave não esteja nesta lista negra, pode-se utilizá-la para realizar a validação da assinatura digital da mensagem recebida.

2.2.7 Infraestrutura de Chaves Públicas

Uma infraestrutura de chaves públicas é um órgão ou iniciativa pública ou privada que tem como objetivo manter uma estrutura de emissão de chaves públicas. Este sistema se baseia no princípio da terceira parte confiável para oferecer uma mediação de credibilidade e confiança em transações entre partes que utilizam certificados digitais.

Devido ao grande número de veículos registrados em países diferentes e que viajam longas distâncias, para além de suas regiões de registro, faz-se necessária uma solução para distribuição e gerenciamento de chaves e certificados que seja extensível [46]. Cada CA possui uma região de domínio (cidade, estado, país etc.) e gerencia as identidades de todos os nós nela registrados. Para possibilitar a interação entre nós de domínios diferentes, as CAs fornecem certificados umas as outras ou fornecem certificados "estrangeiros" aos veículos que são registrados em outras CAs quando estes atravessarem os limites do domínio onde são registrados [12]. Deste modo, o projeto de um mecanismo para distribuir chaves e listas de certificados revogados em uma rede que se espalha por todo o mundo é um desafio por si só.

Uma solução que leve em consideração tanto aspectos técnicos quanto políticos é um pré-requisito para este sistema. Provavelmente, a participação de autoridades governamentais no processo de registro de veículos implicará em um certo grau de centralização que contribuirá para a solução deste desafio. Além das entidades governamentais, outro candidato para o papel de autoridade certificadora são os fabricantes de veículos. Em qualquer um dos casos, as autoridades certificadoras precisam reconhecer umas às outras, mesmo em diferentes países, para que veículos de lugares diferentes ou de fabricantes diferentes possam se autenticar entre si.

2.3 SOLUÇÕES PARA PRIVACIDADE DE LOCALIZAÇÃO

Embora as soluções que asseguram os serviços apresentados na subseção 2.2 sejam igualmente importantes, a garantia de privacidade de localização é o único serviço não assegurado pela arquitetura WAVE. Deste modo, esta subseção apresenta soluções encontradas na literatura.

2.3.1 Servidores de Anonimato

Um servidor de anonimato oferece privacidade de localização por meio de serviços como k-anonimato de informações de localização por meio de camuflagem espaço-temporal [47, 48]. A camuflagem temporal refere-se ao reposicionamento de um ponto em um determinado momento, por um intervalo de tempo com k pontos, incluindo o ponto que está sendo camuflado pelo servidor. Do mesmo modo, a camuflagem espacial refere-se ao reposicionamento de um ponto no espaço por um intervalo espacial maior que contenha k nós móveis. Deste modo, o nó camuflado não consegue ser distinguido em um conjunto de k nós móveis. Entretanto, este modo de obtenção de anonimato é impróprio para as aplicações de segurança do trânsito, visto que tais aplicações requerem informações precisas de localização.

2.3.2 Assinatura de Grupo

Um esquema de assinatura de grupo permite aos membros de um grupo assinar mensagens em nome deste grupo. Assim, a assinatura pode ser verificada através da chave pública do grupo e esta não revelará a identidade do assinante nem permitirá que este seja rastreado. Além disso, não é possível saber se duas assinaturas diferentes foram emitidas pelo mesmo membro do grupo. Para garantir a irretratabilidade, o esquema permite que o gerenciador do grupo, uma terceira parte confiável, possa abrir a assinatura e revelar a identidade do membro do grupo, caso necessário.

Assinaturas de grupo foram primeiramente propostas por Chaum e Heyst [49]. Entretanto, o esquema original requer que a assinatura de grupo seja linear no tamanho do grupo. Recentemente, em muitos esquemas propostos, o tamanho da assinatura independe do tamanho do grupo. A "assinatura de grupo curta" proposta por Boneh, Boyen e Shacham [50] é a que possui a menor, mais eficiente e mais segura assinatura entre estes esquemas, de modo que esta assinatura resulta em 192 bytes e atende às restrições temporais exigidas por aplicações de segurança do trânsito. Consequentemente, esta solução tem sido explorada por diversos autores na comunidade científica [51, 52, 53, 54].

Entretanto, embora esta aparente ser a melhor solução para o desafio de prover privacidade na comunicação veicular, ela possui a desvantagem de ser pouco extensível. No esquema de assinatura de grupos, o grupo criado por seu gerenciador é sempre fixo e uma grande sobrecarga resulta da necessidade de se remover um membro deste grupo. Para tanto, há duas soluções comumente consideradas. Uma destas se baseia na atualização das chaves. Esta solução consiste em gerar uma nova chave secreta para todos os membros do grupo, excetuando-se o membro revogado, e uma nova chave pública do grupo. A desvantagem desta é a sobrecarga na comunicação para distribuição de novas chaves. Uma outra solução considera uma lista de revogados, semelhante a que é utilizada em uma infraestrutura de chaves públicas. Deste modo, por meio destas listas pode-se verificar se o membro é válido ou foi revogado. A desvantagem deste método é que o número de verificações nesta lista cresce linearmente com o número de membros revogados, e cada uma destas comparações é muito mais custosa para o esquema de assinatura de grupo, quando comparada às realizadas em uma lista de certificados revogados utilizada em uma infraestrutura de chaves públicas. Um esquema misto é apresentado por Xiaodong Lin *et al* [55], onde as listas de revogados são utilizadas até que estas alcancem um tamanho preestabelecido, a partir de quando se utiliza o método de atualização das chaves. Entretanto, estes trabalhos não demonstraram que este esquema é suficientemente estensível para VANETs.

2.3.3 Soluções Baseadas em Pseudônimos

Embora o uso de certificados ofereça muitos benefícios para a autenticação dos membros da comunicação, faz-se necessário um meio de esconder a identidade do dono deste certificado para que seja assegurado o princípio da privacidade. Ao mesmo tempo, deve-se garantir também o princípio da irretratabilidade.

Uma resposta para este desafio é um esquema baseado no uso de identidades temporárias autenticáveis, os pseudônimos [19, 56]. Esta alternativa exige que cada nó veicular seja equipado com um conjunto de certificados, um para cada pseudônimo, que deve ser emitido por uma terceira parte confiável, como uma CA em uma PKI. Uma vez que apenas a entidade que emitiu o pseudônimo pode revelar a identidade do nó veicular correspondente, os requisitos de privacidade e irretratabilidade são endereçados ao mesmo tempo.

Inicialmente, foi proposto por Raya e Hubaux [19] o uso de um esquema onde pseudônimos devem ter um tempo de validade curto e devem ser mudados continuamente [19]. A mudança de pseudônimo significa, na prática, a mudança do par de chaves pública/privada utilizado no mecanismo de assinatura digital e a mudança dos endereços do nó veicular em todas as camadas da pilha de rede [57]. Os pseudônimos devem ser mudados continuamente, pois caso um atacante consiga desvendar a identidade por trás de um nó veicular, a mudança contínua poderia preservar a privacidade deste. O uso de pseudônimos com curta validade objetiva também facilitar o processo de revogação. Quando a validade do conjunto de pseudônimos expirar, o nó deve requisitar da PKI um novo conjunto de pseudônimos. Deste modo, para excluir um membro da comunicação, basta que a infraestrutura negue atendimento ao nó que será revogado.

Entretanto, um atacante pode derivar, por meio de equações cinemáticas, a próxima posição de qualquer nó veicular utilizando as informações de posição, velocidade e direção, emitas periodicamente por estes, de modo a correlacionar diferentes pseudônimos utilizados por um mesmo nó. Consequentemente, a privacidade de localização de um nó pode ser violada e sua identidade revelada através do mapeamento de suas localizações [58, 20].

Desde então, a comunidade científica tem apresentado diversos trabalhos para assegurar a privacidade de localização dos participantes da comunicação veicular.

No esquema AMOEBA [59], para mitigação de ataques à privacidade de localização, foi proposto o uso de um período de silêncio aleatório após a atualização de um pseudônimo. Deste modo, quando um grupo de nós mudam seus pseudônimos, a variação dos estados destes durante um período silencioso possibilita descorrelacionar a identidade destes de suas respectivas localizações. Entretanto, o uso deste método para alcançar privacidade implica em um incremento do risco de acidentes pois tais períodos violam os requisitos das aplicações de segurança do trânsito.

No modelo "*mix-context*" [60], um nó muda seu pseudônimo quando se encontra em torno de um número mínimo de outros nós com estado semelhante. Esta abordagem é estendida por Jianxiong Liao e Jianqing Li [61], os quais elaboraram o "Algoritmo Síncrono de Mudança de Pseudônimos". Este algoritmo aumenta a probabilidade de que k nós com estados semelhantes mudem seus pseudônimos ao mesmo tempo. No entanto, a eficácia de tal abordagem contra um ataque capaz de correlacionar pseudônimos por meio de algum modelo analítico baseado em equações cinemáticas que utiliza as informações de estado disseminadas pelos veículos é desconhecida.

Em [62, 21], foi proposto por Beresford o conceito de "*mix-zone*", que são regiões onde nós anônimos podem alterar seus identificadores de um modo que impossibilita ataques de rastreamento. Em [63], Joo-Han Song *et al.* propuseram uma abordagem onde um nó muda o seu pseudônimo somente se encontrar um número mínimo de nós na *mix-zone*, de modo a reduzir a probabilidade de sucesso de um ataque de rastreamento que correlacione informações de veículos entrando e saindo de tais regiões. Embora estes trabalhos se baseiem no conceito de *mix-zones*, a primeira solução que descreve um meio para implantação desta abordagem em VANETs foi apresentada por Freudiger *et al.* [5], o qual descreve o protocolo CMIX, que significa *Cryptographic MIX-zones*. Neste protocolo, quando um nó entra em uma *mix-zone*, este recebe uma chave secreta de grupo, enviada pela RSU que gerencia esta *mix-zone*. Esta chave é usada dentro da *mix-*

zone para codificar as mensagens periódicas que informam o estado dos nós veiculares. Esta chave é compartilhada apenas com membros autenticados da VANET. No entanto, a codificação destas mensagens por meio de uma chave compartilhada torna esta solução vulnerável a ataques de um nó malicioso interno à VANET. Deste modo, embora as *mix-zones* baseadas no CMIX evitem ataques provindos de fora da rede de comunicação veicular, elas são vulneráveis a ataques internos. Caso um atacante disponha de um dispositivo válido na comunicação veicular em cada *mix-zone*, ele conseguirá correlacionar os pseudônimos mudados nestas regiões e, assim, violar a privacidade de localização de todos os usuários. Até onde sabemos, tal vulnerabilidade ainda não foi tratada em outros trabalhos apresentados pela comunidade científica. Assim, uma nova abordagem para tratar esta vulnerabilidade é apresentada neste trabalho, de modo a aumentar o nível de privacidade de localização que as *mix-zones* podem oferecer.

CAPÍTULO 3

PRIVACIDADE DE LOCALIZAÇÃO EM MIX-ZONES

É apresentada neste capítulo uma abordagem para tratar a vulnerabilidade das *mix-zones* a ataques internos, de modo a aumentar o nível de privacidade de localização oferecido por estas regiões. Entretanto, a abordagem apresentada implica em uma sobrecarga na quantidade de comunicação como efeito colateral. Para resolver esta desvantagem, são empregados mecanismos que permitem reduzir a quantidade de tráfego proveniente das mensagens periódicas relacionadas à segurança do trânsito, sem, entretanto, afetar esta.

Este capítulo está estruturado do seguinte modo. O modelo geral do sistema de comunicação veicular adotado é descrito na seção 3.1. O protocolo CMIX, base de construção das *mix-zones* criptográficas, é descrito na seção 3.2. A seção 3.3 apresenta a solução proposta neste trabalho e descreve um modelo analítico de ataque que permite avaliar o nível de privacidade de localização por esta oferecido.

3.1 MODELO DO SISTEMA

Esta seção apresenta o modelo geral adotado. A subseção 3.1.1 apresenta os principais pressupostos assumidos no ambiente de comunicação veicular. Por meio destes, são assegurados os diversos requisitos de segurança apresentados no capítulo 2. Estes pressupostos são comuns em trabalhos relacionados [5, 63, 58, 12] e não limitam a abrangência da solução proposta. A subseção 3.1.2 descreve um modelo de *mix-zone*. Os tipos de atacantes considerados na avaliação da solução proposta são descritos na subseção 3.1.3.

3.1.1 Pressupostos Básicos

Primeiramente, no que se refere às unidades de bordo e de acostamento, é assumido que tais dispositivos são invioláveis quanto a roubo de identidade e alteração de mensagens construídas dentro destes. Este pressuposto é muito importante para a proposta apresentada, pois esta depende de um elemento centralizador da comunicação que deve ser confiável, a RSU gerenciadora de *mix-zones*. Deste modo, é assumido que uma entidade de confiança (por exemplo, o governo) controla todas as unidades de acostamento e não permite invasões ou violações às unidades que gerenciam alguma *mix-zone*.

Por meio de sensores e de um GPS equipados nos veículos, as OBUs transmitem periodicamente mensagens de estado, que contêm posição, velocidade e direção do nó veicular. Neste trabalho, é assumido que o meio de comunicação é confiável, ou seja, não há perda de mensagens. Estas mensagens são assinadas com um pseudônimo do nó veicular e o certificado correspondente a este pseudônimo é anexado. A assinatura digital e o certificado anexado a cada mensagem garantem autenticação, irretratabilidade e verificação de integridade. Para questões legais de responsabilização, a identidade por trás de um pseudônimo apresentado pode ser revelada pela autoridade certificadora que o emitiu.

Uma PKI confiável deve estar presente nas VANETs. Para isto, as CAs são operadas por organizações governamentais e / ou fabricantes de automóveis, que operam em conformidade com políticas de privacidade que preservam o sigilo dos pseudônimos. Antes de entrar na rede, cada nó i recebe uma identidade de longo prazo emitida por uma CA. O nó veicular usa esta identidade, periodicamente, para solicitar um conjunto de pseudônimos a um Provedor de Pseudônimo (PP). Para cada pseudônimo $P_{i,k}$, onde $k \in \{1, ..., Z\}$ e Z é o tamanho do conjunto, são gerados um par de chaves público / privada $(K_{i,k}, K_{i,k}^{-1})$ e um certificado correspondente $Cert_{i,k}(K_{i,k})$.

Para evitar que um nó malicioso utilize seu conjunto de pseudônimos para realizar um tipo de ataque em que este responde por múltiplas identidades, conhecido como "ataque Sybil", pode-se utilizar soluções encontradas na literatura [64]. Limitar a validade de

cada pseudônimo para um dia e horário único e o seu prazo para um período curto (e.g., 1 minuto) também é um modo de impedir tais ataques, pois o uso de mais de uma identidade em um dado instante será facilmente verificado por meio da validade deste. Atacantes identificados devem ser impedidos de adquirir novos pseudônimos nos PPs. Para isto, a identidade de longo prazo destes deve ser acrescentada em listas de membros revogados compartilhadas pelos PPs.

3.1.2 Modelo de Mix-Zone

Mix-zones são regiões de anonimato que visam a impedir a correlação de pseudônimos utilizados, consecutivamente, pelo mesmo nó. A eficácia destas regiões no fornecimento de privacidade de localização depende da densidade de veículos e da imprevisibilidade do percurso destes. Dentro destas zonas, localizadas em pontos predeterminados, deve ocorrer a mudança de pseudônimo. Uma vez que uma maior mistura de veículos ocorre nos cruzamentos rodoviários, onde a velocidade e a direção dos veículos mudam com maior frequência, esta é a melhor localização para as *mix-zones* [5]. A figura 3.1 apresenta um exemplo de uma *mix-zone* com quatro entradas e quatro saídas. Uma RSU com alcance de transmissão R_{RSU} gerencia esta *mix-zone*, cujo raio é definido como R_{mz}.

3.1.3 Tipos de Atacantes

Considera-se externo o atacante que escuta passivamente a comunicação provinda das *mix-zones*, mas não é capaz de decodificar as mensagens transmitidas nestas regiões, por não ter acesso à chave secreta de grupo nela utilizada. A proteção oferecida pelas soluções existentes, baseadas em *mix-zones*, visam a impedir a exposição da localização dos nós veiculares contra estes atacantes. O atacante interno, por outro lado, possui um dispositivo de comunicação que é válido na VANET. Deste modo, este tipo de atacante é capaz de obter a chave secreta de grupo usada em qualquer *mix-zone* e, deste modo, ter acesso às informações de estado disseminadas pelos nós veiculares no interior destas.

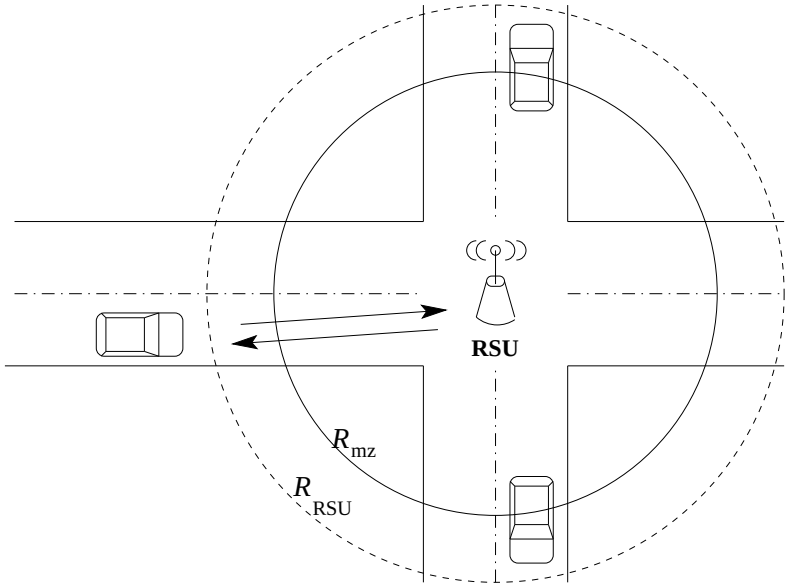


Figura 3.1: Exemplo de uma *mix-zone* com quatro entradas e quatro saídas.

Assegurar a privacidade de localização dos nós veiculares contra este tipo de atacante é o objetivo da proposta apresentada neste trabalho.

Em relação à abrangência da área de atuação de um atacante na VANET, este pode ser local ou global. A ação do atacante local é restrita a locais específicos, como as *mix-zones*, enquanto o atacante global é assumido estar presente em todos os pontos. Nas simulações apresentadas no capítulo 4, um atacante interno local é considerado no primeiro cenário de avaliação e um atacante interno global no segundo.

3.2 O PROTOCOLO CMIX

Esta seção apresenta como o protocolo CMIX é utilizado nas *mix-zones*. Por meio do protocolo CMIX, regiões anonimizantes (mix-zones) são formadas. Nestas regiões, os usuários podem mudar de pseudônimos para dificultar a ação de atacantes que estejam monitorando a comunicação para rastreá-los. Este trabalho visa aumentar a privacidade de localização em redes veiculares baseadas no CMIX.

Quando um nó veicular entra em uma *mix-zone*, a RSU que a gerencia inicia um

mecanismo para autenticar este nó e compartilhar a chave de grupo secreta da *mix-zone* [5]. A RSU anuncia sua presença através de *beacons* transmitidos periodicamente, os quais informam a localização e o raio R_{mz} que delimita a *mix-zone* (ver figura 3.1). Tão logo um veículo i entra no alcance de transmissão da RSU, este inicia o protocolo de negociação de chave apresentado na tabela 3.1.

Tabela 3.1: O protocolo de negociação de chave [5]. $Sign()$ é a assinatura da mensagem, $Cert$ é o certificado do remetente da mensagem. E indica uma operação de cifragem.

$i \rightarrow$ RSU:	Request, T_s, $Sign_i$ (Request, T_s), $Cert_{i,k}$
RSU $\rightarrow i$:	$E_{K_{i,k}}$ (i, S, T_s, $Sign_{RSU}$ (i, S, T_s)), $Cert_{RSU}$
$i \rightarrow$ RSU:	Ack, T_s, $Sign_i$(Ack,T_s), $Cert_{i,k}$

Primeiramente, um nó veicular i envia uma mensagem requisitando a chave de grupo da *mix-zone*. Esta mensagem é assinada com seu pseudônimo e o correspondente certificado é enviado também. Em seguida, a RSU verifica a mensagem recebida e autentica este nó. Caso este seja um nó válido, a RSU responde com uma mensagem assinada contendo a chave de grupo S da *mix-zone*, codificada pela chave pública de i. Por fim, i valida a mensagem recebida e responde com uma mensagem de confirmação. Um marcador temporal T_s é adicionado a estas mensagens para evitar ataques de repetição.

A chave S deve ser usada para codificar todas os *beacons* de segurança difundidos por i, tão logo este entre na região da *mix-zone* definida por seu raio. Para aumentar a segurança da *mix-zone*, caso sua chave secreta seja comprometida, uma atualização desta chave deve ocorrer regularmente. Uma vez que esta atualização pode gerar uma grande sobrecarga na comunicação, é preferível que ocorra quando a *mix-zone* estiver vazia.

Conforme descrito anteriormente, esta solução é efetiva apenas contra um atacante externo. Deste modo, uma nova solução precisa ser desenvolvida para impedir ataques internos.

3.3 SOLUÇÃO PARA A VULNERABILIDADE DO CMIX

Um modo de evitar a ação do atacante interno é fazer com que o acesso às mensagens de estado difundidas por um nó limite-se aos correspondentes vizinhos deste. Por meio deste procedimento, a ação do atacante é suficientemente dificultada. Um modo de realizar esta abordagem é fazer com que cada nó transmita suas mensagens diretamente aos nós vizinhos. Para isto, as mensagens transmitidas deveriam ser codificadas com as chaves públicas destes vizinhos, de modo que seria necessário transmitir a mesma mensagem diversas vezes, codificada por meio de chaves diferentes. Infelizmente, este procedimento é muito custoso. Primeiramente, devido ao tamanho de cada mensagem (251 bytes no padrão WAVE, dos quais 125 bytes correspondem ao certificado, 56 bytes à assinatura e 43 bytes, no máximo, às informações de estado), de modo que um nó com muitos vizinhos iria consumir muito mais da banda de comunicação. Outro fator é o custo relacionado às operações de codificação e decodificação por meio de criptografia de chave assimétrica, que é da ordem de mil vezes maior que o da criptografia simétrica [65], de modo que os requisitos temporais das aplicações de segurança do trânsito poderiam ser violados.

Outra forma de resolver este problema é direcionar as mensagens de estado para a RSU que gerencia a *mix-zone*, a qual pode encaminhar as informações de estado recebidas dos nós veiculares para os correspondentes vizinhos destes. Uma vez que a comunicação entre a RSU e os nós veiculares pode ocorrer por meio de uma comunicação secreta, codificada por chave simétrica, a desvantagem dos custos devido às operações de codificação e decodificação são mínimas e pouco impactam nas restrições temporais das aplicações de segurança no trânsito. Deste modo, adotando tal solução, faz-se necessário incluir no protocolo de negociação de chave, uma outra chave secreta, diferente para cada nó veicular, que será usada para codificar a comunicação entre este e a RSU. A tabela 3.2 apresenta a modificação necessária no protocolo de negociação de chave.

Nesta nova versão, a chave C_i foi incluída na mensagem transmitida pela RSU (segunda mensagem da tabela 3.2). Quando a RSU encaminhar as informações de estado

Tabela 3.2: O protocolo de negociação de chave estendido. $Sign()$ é a assinatura da mensagem, $Cert$ é o certificado do remetente da mensagem. E indica uma operação de criptografia.

$i \rightarrow$ RSU:	Request, T_s, $Sign_i$ (Request, T_s), $Cert_{i,k}$
RSU $\rightarrow i$:	$E_{K_{i,k}}$ (i, S, C_i, T_s, $Sign_{RSU}$ (i, S, C_i, T_s)), $Cert_{RSU}$
$i \rightarrow$ RSU:	Ack, T_s, $Sign_i$(Ack,T_s), $Cert_{i,k}$

de um nó veicular para um vizinho j deste, a correspondente chave C_j deve ser usada para codificar a mensagem com as informações encaminhadas. O tamanho desta mensagem é menor, pois a RSU não precisa assiná-las digitalmente e, consequentemente, um certificado digital também não é necessário. Os nós veiculares, por sua vez, continuam utilizando a chave S para codificar e difundir seus *beacons*. Entretanto, um nó i deve codificar as informações de estado em suas mensagens por meio da correspondente chave C_i, para que apenas a RSU possa decodificar esta parte da mensagem. Outras informações presentes na mensagem, que sejam de interesse geral para as aplicações de segurança, por exemplo, um marcador temporal, podem ser decodificadas por meio da chave S.

Entretanto, esta abordagem implica em uma sobrecarga na comunicação, que varia segundo o número médio de vizinhos de cada nó veicular, para os quais a RSU deve enviar uma mensagem. Deste modo, mecanismos são necessários para reduzir o impacto desta desvantagem, de modo a tornar esta solução viável. Um modo de reduzir esta sobrecarga é usar um mecanismo que permita reduzir a quantidade de comunicação necessária para a garantia de segurança do trânsito.

Dois mecanismos para redução de comunicação são descritos na subseção 3.3.1, assim como a implementação destes nas *mix-zones* de modo que atenda à solução proposta para impedir ataques internos. Na subseção 3.3.2, uma análise da segurança e da eficiência da solução proposta é apresentada. Na subseção 3.3.3, um modelo analítico de ataque foi desenvolvido para possibilitar o estudo do nível de privacidade de localização fornecido por esta solução. O modelo desenvolvido permite descobrir a taxa de sucesso de um atacante interno em seu intento de rastrear o percurso dos usuários em uma *mix-zone*.

3.3.1 Mecanismos para Redução de Comunicação

Uma solução, descrita por Shahram Rezaei *et al* [4], emprega um esquema onde um nó veicular i utiliza um modelo analítico baseado em equações cinemáticas para estimar as informações de estado de nós vizinhos. Estes últimos, por sua vez, somente disseminam suas informações de estado a partir do momento em que detectam que as equações utilizadas por i produzirão resultados que extrapolam o erro aceitável na estimativa da futura posição destes. Consequentemente, a quantidade de comunicação pode ser consideravelmente reduzida, sem afetar a segurança do trânsito.

Uma vez que os nós veiculares sejam capazes de prever o estado futuro de seus vizinhos, considerando uma margem de erro aceitável, o número de *beacons* disseminados para promover a segurança do trânsito pode ser reduzido consideravelmente. Para tanto, o conjunto de equações do modelo utiliza como entrada as informações de estado recebidas de um nó veicular e produz uma previsão dos próximos estados deste ao longo do tempo. Uma vez que um nó pode aplicar a este modelo as informações de seu próprio estado, este nó saberá a partir de quando seus futuros estados produzidos pelas equações computadas por seus vizinhos produzirão saídas que ultrapassam a margem de erro aceitável. Somente então, novos *beacons* são disseminados para que os vizinhos deste possam produzir previsões atualizadas dos estados futuros deste nó. Os valores utilizados para definir o erro aceitável para as informações de posição, velocidade e ângulo de direção podem ser encontrados no trabalho de Shladover e Tan [66]. A figura 3.2 mostra o diagrama de blocos deste esquema.

Conforme mostra a figura, cada veículo possui um componente chamado "Autoestimador", o qual é usado para gerar suas informações de estado. Para isto, o Autoestimador utiliza informações provenientes de um GPS e de sensores do veículo. O conjunto de informações de estado de um veículo é representado pelo vetor $\overrightarrow{X}_i(t)$, o qual é a melhor estimativa do estado de um veiculo i no instante t.

Os componentes do tipo "Estimador de Vizinho" (EV) são responsáveis por estimar os estados futuros dos n vizinhos de um nó veicular i. Para isto, este tipo de estimador

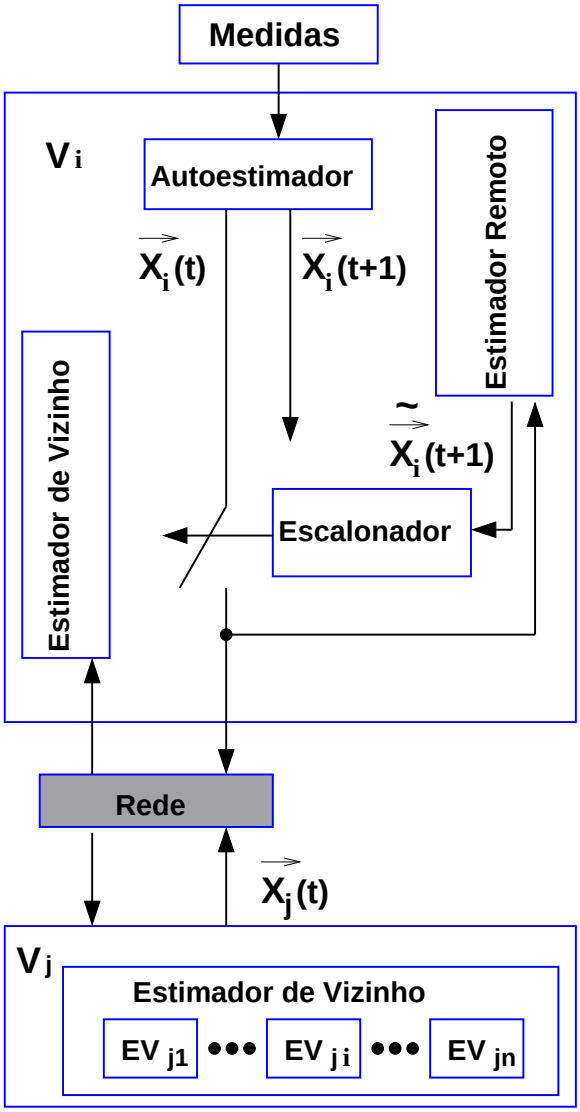


Figura 3.2: Diagrama de blocos do mecanismo para redução de comunição. [4]

recebe como entrada o estado $\overrightarrow{X}_j(t)$ de cada vizinho j, para $1 \leq j \leq n$, e produz como saída o estado $\widetilde{\overrightarrow{X}}_j(t+1)$, que representa a estimativa do estado de j no período seguinte. A notação $\overrightarrow{X}$ está sendo utilizada aqui para representar estados calculados pelo Autoestimador, enquanto a notação $\widetilde{\overrightarrow{X}}$ é usada para estados estimados em outras componentes. As equações utilizadas para computar os estados estimados são conforme as descritas em um modelo simplificado apresentado em 1 [4].

$$
\begin{aligned}
\widetilde{X}(t+1) &= \widetilde{X}(t) + \widetilde{V}(t) \times cos(\widetilde{\phi}(t)) \times \Delta T; \\
\widetilde{Y}(t+1) &= \widetilde{Y}(t) + \widetilde{V}(t) \times sin(\widetilde{\phi}(t)) \times \Delta T; \\
\widetilde{V}(t+1) &= \widetilde{V}(t); \\
\widetilde{\phi}(t+1) &= \widetilde{\phi}(t) + \widetilde{\dot{\phi}}(t) \times \Delta T; \\
\widetilde{\dot{\phi}}(t+1) &= \widetilde{\dot{\phi}}(t);
\end{aligned}
\tag{1}
$$

No modelo acima, $\widetilde{X}$ e $\widetilde{Y}$ representam as posições no plano XY, $\widetilde{V}$ representa a velocidade, $\widetilde{\phi}$ o ângulo da direção seguida pelo veículo e $\widetilde{\dot{\phi}}$ a taxa de variação deste ângulo. Quando um nó veicular recebe mensagens contendo o estado de um vizinho, as equações do modelo são atualizadas com estas informações e os resultados são utilizados pelas aplicações de segurança do trânsito para evitar colisões. A primeira estimativa considera o atraso δ relativo ao tempo necessário para que uma mensagem enviada por um nó seja recebida pelos seus vizinhos. Este valor pode ser calculado pela RSU e acrescido às informações encaminhadas ou pode ser calculado pelo receptor se houver uma referência temporal compartilhada pelos veículos. Em seguida, os estados futuros dos nós vizinhos são estimados a cada período ΔT, até que novas informações sejam recebidas. Seja $\delta = 2ms$ e as informações de estado $X = 10m$, $Y = 20m$, $V = 16m/s$, $\phi = 0°$ e $\dot{\phi} = 0$ transmitidas por um nó em um período t_o. Os vizinhos deste, ao receber a mensagem de estado encaminhada pela RSU, estimarão os seguintes valores por 1:

$$
\widetilde{X} = 20,032m; \qquad \widetilde{Y} = 20m; \qquad \widetilde{V} = 16m/s; \qquad \widetilde{\phi} = 0°; \qquad \widetilde{\dot{\phi}} = 0;
$$

Estes resultados mostram que o veículo deslocou-se 32 cm no eixo X. Estes valores são utilizados como base para as estimativas do estado deste veículo nos próximos períodos de comunicação. Seja $\Delta T = 100ms$, o estado estimado para o período seguinte $(t_o + 1)$ resulta em:

$$\widetilde{X} = 20,8m; \qquad \widetilde{Y} = 20m; \qquad \widetilde{V} = 16m/s; \qquad \widetilde{\phi} = 0°; \qquad \widetilde{\dot{\phi}} = 0;$$

Enquanto um EV estima os próximos estados de vizinhos, o papel do "Estimador Remoto" (ER) em um nó i é derivar o estado deste nó estimado pelos seus vizinhos, ao longo do tempo. Seja ER_i o Estimador Remoto de i e EV_{ji} um Estimador de Vizinho no veículo j que estima os estados de i. O propósito de ER_i é estimar a saída produzida por todo EV_{ji}, para $1 \leq j \leq n$.

Comparando as saídas do ER e do Autoestimador, i sabe o quão próximo as estimativas dos seus vizinhos estão de seu real estado. Esta é a função do componente "Escalonador". Quando este detecta que o erro estimado por seus vizinhos ultrapassará um determinado valor limite, a transmissão do estado $\overrightarrow{X}_i(t)$ é acionada para que o estado estimado de i, em seus vizinhos, não ultrapasse o erro limite no período seguinte.

Entretanto, para que este mecanismo satisfaça os requisitos da solução proposta para assegurar a privacidade dos nós veiculares contra ataques internos à *mix-zone*, mudanças neste mecanismo precisam ser realizadas para que o tráfego de comunicação de segurança do trânsito flua, primeiramente, pela RSU que gerencia a *mix-zone*. A figura 3.3 apresenta as modificações necessárias. O bloco RSU foi acrescentado para gerenciar o tráfego da comunicação de segurança do trânsito. Todos os nós na *mix-zone* devem transmitir suas mensagens de estado tão somente para a RSU. Esta possui um Estimador de Vizinho para todos os nós veiculares na *mix-zone*. Por meio destes estimadores, a RSU conhece a localização de todos os nós veiculares em sua região. Deste modo, a RSU pode computar o conjunto de nós vizinhos de cada um destes. Para isto, uma determinada distância limite d é considerada para o cálculo deste conjunto de vizinhos, de modo que veículos que estejam a uma distância de d metros, um do outro, são considerados veículos vizinhos. Quando a RSU recebe uma mensagem de um nó i, a informação de estado $\overrightarrow{X}_i(t)$ deste nó é obtida decodificando esta parte da mensagem por meio da chave C_i. Em seguida, a RSU encaminha este estado para todos os nós no conjunto de vizinhos de i, codificando

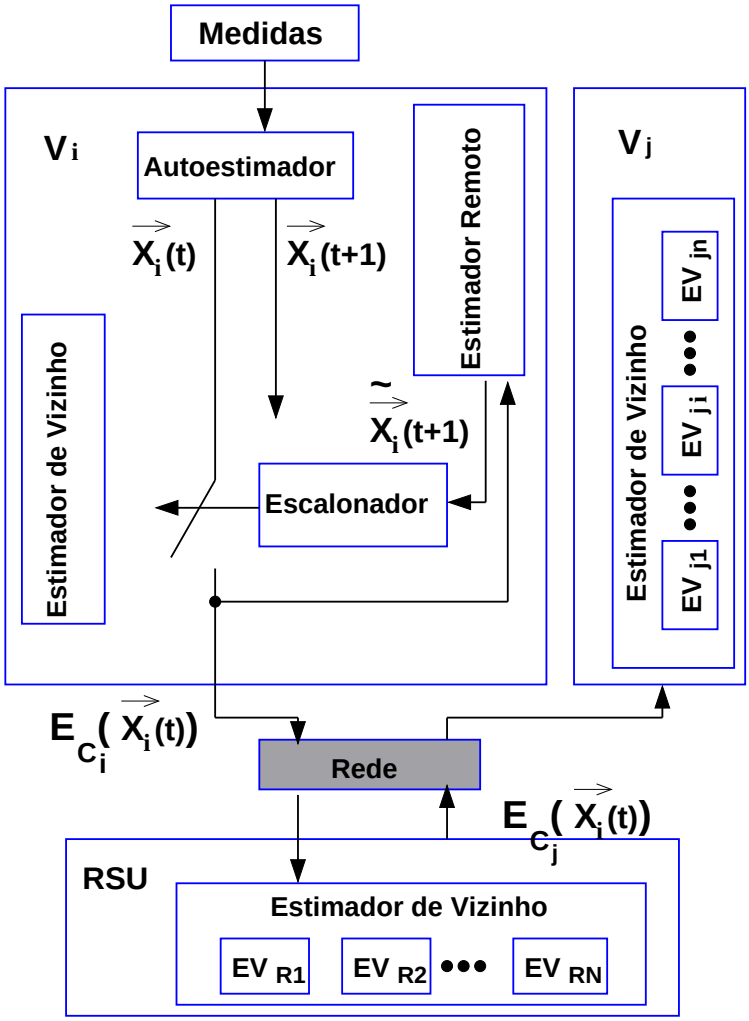
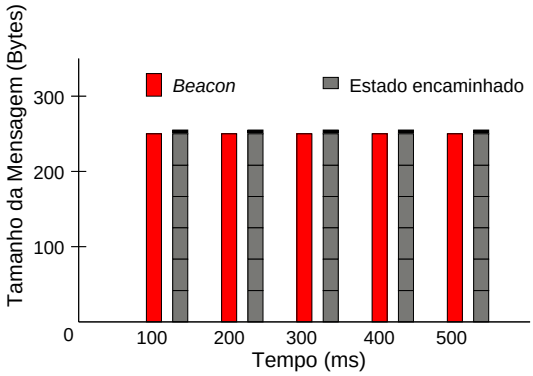


Figura 3.3: Diagrama de blocos modificado.

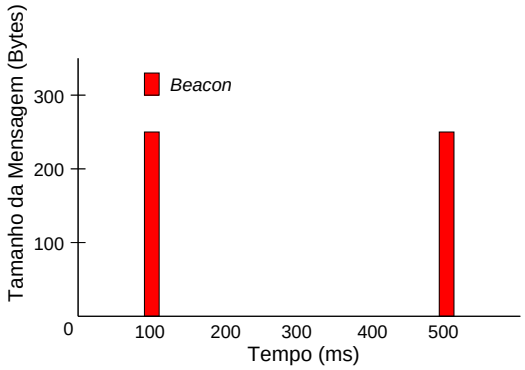
cada mensagem por meio da correspondente chave secreta destes.

Um segundo mecanismo foi utilizado para reduzir o número de mensagens geradas devido ao processo de encaminhamento das informações de estado. Este segundo mecanismo consiste em utilizar o processo de encaminhamento apenas para nós veiculares nos caminhos de saída da *mix-zone*. Deste modo, a sobrecarga gerada pelas mensagens do processo de encaminhamento é evitada nos caminhos de entrada e os nós veiculares ainda estarão protegidos contra ataques internos, visto que um atacante não será capaz de descobrir o caminho de saída escolhido por um nó se este transmitir seus estados somente antes de atravessar o cruzamento de uma *mix-zone*. Assim, nos caminhos de

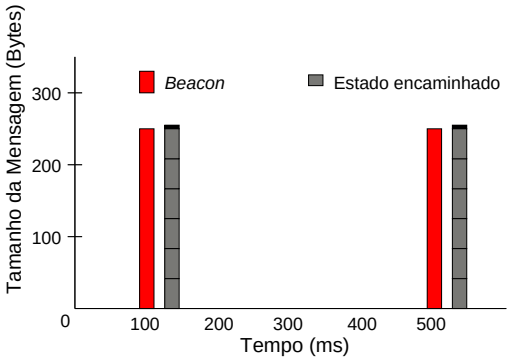
entrada, os nós veiculares utilizam os mecanismos originais do protocolo CMIX e para redução da quantidade de comunicação relativa ao número de *beacons*, de modo que o processo de encaminhamento não ocorre nesta fase. No momento em que um nó alcançar o cruzamento de uma *mix-zone*, o processo de encaminhamento começa a ser utilizado, assim como o mecanismo modificado para redução da quantidade de comunicação.



(a) Em um cenário onde apenas o processo de encaminhamento é empregado, a solução proposta se mostra inviável.



(b) Aplicação dos mecanismos de redução de comunicação nos caminhos de entrada de uma *mix-zone*. O processo de encaminhamento não é aplicado nesta fase.



(c) Aplicação dos mecanismos de redução de comunicação nos caminhos de saída de uma *mix-zone*.

Figura 3.4: Exemplos do processo de encaminhamento quando um nó possui seis vizinhos e o período é 100 ms.

3.3.2 Análise da Solução Proposta

Esta seção apresenta uma análise da eficiência dos mecanismos de redução de sobrecarga na subseção 3.3.2.1. Diversos tipos de ataques contra a solução proposta e soluções para evitá-los são descritos na subseção 3.3.2.2.

3.3.2.1 Eficiência dos Mecanismos para Redução da Sobrecarga

A figura 3.4 mostra uma avaliação do processo de encaminhamento e dos mecanismos para redução de comunicação em uma *mix-zone* onde um dado nó possui seis vizinhos. A figura 3.4a apresenta um cenário onde cada mensagem de estado produzida por um nó resulta em seis mensagens de estado encaminhadas, a cada 100 ms. Conforme pode ser constatado, se os mecanismos de redução de comunicação não forem aplicados, a abordagem proposta não será viável devido à sobrecarga na comunicação resultante do encaminhamento de estados. Por outro lado, as figuras 3.4b e 3.4c mostram o quanto a sobrecarga de comunicação é reduzida quando ambos os mecanismos são empregados. Conforme constatado na figura 3.4b, não há sobrecarga de comunicação nos caminhos de entrada da *mix-zone*, ocorre apenas redução da quantidade de comunicação. Por outro lado, quando o veículo atravessa o cruzamento de uma *mix-zone*, o processo de encaminhamento é utilizado e o seu impacto na comunicação é apresentado na figura 3.4c. Visto que a sobrecarga resultante depende do número médio de vizinhos de cada nó, uma avaliação experimental da solução proposta é apresentada no capítulo 4.

É importante notar que a sobrecarga resultante do uso de criptografia simétrica não influencia de modo significante as restrições temporais das aplicações de segurança do trânsito. Com base no uso do algoritmo criptográfico recomendado pela WAVE [67] e nos experimentos conduzidos por Wei Dai [65] para avaliar o desempenho deste, supondo um nó com seis vizinhos, podemos concluir que na abordagem proposta são gastos menos de uma dezena de microsegundos para decodificar uma mensagem de estado e para codificar uma mensagem contendo seis estados codificados com as chaves dos correspondentes

vizinhos e um marcador temporal codificado pela chave de grupo da *mix-zone*. Deste modo, pode-se estimar que esta sobrecarga é tolerável para as aplicações de segurança do trânsito.

Pode-se verificar que o erro devido à diferença entre as informações de estado transmitidas por um nó i e a variação destas durante o intervalo δ dificilmente afetará os requisitos das aplicações de segurança. Seja $\delta = 50ms$, X o eixo em que os veículos se movimentam, tal como no exemplo da subseção 3.3.1, e a aceleração / desaceleração máxima de um veículo limitada por 1 g. A primeira estimativa de um vizinho, ao receber a mensagem de estado de i, estará entre o deslocamento ΔX_a quando i utiliza aceleração máxima, e o deslocamento ΔX_{-a} quando este utiliza desaceleração máxima, de modo que o maior erro devido ao intervalo δ não pode ser maior que a diferença entre estas duas possibilidade. Seja v_o a velocidade de i ao transmitir suas informações de estado. Utilizando as equações newtonianas do movimento, tem-se que o erro será menor que [4]:

$$\begin{aligned}\Delta X_a - \Delta X_{-a} &= v_o \times (\Delta T) + \frac{a}{2} \times (\Delta T)^2 - (v_o \times (\Delta T) + \frac{-a}{2} \times (\Delta T)^2) \\ &= \frac{g}{2} \times 0.05^2 - \frac{-g}{2} \times 0.05^2 = 0,024m.\end{aligned}$$

3.3.2.2 Análise da Segurança Provida pela Solução Proposta

Como consequência da aplicação da solução proposta, considerando todos os mecanismos de otimização também propostos, a ação de um atacante interno é suficientemente limitada. Embora um atacante interno possa monitorar os nós veiculares quando estes estão em seus caminhos de entrada, um atacante não consegue determinar qual caminho de saída é escolhido por estes, pois quando passam para um caminho de saída, a comunicação das informações de estado destes se restringe aos seus vizinhos.

É possível que um atacante pare no cruzamento para tornar-se vizinho dos nós quando estes mudam para um caminho de saída, de modo a realizar um ataque à privacidade de

localização destes. Entretanto, a RSU pode evitar encaminhar as informações de estado para nós veiculares que estejam na *mix-zone* após uma determinada quantidade de tempo, o qual pode variar segundo o fluxo de trânsito desta região. Caso um veículo esteja na *mix-zone* por um intervalo de tempo maior que o estipulado, por exemplo, devido a problemas motores, as informações deste ainda serão transmitidas aos seus vizinhos para que estes evitem colisões. Deste modo, esta solução não reduz o nível de segurança do trânsito na *mix-zone*.

Existe ainda outro método de ataque interno. Uma vez que os nós veiculares assinam suas mensagens, as quais são autenticadas por meio da chave pública declarada no certificado digital anexado, caso um nó mude seu pseudônimo isoladamente em um dado período, torna-se trivial para um atacante descobrir o novo pseudônimo usado por este nó. Para realizar este ataque, o atacante compara os pseudônimos utilizados em tal período com os pseudônimos utilizados no período seguinte. Para resolver esta vulnerabilidade, basta que a RSU emita, periodicamente, mensagens requisitando a mudança simultânea de pseudônimos pelos nós veiculares na *mix-zone*.

Contudo, é possível que um atacante tente estimar a correlação entre os pseudônimos utilizados por nós veiculares que entram e saem de uma *mix-zone*, de modo a mapear com sucesso a mudança de pseudônimo destes. Para isso, algum modelo analítico baseado em equações cinemáticas pode ser usado.

3.3.3 A Operação do Atacante

Em [58], Buttyán *et al.* propuseram que um atacante pode usar eventos registrados para obter uma distribuição de probabilidade de atraso dos veículos na *mix-zone* para correlacionar os pseudônimos usados por veículos entrando e saindo desta região. Um evento é definido como uma tupla constituída por um marcador temporal e o acesso usado para entrar ou sair de uma *mix-zone*.

Seja α_{mn} a probabilidade de escolha do acesso n após um veículo entrar na *mix-zone*

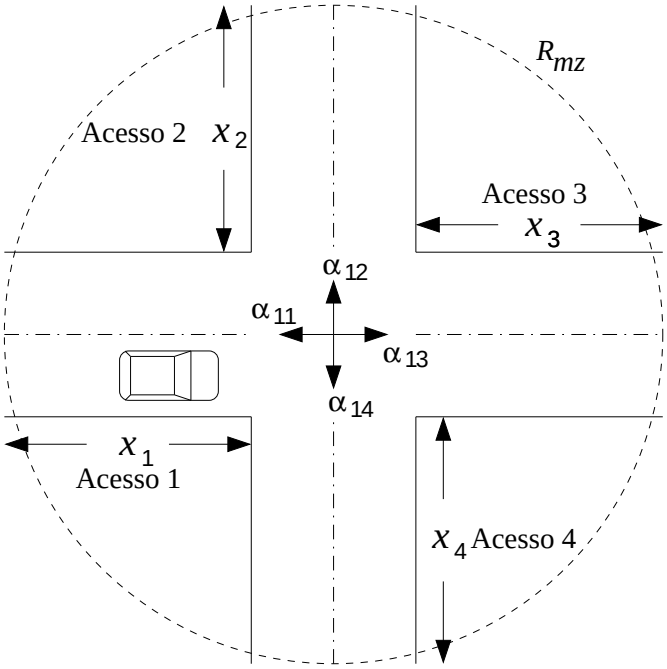


Figura 3.5: Exemplo de uma *mix-zone* com quatro acessos.

por um acesso m. Cada *mix-zone* tem D acessos e $\sum_{n=1}^{D}(\alpha_{mn}) = 1$. Na figura 3.5 é apresentado uma *mix-zone* com quatro acessos. Para efeitos de simplificação, é assumido que $\alpha_{mn} = 1/3$ para $m \neq n$ e $\alpha_{mn} = 0$ se $m = n$, de modo que nenhum veículo que entra na *mix-zone* volta pelo mesmo caminho e a probabilidade de escolha de um dos caminhos de saída é a mesma. O objetivo geral do atacante é mapear com sucesso o evento de saída S ao evento de entrada E que correlacionam com sucesso os pseudônimos utilizados por cada nó ao entrar e sair de uma *mix-zone*. Para isto, quando um nó passa pelo cruzamento de uma *mix-zone* ou sai desta, o atacante registra um evento de entrada ou um evento de saída, respectivamente. O conceito de evento pode ser expandido para incluir no evento de entrada a velocidade transmitida pelo nó veicular antes de atravessar o cruzamento, ou seja, o último estado transmitido por tal nó acessível ao atacante interno, e para incluir no evento de saída a velocidade informada pelos nós veiculares quando estes estão usando seu novo pseudônimo fora da *mix-zone*.

O atacante registra cada evento E, definido na tupla (v_i, t_i, m), onde v_i é a velocidade de um veículo que entrou por um acesso m antes de atravessar o cruzamento no instante t_i,

em uma lista L_E. Cada evento de saída é registrado na lista L_S e é definido na tupla ($v_{i'}$, $t_{i'}$, n), onde $v_{i'}$ é a velocidade informada na primeira mensagem transmitida quando o veículo i' sai da *mix-zone* por um acesso n. Para rastrear um nó, um atacante deve determinar a relação (E, S) que correlaciona com êxito o pseudônimo $P_{i,k}$ e o pseudônimo $P_{i,k'}$, usados por um nó i na entrada e na saída da *mix-zone*, respectivamente. É importante enfatizar que, como o atacante tem acesso à velocidade v_i antes de o nó atravessar o cruzamento, este modelo de ataque não precisa considerar o intervalo de tempo gasto com um semáforo.

Supondo que cada veículo realiza um movimento uniformemente acelerado, o atacante pode calcular, usando as equações newtonianas do movimento, a variação de espaço $x_n^{'}$ realizada em cada relação, tal como apresentado em 2.

$$x_n^{'} = (t_{i'} - t_i)(v_{i'} + v_i)/2 \tag{2}$$

Em seguida, o adversário compara a distância estimada $x_n^{'}$ com a distância conhecida x_n para cada par de eventos em (L_E,L_S) e decide pela relação em que o erro estimado é mínimo. O par de eventos escolhido representa a melhor estimativa do atacante para rastrear um nó veicular. Sejam A e B dois veículos saindo pelo acesso 3 de uma mix-zone e um atacante que registrou dois eventos de entrada E_A (10,0,4) e E_B (14,1,1) e dois eventos de saída S_A (22.5,6,3), S_B (24,6,3). Considere $x_3 = 100m$ e que a saída do acesso 3 possui duas pistas, de modo que os dois veículos utilizaram pistas diferentes. Os eventos são registrados em suas respectivas listas. Aplicando 2 à combinação de eventos nestas listas, tem-se que $x^{'}_{3\,E_AS_A} = 97.5\ m$, $x^{'}_{3\,E_AS_B} = 102.1\ m$, $x^{'}_{3\,E_BS_A} = 87.7\ m$ e $x^{'}_{3\,E_BS_B} = 95\ m$. Em seguida, o ataque é realizado de modo que cada veículo na lista de eventos de entrada é correlacionado ao veículo da lista de saída para o qual a combinação resultou no menor erro. Deste modo, a combinação (E_A,S_B) é escolhida para o veículo A e a combinação (E_B,S_B) é escolhida para o veículo B. Este exemplo mostra que apenas a tentativa de rastrear o veículo B teve sucesso.

CAPÍTULO 4

ANÁLISE EXPERIMENTAL

Neste capítulo, é avaliado o nível de privacidade de localização fornecido pela solução proposta contra um atacante interno. A seção 4.1 descreve as ferramentas de simulação utilizadas nos experimentos. Por meio destas, dois experimentos foram realizados. A seção 4.2 descreve os resultados obtidos por meio destes experimentos.

4.1 AMBIENTE DE SIMULAÇÃO

Esta seção detalha o simulador utilizado nos experimentos deste trabalho. A subseção 4.1.1 apresenta as ferramentas capazes de simular redes de comunicação veicular e justifica a escolha do simulador adotado. A subseção 4.1.2 detalha este simulador e descreve parâmetros do ambiente de simulação nos experimentos realizados.

4.1.1 Simuladores

As aplicações de segurança veicular devem ser exaustivamente testadas antes de sua implantação. Ferramentas de simulação de VANETs têm sido usadas para substituir experimentos com veículos, devido a sua simplicidade, flexibilidade e custo. Nesta subseção, são analisados vários simuladores disponíveis e atualmente em uso pela comunidade científica. Simuladores proprietários, como TSIS-CORSIM [68], Carisma [69], VisSim [70], QualNet [71] e OPNET [72], não foram analisados neste trabalho, pois não permitem livre acesso ao código fonte do simuldador. Apenas as ferramentas de software livre e abertas foram consideradas.

Existem duas abordagens para simulação de VANETs. Uma destas abordagens, apresentada na subseção 4.1.1.1, consiste em usar simuladores projetatos especificamente para

estas redes. A outra abordagem consiste em utilizar simuladores de trânsito e simuladores de rede em paralelo, apresentada na subseção 4.1.1.2.

4.1.1.1 Simuladores Projetados para VANETs

Nesta abordagem, a integração entre um modelo de mobilidade de trânsito e um modelo de comunicação de rede é assegurada na fase de projeto. Esta integração é realizada implicitamente, uma vez que os desenvolvedores projetam o simulador com esta integração em mente. Devido à complexidade de desenvolvimento deste modelo, voltado simultaneamente para comunicação e mobilidade, poucas ferramentas foram desenvolvidas com esta integração.

Um exemplo desta abordagem é o GrooveSim [73], um simulador de roteamento geográfico em VANETs. Este tem vários modos de operação que permitem: avaliação de protocolos de rede, geração de cenários de teste para simulação, extração de modelos de propagação de comunicação sem fio móvel em tempo real, entre outras funcionalidades. A limitação mais significativa do GrooveSim é o modelo de mobilidade simplificado, o qual, entre outras coisas, não permite aos veículos a mudança de faixa em uma mesma pista.

A ferramenta STRAW (*Street Random Waypoint*) [74] permite construir um modelo de mobilidade que restringe a circulação de veículos de acordo com o mapa de uma cidade. Diferentes perfis de tráfego (e.g., um congestionamento de veículos) e mecanismos de controle específicos podem ser usados. Esta ferramenta é uma extensão de um simulador de rede sem fio desenvolvido na Universidade de Cornell. O modelo de mobilidade do STRAW é também simplificado e não considera a transição de veículos entre múltiplas faixas de uma pista.

Por outro lado, o NCTuns [75], um simulador que possui mobilidade e comunicação integrados, possui muitas facilidades e flexibilidade para implementação de aplicações e protocolos de VANETs. Contudo, este não é ideal para simulações em larga escala. Por

exemplo [76], um cenário de simulação com apenas 100 veículos requer 22 minutos. Para o dobro de veículos, a quantidade de tempo requerida aumenta quatro vezes, considerando um processador de 1.8 GHz. De um modo geral, os simuladores altamente integrados são mais adequados para experimentos simples, mas devido à complexidade inerente ao modelo, simulações em larga escala não são viáveis.

4.1.1.2 Simuladores de Trânsito e Redes em Paralelo

Esta abordagem baseia-se no uso de simuladores de trânsito e de redes de forma paralela, onde a saída produzida por um destes serve como entrada para o outro. A disponibilidade pública e a popularidade destas ferramentas têm sido os principais motivos de sucesso desta abordagem. A principal dificuldade no desenvolvimento de simulações nestas ferramentas é que a maioria dos simuladores baseia-se no uso de simuladores de trânsito para gerar um perfil de trânsito que é utilizado, em seguida, como um modelo de mobilidade para os nós de um simulador de MANETs, mas eventos que ocorrem nas aplicações da rede de comunicação veicular não influenciam a mobilidade destes no simulador de trânsito, ou seja, não ocorre um acoplamento bidirecional.

Os simuladores de trânsito VanetMobiSim [77] e SUMO [78] são os dois principais geradores de trilhas de movimento veicular. Estas ferramentas consideram características de mobilidade no nível macro, tais como topologia de estradas, pistas com múltiplas faixas, limite de velocidade da pista, e no nível micro, como cruzamentos regulados por sinais de trânsito.

Os simuladores de rede NS-2 [79] (*Network Simulator 2*) e OMNET++[80] (*Objective Modular Network Testbed in C++*) podem ser acoplados ao SUMO por meio das ferramentas TraNS (*Traffic and Network Simulator*)[81] e VeiNS (*Vehicles in Network Simulation*) [82], respectivamente. O NS-2 tem como vantagem possuir uma grande quantidade de protocolos implementados. O OMNET++ é um ambiente de simulação de eventos discretos, sua principal área de aplicação é a simulação de redes de comunicação,

mas devido a sua arquitetura genérica e flexível, pode ser utilizado em outras áreas, como redes de filas e arquiteturas de hardware. Algumas das vantagens do OMNET++ em relação ao NS-2 são:

- OMNET++ fornece uma arquitetura de componentes para os modelos. A arquitetura modular permite grande flexibilidade e facilidade de implementação de novas aplicações. Componentes (módulos) são programados em C++, em seguida, montados em componentes maiores. Isto resulta na possibilidade de reusabilidade dos modelos desenvolvidos.

- O kernel de simulação do OMNET++ é uma biblioteca de classes, ou seja, módulos no OMNET++ são independentes do kernel. O pesquisador pode escrever seus componentes (módulos simples) contando com uma API do kernel de simulação. Os fontes do OMNET++ nunca recebem *patchs* dos modelos implementados. Este aspecto difere do NS-2, pois neste o limite entre o núcleo de simulação e os modelos não é claro, ou seja, não há uma API bem definida.

- O OMNET++ permite mostrar transmissões de pacotes durante a simulação. Por meio do Tkenv, um ambiente de execução interativo é oferecido, o qual permite a mudança de parâmetros e a análise da evolução da simulação.

- OMNET++ pode simular topologias de rede em grande escala. O limite é a capacidade de memória virtual disponível. O NS-2 tem problemas de extensibilidade na simulação de topologias de rede.

- OMNET++ tem um manual bem escrito e atualizado. A documentação do NS-2 encontra-se fragmentada.

4.1.1.3 Escolha do Simulador

Visto que os simuladores GrooveSim e STRAW não implementam a transição de veículos entre múltiplas faixas de uma pista, a simulação nestas farramentas torna-se

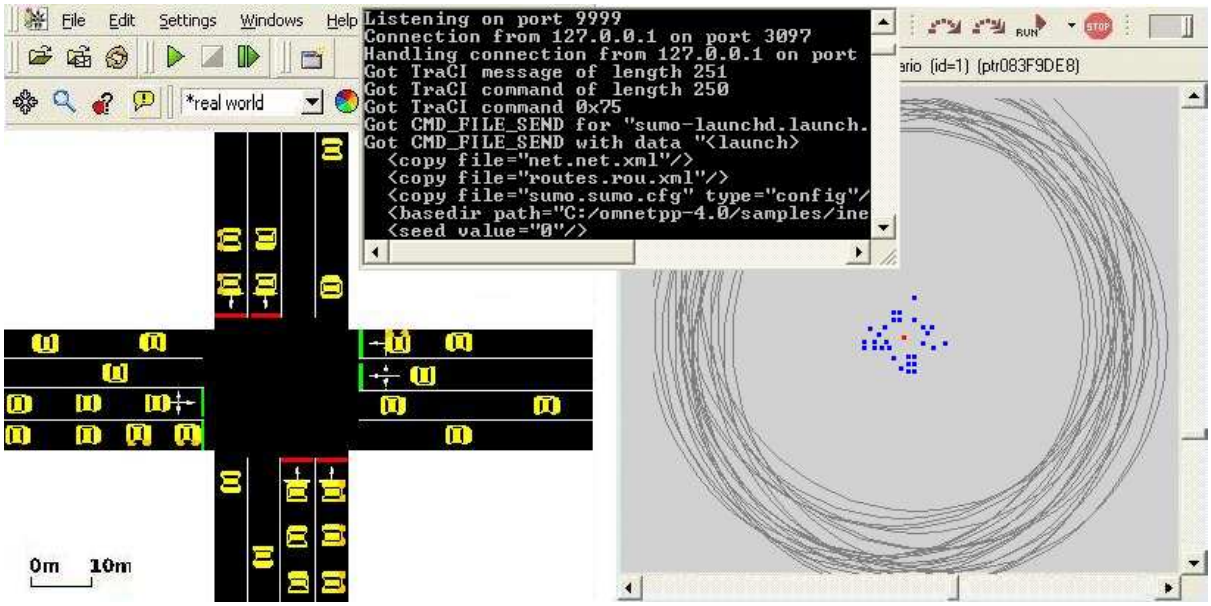


Figura 4.1: Ambiente de simulação usando o *framework* VeiNS. Na esquerda, o tráfego gerado pelo SUMO. Na direita, os nós corespondentes do OMNET++. No centro, uma console que mostra a conexão entre estes dois simuladores.

mais distante do comportamento real dos veículos. Por sua vez, o simulador NCTuns não permite a realização dos experimentos na escala desejada. Deste modo, foi adotada a abordagem baseada na integração em paralelo dos modelos de trânsito e rede. Uma vez que o simulador VanetMobiSim não permite acoplamento bidirecional, o simulador SUMO foi adotado como simulador de trânsito. Entre as ferramentas TraNS e VeiNS, que permitem a integração de um simulador de rede ao SUMO, foi escolhida a ferramenta VeiNS, pois o OMNET++ possui mais vantagens, em relação ao NS-2, para o desenvolvimento dos experimentos deste trabalho.

4.1.2 Implementação

Conforme justificado na subseção anterior, foi utilizado o *framework* VeiNS para a execução dos experimentos. VeiNS é um *framework* de simulação de comunicação inter-veicular que utiliza um modelo de simulação bidirecionalmente acoplado. Ele permite o uso do simulador de rede OMNET++/INET, juntamente com o simulador de trânsito

Tabela 4.1: Parâmetros gerais de configuração dos simuladores.

Parâmetro	Valor
MAC	IEEE 802.11
Taxa de transmissão	6 Mb/s
Frequência da portadora	5.9 GHz
Potência de transmissão	24.430 mW
Limite de atenuação	-80 dBm
Coeficiente de atenuação	2
Velocidade máxima	30 m/s
Tamanho de veículos	5 m

SUMO. Os simuladores são postos a funcionar em paralelo e se comunicam através de um soquete TCP, por meio de um protocolo padrão.

O modelo de nó veicular do VeiNS foi utilizado para a implementação dos nós veiculares e para desenvolver um modelo para implementação das unidades de acostamento. Uma vez que estas gerenciam a comunicação em suas correspondentes *mix-zones*, o atacante interno considerado nos experimentos foi simulado por estas unidades. Para isto, o procedimento descrito no ataque apresentado na seção 3.3.3 foi utilizado, de modo que as informações dos veículos foram coletadas nos devidos momentos e aplicadas à equação do modelo. Em seguida, os pseudônimos correlacionados com sucesso nos ataques foram identificados para gerar as estatísticas apresentadas nos resultados.

Na topologia escolhida para as *mix-zones*, um semáforo gerencia um cruzamento com quatro acessos, onde cada pista de cada acesso possui duas faixas, conforme ilustrado na figura 4.1. O semáforo mostra 30 segundos de sinal verde para dois acessos na mesma direção, seguido por 30 segundos de luz vermelha (ou seja, um período de 60 segundos).

A tabela 4.1 apresenta alguns dos parâmetros de configuração dos simuladores OMNET++ e SUMO. Para o controle de acesso ao meio, foi estabelecido o padrão IEEE 802.11. Tal como em configurações de experimentos em trabalhos relacionados [34, 61], foi definida uma taxa nominal de transmissão de dados de 6 Mb/s e para a atenuação do sinal, assumindo um coeficiente de atenuação no espaço livre, a aplicação dos parâmetros apresentados (coeficiente de atenuação, limite de atenuação, potência de transmissão) no

modelo de propagação utilizado pelo OMNET++ resulta em um alcance de transmissão de 200 metros. A frequência de transmissão foi definida com um valor de 5.9 GHz, faixa do espectro reservada para redes veiculares. A velocidade máxima e o tamanho de cada veículo foram assumidos como $30m/s$ e $5m$, respectivamente.

4.2 SIMULAÇÃO

Dois tipos de experimentos são apresentados nesta seção. O primeiro (subseção 4.2.1) ocorre em um cenário de simulação controlado em uma *mix-zone*, por onde passam 2.000 veículos durante a simulação. O segundo experimento (subseção 4.2.2) utiliza um cenário realista de comunicação em VANET.

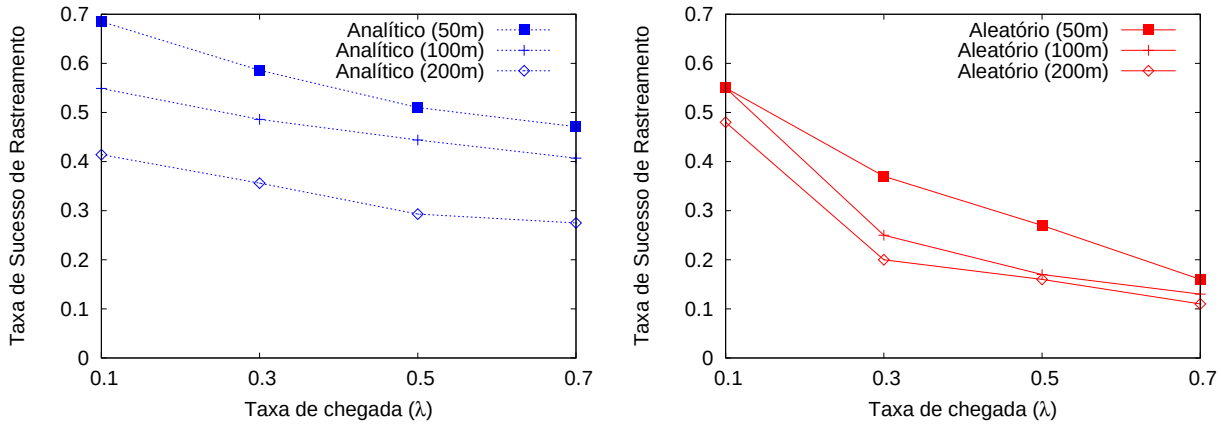
4.2.1 Primeiro Experimento: Mix-Zone Única

Neste experimento, considerou-se uma única *mix-zone* e um atacante interno. Uma vez que este atacante é capaz de rastrear qualquer veículo com chance de 100% de sucesso na solução original baseada no protocolo CMIX, primeiramente, foi avaliada a eficácia da solução proposta contra este atacante, através de dez simulações. Para isso, foi medida a taxa de sucesso de rastreamento do atacante, que é a relação entre o número de ataques bem-sucedidos e o número total de ataques. Assumiu-se que os eventos de chegada de veículos seguem uma distribuição de *Poisson* com λ entre $[0.1, 0.7]$ veículos/segundo. Os resultados obtidos para valores de λ maiores que 0.7 não variaram, pois após este valor a taxa de chegada na fila dentro da mix-zone torna-se maior que a taxa de saída. Deste modo, o tamanho da fila de veículos cresce rapidamente e o número de veículos dentro da *mix-zone* permanece constante.

A figura 4.2 mostra a efetividade dos ataques. Na figura 4.2a o atacante usa o modelo de ataque descrito na seção 3.3.3 enquanto a figura 4.2b apresenta os resultados de quando um atacante estima aleatoriamente a correlação entre os pseudônimos usados por cada veículo. Em ambos os cenários, quanto mais veículos entram na *mix-zone*, menor é a taxa

de sucesso de rastreamento. Este comportamento é esperado, pois se o atacante registra mais eventos, a chance de escolher o pseudônimo errado é maior. A eficácia do atacante diminui quando o raio da *mix-zone* aumenta. *Mix-zones* maiores comportam um número de veículos maior, o que contribui para tornar o ataque menos efetivo.

Pode-se notar a efetividade da abordagem proposta. Estes resultados sugerem que mesmo que o atacante utilize dados baseados na dinâmica dos veículos, a sua capacidade de rastreamento não parece muito melhor em relação ao rastreamento de veículos de forma aleatória. Além disso, considerando que os veículos passarão por várias *mix-zones* durante a viagem, a probabilidade acumulada de sucesso de rastreamento tende a ser bastante baixa. Por exemplo, se um veículo passar por quatro *mix-zones* semelhantes à descrita, com taxa média de chegada igual a 0.3 veículos/s e raio definido como $200m$, a probabilidade acumulada de sucesso do atacante será em torno de 1%. Vale a pena mencionar que os resultados obtidos na avaliação do nível de privacidade de localização considerando um atacante interno é semelhante ao obtido na avaliação para um atacante externo em outros trabalhos [5, 63].



(a) (b)

Figura 4.2: Variação da taxa de sucesso de rastreamento para diferentes valores de taxa de chegada de veículos e raios de *mix-zone*.

Como explicado anteriormente, a solução proposta implica em um certo número de mensagens transmitidas pela RSU devido ao processo de encaminhamento de estados. Para avaliar esta sobrecarga, observou-se o número de mensagens transmitidas pela RSU

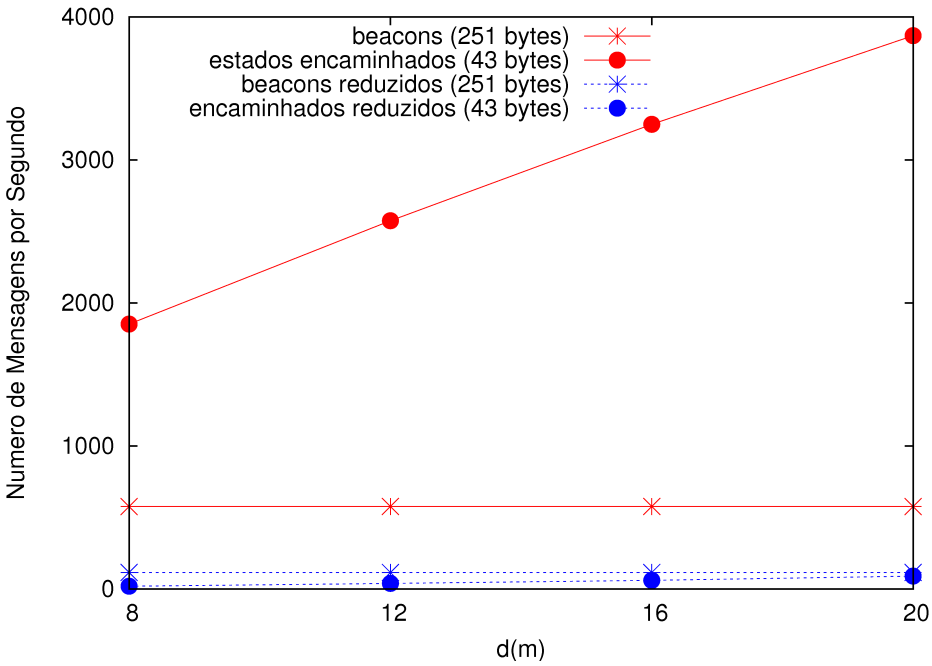


Figura 4.3: Número de mensagens transmitidas devido ao processo de encaminhamento versus o parâmetro d. Foram avaliados cenários antes e após a aplicação dos mecanismos.

em dois cenários. A figura 4.3 apresenta esta sobrecarga em termos de mensagens de estado encaminhado por segundo. No primeiro cenário foi avaliado o número de *beacons* na comunicação antes da aplicação da solução proposta. Neste caso, os resultados mostram que quando aplicado o mecanismo de encaminhamento sem as estratégias para redução de comunicação, a sobrecarga de comunicação é alta. No segundo cenário, as estratégias de redução de comunicação foram utilizadas. Neste cenário, o númerio de *beacons* é em torno de um quinto do número de *beacons* no cenário anterior e que o número de mensagens de estado encaminhado é reduzido pelo menos quinze vezes. Podemos concluir que a solução é viável pois a quantidade de comunicação após a aplicação da solução proposta é mais que duas vezes menor e ainda que um mecanismo de tolerância a falhas seja utilizado, de modo a duplicar essa quantidade de comunicação, a solução não se tornaria inviável. Oos resultados indicam também que a sobrecarga aumenta linearmente com o parâmetro d, o qual delimita a região de vizinhança. Este comportamento é esperado, uma vez que os veículos possuem um maior conjunto de vizinhança para valores maiores de d. Finalmente, a sobrecarga aumenta com o aumento do tamanho da *mix-zone*, o que

também é esperado.

4.2.2 Segundo Experimento: Mix-Zone vs. Mix-Context

O objetivo deste experimento é comparar duas abordagens distintas, *mix-zone* e *mix-context*. Foi assumido um atacante interno global neste experimento. Segundo descrito na seção 2, de acordo com a abordagem *mix-context*, a mudança de pseudônimos ocorre apenas se houver um conjunto de k veículos próximos uns dos outros e com estados semelhantes. Isto significa que os veículos podem mudar de pseudônimo em locais arbitrários ao longo de sua jornada, ao contrário do modelo *mix-zone*, que predefine lugares específicos para tais operações. Para implementar a abordagem *mix-context*, foi escolhido o *Synchronous Pseudonym Change Algorithm* [61]. Na configuração da abordagem *mix-context* foi considerado um valor $k = 3$ veículos que mudam de pseudônimo simultaneamente quando a distância entre estes é menor que 10 metros e não diferem, entre si, em mais de 0.5 m/s.

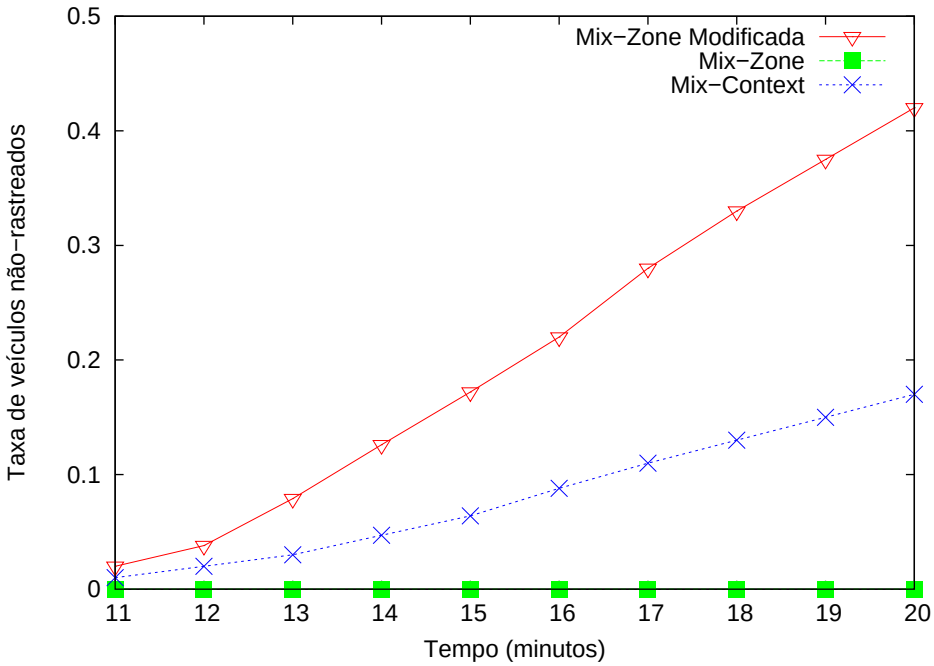


Figura 4.4: Total de veículos não rastreados para ambas as abordagens. Foram considerados os veículos que participaram da simulação por pelo menos 10 minutos.

Para este experimento foram utilizados dados do projeto TAPAS [22]. Estes dados representam um cenário realista do tráfego local de Colônia, uma cidade na Alemanha. Os dados correspondentes ao período entre 07:00h à 07:20h da manhã foram utilizados no mapa rodoviário desta cidade (ver figura 4.5). Os primeiros dez minutos foram utilizados para inicialização do ambiente. Quanto à solução proposta, foram consideradas dez *mix-zones* uniformemente distribuídas nesta cidade.

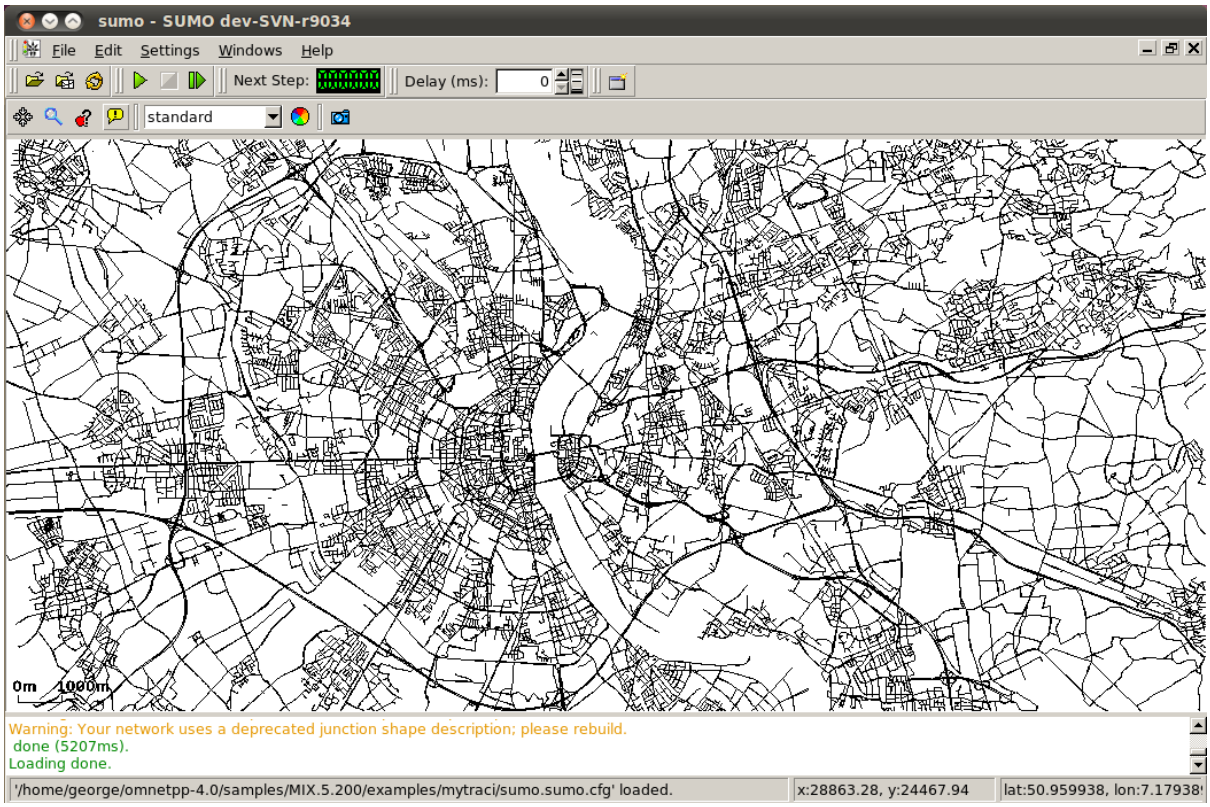


Figura 4.5: Mapa rodoviário da cidade de Colônia.

O modelo analítico descrito na seção 3 foi usado para implementar o atacante de ambas as abordagens. Na solução *mix-context*, um evento de entrada é definido quando k nós mudam seus pseudônimos e um evento de saída ocorre no período que se segue a este.

Os resultados apresentados na figura 4.4 indicam a taxa de veículos que não foram rastreados. Estes resultados sugerem que a solução proposta neste trabalho oferece muito mais proteção contra ataques internos do que a solução *mix-context*. De fato, como pode

ser observado, durante o intervalo de 10 min, o número total de veículos não rastreados é cerca de 2.4 vezes maior para a solução proposta.

CAPÍTULO 5

CONCLUSÃO

5.1 CONCLUSÃO E TRABALHOS FUTUROS

A implantação das redes de comunicação veicular oferecem muito benefícios importantes. O principal destes é a possibilidade da prevenção de colisões entre veículos. Entretanto, os principais padrões desenvolvidos para estas redes não são capazes de assegurar a privacidade de localização de seus usários. A ausência desta garantia pode inibir a participação destes na comunicação veicular, resultando no fracasso de sua implantação. Para assegurar a privacidade de localização dos usuários das VANETs, foi proposto na comunidade científica o uso de pseudônimos temporários e *mix-zones*, regiões onde a comunicação é codificada por meio de uma chave secreta de grupo. Nestas regiões, os usuários mudam seu pseudônimo para despistar quaisquer atacantes que estejam monitorando a comunicação nestas redes com o intuito de registrar os percursos dos usuários destas. Contudo, a solução que implementa o conceito de *mix-zones* nas VANETs se baseia no uso de chaves criptográficas de grupo, de modo que esta não é capaz de impedir ataques realizados por um nó malicioso que seja um membro válido nestas redes.

Neste trabalho foi proposta uma abordagem para inibir ataques internos às *mix-zones*. Na solução proposta, a RSU que gerencia uma *mix-zone* negocia uma chave secreta diferente para cada membro desta região. As informações de estado transmitidas pelos nós veiculares são codificadas por estas chaves. Quando a RSU recebe estas mensagens, após decodificá-las, ela encaminha estas informações de estado para os vizinhos do originador da mensagem. Uma vez que apenas os vizinhos de um dado nó podem acessar informações de estado deste, o nível de privacidade de localização aumenta, pois a ação de um nó malicioso limita-se aos nós vizinhos deste, apenas pelo tempo em que estes estejam próximos, segundo um valor predefinido. Além disso, uma vez que o tráfego de

comunicação passa pela RSU, esta pode evitar que tais informações cheguem a um nó malicioso.

Devido a sobrecargas na comunicação, resultante da solução proposta, mecanismos adicionais foram desenvolvidos. Os resultados de experimentos realizados para estimar o impacto desta sobrecarga mostraram que estes mecanismos reduzem consideravelmente a quantidade de comunicação necessária para garantia da segurança do trânsito, de modo que a solução proposta se mostrou viável.

Foram realizadas simulações para medir o nível de privacidade de localização fornecido pela nova solução. Para isso, um modelo analítico de ataque foi desenvolvido. Este modelo permitiu descobrir a taxa de sucesso de um atacante em seu intento de rastrear o percurso dos usuários em uma *mix-zone*. Para fins de comparação, um modelo de ataque baseado em estimativas aleatórias foi considerado. A primeira avaliação foi apresentada em um experimento controlado, enquanto um outro experimento considerou um cenário com o comportamento veicular de uma cidade. No primeiro cenário, os resultados mostraram que a proposta fornece um alto nível de privacidade de localização. Foi observado também que estes resultados são pouco melhores quando comparados aos apresentados pelo modelo aleatório, ou seja, ataques mais sofisticados à abordagem proposta são pouco efetivos. No segundo cenário, o nível de privacidade de localização contra um atacante global foi comparado ao provido pela solução "*mix-context*", que se baseia em um modelo alternativo ao da solução proposta. Este experimento demonstrou que o uso de *mix-zones* em um cenário da escala de uma cidade é mais eficaz na proteção da privacidade de localização dos usuários das redes veiculares. Pode-se concluir que, por meio da solução apresentada, os futuros usuários destas redes não rejeitarão a sua implantação, pois esta assegura um nível de privacidade de localização adequado.

Trabalhos futuros podem ser realizados para ampliar esta contribuição. Outros modelos analíticos de ataque, para avaliação do nível de privacidade de localização oferecido pela solução proposta, podem ser desenvolvidos por meio de abordagens baseadas em teoria das filas. É possível também substituir o método utilizado para identificar um

possível nó malicioso, baseado na quantidade de tempo deste em uma *mix-zone*, por outros métodos que analisem o comportamento individual dos nós veiculares nestas regiões.

REFERÊNCIAS

[1] Antonio Marcos Carianha, Luciano Porto Barreto, and George Lima. Improving Location Privacy in Mix-Zones for VANETs. *International Workshop on Hot Topics on Wireless Network Security and Privacy (HotWiSec)*, 2011.

[2] Pedro Henrique dos Santos Lemos. VANETs - Vehicular Adhoc Networks. Disponível em: <www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/lemos>. Acesso em: 17 Ago. 2011.

[3] R. S. Alves, I. V. Campbell, R. S. Couto, M. E. M. Campista, I. M. Moraes, M. G. Rubinstein, L. H. M. K. Costa, O. C. M. B. Duarte, and M. Abdalla. Redes veiculares: Princípios, aplicações e desafios. *XXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 199–254, 2009.

[4] Shahram Rezaei, Raja Sengupta, Hariharan Krishnan, Xu Guan, and Raman Bhatia. Tracking the position of neighboring vehicles using wireless communications. *Transportation Research Part C: Emerging Technologies*, 18(3):335–350, 2010.

[5] J. Freudiger, M. Raya, M. Feleghhazi, P. Papadimitratos, and J.-P. Hubaux. Mix-zones for location privacy in vehicular networks. In *First International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, 2007.

[6] Community Road Accident Database. CARE database - reports and graphics. Disponível em: <ec.europa.eu/transport/home/care/index_en.htm>. Acesso em: 17 Ago. 2011.

[7] American Automobile Association (AAA). Crashes vs. Congestion - What's the Cost to Society? Disponível em: <www.aaanewsroom.net>. Acesso em: 17 Ago. 2011.

[8] National Highway Traffic Safety Administration (NHTSA) report on traffic fatalities. Disponível em: <www-fars.nhtsa.dot.gov/Main/index.aspx>. Acesso em: 17 Ago. 2011.

[9] Seguro Obrigatório de Danos Pessoais Causados Por Veículos Automotores de Via Terrestre (DPVAT). Disponível em: <www.dpvatseguro.com.br/conheca/informacoes.asp>. Acesso em: 17 Ago. 2011.

[10] Seguradora Líder dos Consórcios do Seguro DPVAT. Indenizações - Quantidade e Valores. Disponível em: <www.seguradoralider.com.br/estat_ind_ano_2010.asp>. Acesso em: 17 Ago. 2011.

[11] Tim Leinmüller, Elmar Schoch, and Christian Maihöfer. Security issues and solution concepts in vehicular ad hoc networks. In *Proceedings of the 4th Annual Conference on Wireless On demand Network Systems and Services (WONS 2007)*, 2007.

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

[13] Y. Liu, J. Bi, and J. Yang. Research on vehicular ad hoc networks. *Control and Decision Conference (CCDC'09)*, 2009.

[14] Florian Schaub, Zhendong Ma, and Frank Kargl. Privacy requirements in vehicular communication systems. In *Proceedings of the 2009 International Conference on Computational Science and Engineering - Volume 03*, pages 139–145. IEEE Computer Society, 2009.

[15] Christine Laurendeau and Michel Barbeau. Threats to security in DSRC/WAVE. In *Ad-Hoc, Mobile, and Wireless Networks*, volume 4104 of *Lecture Notes in Computer Science*, pages 266–279. 2006.

[16] Roberto A. Uzcátegui and Guillermo Acosta-Marum. WAVE: a tutorial. *Communications Magazine*, 47:126–133, 2009.

[17] 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 (WAVE). IEEE 802.11p, 2010.

[18] Institute of Electrical and Electronics Engineers. IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. IEEEP1609.2., 2006.

[19] Maxim Raya and Jean-Pierre Hubaux. The security of vehicular ad hoc networks. In *3rd ACM workshop on Security of Ad hoc and Sensor Networks (SASN)*, 2005.

[20] B. Wiedersheim, Zhendong Ma, F. Kargl, and P. Papadimitratos. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In *Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*, pages 176–183, 2010.

[21] Alastair R. Beresford. Location Privacy in Ubiquitous Computing. Dissertation, University of Cambridge, 2005.

[22] Christian Varschen and Peter Wagner. Mikroskopische Modellierung der Personenverkehrsnachfrage auf Basis von Zeitverwendungstagebüchern. *Aachener Kolloquium "Mobilität und Stadt"(AMUS)*, 2006.

[23] O. T. Cruces. Applying Delay Tolerant Protocols to VANETs. Dissertation, Techinal University of Catalonia, 2008.

[24] Carl Eklund, Kenneth L. Stanwood, Stanley Wang, and Ensemble Communications Inc. IEEE Standard 802.16: A technical overview of the WirelessMAN Air Interface for broadband wireless access. *IEEE Communications Magazine*, 40:98–107, 2002.

[25] United States Department of Defense. Official U.S. Government information about the Global Positioning System (GPS) and related topics. Disponível em: <www.gps.gov>. Acesso em: 17 Ago. 2011.

[26] European Space Agency. Galileo Navigation. Disponível em: <www.esa.int/esaNA/galileo.html>. Acesso em: 17 Ago. 2011.

[27] Rayman Singh and Arobinda Gupta. Traffic congestion estimation in VANETs and its application to information dissemination. In *Distributed Computing and Networking*, volume 6522 of *Lecture Notes in Computer Science*, pages 376–381. 2011.

[28] Christian Lochert, Björn Scheuermann, Christian Wewetzer, Andreas Luebke, and Martin Mauve. Data aggregation and roadside unit placement for a VANET traffic information system. In *Proceedings of the 5th ACM International Workshop on VehiculAr Inter-NETworking*, VANET'08, pages 58–65. ACM, 2008.

[29] S. Manui and M. Kakkasageri. Issues in mobile ad hoc networks for vehicular communication. *IETE Technical Review*, 25:59–72, 2008.

[30] The FCC Dedicated Short Range Communications (DSRC). Disponível em: <wireless.fcc.gov/services/its/dsrc>. Acesso em: 17 Ago. 2011.

[31] Federal Communications Commision, "FCC 99-305", FCC Report and Order, 1999.

[32] CAR 2 CAR Communication Consortium. Disponível em: <www.car-to-car.org>. Acesso em: 17 Ago. 2011.

[33] Internet ITS consortium. Disponível em: <www.internetits.org>. Acesso em: 17 Ago. 2011.

[34] Daniel Jiang, Qi Chen, and Luca Delgrossi. Optimal data rate selection for vehicle safety communications. In *Proceedings of the 5th ACM International Workshop on VehiculAr Inter-NETworking*, VANET '08, pages 30–38. ACM, 2008.

[35] Institute of Electrical and Electronics Engineers. IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Networking Services. IEEEP1609.3, 2007.

[36] Institute of Electrical and Electronics Engineers. IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Multi-Channel Operation. IEEEP1609.4, 2006.

[37] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 4th edition, 2005.

[38] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons, 2nd edition, 1996.

[39] Certicom Research. Standards for Efficient Cryptography - SEC 1: Elliptic Curve Cryptography. Version 2.0, 2010.

[40] FIPS PUB 197 Advanced Encryption Standard (AES), 2001.

[41] Internet Engineering Task Force: IETF Request for Comments: 3565, Use of Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS). IETF RFC 3565, 2003.

[42] R. L. Rivest, The MD5 Message-Digest Algorithm, Request for Comments (RFC 1320), Internet Activities Board, Internet Privacy Task Force, 1992.

[43] FIPS 180-1, Secure hash standard, NIST, US Department of Commerce, Washington D. C., 1995.

[44] D. Johnson, A. Menezes, and S. Vanzone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *Certicom Research*, 2001.

[45] Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux. Design and analysis of a lightweight certificate revocation mechanism for VANET. In *Vehicular Ad Hoc Networks*, pages 89–98, 2009.

[46] B. Parno and A. Perrig. Challenges in securing vehicular networks. *Proceedings of the 4th Workshop on Hot Topics in Networks (HotNets-IV)*, 2005.

[47] Ginger Myles, Adrian Friday, and Nigel Davies. Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing*, pages 56–64, 2003.

[48] Bugra Gedik and Ling Liu. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*, 7:1–18, 2008.

[49] D. Chaum and E. V. Heijst. Group signatures. *Proc. Advances in Cryptology (Eurocrypt'91)*, 1991.

[50] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. *Proceedings of CRYPTO'04, LNCS Series*, 2004.

[51] A. Studer, E. Shi, F. Bai, and A. Perrig. TACKing together efficient authentication, revocation, and privacy in VANETs. *IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc (SECON'09)*, 2009.

[52] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy. Efficient and robust pseudonymous authentication in VANET. *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks*, 2007.

[53] J. Guo, J. P. Baugh, and S. Wang. A group signature based secure and privacy-preserving vehicular communication framework. *Mobile Networking for Vehicular Environments*, 2007.

[54] Yong Hao, Yu Cheng, and Kui Ren. Distributed key management with protection against RSU compromise in group signature based VANETs. In *GLOBECOM*, pages 4951–4955, 2008.

[55] X. Lin, X. Sun, P. H. Ho, and X. Shen. GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, 2007.

[56] B. Chaurasia, S. Verma, G. S. Tomar, and S. M. Bhaskar. Pseudonym based mechanism for sustaining privacy in VANETs. *Computational Intelligence, Communication Systems and Networks (CICSYN)*, 2009.

[57] E. Fonseca, A. Festag, R. Baldessari, and R. L. Aguiar. Support of anonymity in VANETs - Putting pseudonymity into practice. *Wireless Communications and Networking Conference (WCNC)*, pages 3400–3405, 2007.

[58] Levente Buttyán, Tamás Holczer, and István Vajda. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In *Security and Privacy in Ad-hoc and Sensor Networks*, volume 4572 of *Lecture Notes in Computer Science*, pages 129–141. Springer Berlin / Heidelberg, 2007.

[59] Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran. AMOEBA: Robust location privacy scheme for VANET. *IEEE Journal on Selected Areas in Communications*, pages 1569–1589, 2007.

[60] Matthias Gerlach and Felix Guttler. Privacy in VANETs using changing pseudonyms - Ideal and real. In *Proceedings of the 65th Vehicular Technology Conference (VTC)*, pages 2521–2525, 2007.

[61] Jianxiong Liao and Jianqing Li. Effectively changing pseudonyms for privacy protection in VANETs. *International Symposium on Parallel Architectures, Algorithms and Networks*, pages 648–652, 2009.

[62] Alastair R. Beresford and Frank Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2:46–55, 2003.

[63] Joo-Han Song, Vincent W. S. Wong, and Victor C. M. Leung. Wireless location privacy protection in vehicular ad-hoc networks. In *IEEE International Conference on Communications (ICC)*, pages 2699–2704, 2009.

[64] Chen Chen, Xin Wang, Weili Han, and Binyu Zang. A robust detection of the Sybil attack in urban VANETs. *Distributed Computing Systems Workshops, International Conference on*, pages 270–276, 2009.

[65] Wei Dai. Crypto++ 5.6.0 Benchmarks. Disponível em: <www.cryptopp.com/benchmarks-amd64.html>. Acesso em: 17 Ago. 2011.

[66] S.E. Shladover and S.-K. Tan. Analysis of vehicle positioning accuracy requirements for communication-based cooperative collision warning. *Journal of Intelligent Transportation Systems*, 10:131–140, 2006.

[67] N. Dworkin. NIST Special Publication SP 800-38C. Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, 2004.

[68] McTrans Moving Technology. Traffic Software Integrated System-Corridor Simulation (TSIS-CORSIM). Disponível em: <mctrans.ce.ufl.edu/featured/tsis>. Acesso em: 17 Ago. 2011.

[69] S. Eichler, B. Ostermaier, C. Schroth, and T. Kosch. Simulation of car-to-car messaging: Analyzing the impact on road traffic. *Proceedings of the 13th Annual Meeting of the IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, 2005.

[70] Visual Solutions, Inc. VISSIM. Disponível em: <www.ptvamerica.com/vissim.html>. Acesso em: 17 Ago. 2011.

[71] Scalable Network Technologies, Inc. Qualnet Simulator. Disponível em: <www.scalablenetworks.com/products/download.php>. Acesso em: 17 Ago. 2011.

[72] OPNET Technologies, Inc. OPNET Modeler. Disponível em: <www.opnet.com>. Acesso em: 17 Ago. 2011.

[73] R. Mangharam, D. S. Weller, D. D. Stancil, R. Rajkumar, and J. S. Parikh. A topology-accurate simulator for geographic routing in vehicular networks. *Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, 2005.

[74] Aqualab. STreet RAndom Waypoint (STRAW). Disponível em: <www.aqualab.cs.northwestern.edu/projects/STRAW/index.php>. Acesso em: 17 Ago. 2011.

[75] EstiNet Technologies, Inc. NCTUns Network Simulator and Emulator. Disponível em: <nsl10.csie.nctu.edu.tw>. Acesso em: 17 Ago. 2011.

[76] V. Cristea, V. Gradinescu, C. Gorgorin, R. Diaconescu, and L. Iftode. *Simulation of VANET applications.* In Automotive Informatics and Communicative Systems, H. Guo (ed.), Information Science Reference, 2009.

[77] J. Haerri, M. Fiore, F. Fethi, and C. Bonnet. VanetMobiSim: generating realistic mobility patterns for VANETs. *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET'06)*, 2006.

[78] D. Krajzewicz and C. Rossel. Simulation of Urban MObility (SUMO). German Aerospace Centre. Disponível em: <sumo.sourceforge.net/index.shtml>. Acesso em: 17 Ago. 2011, 2007.

[79] K. Fall and K. Varadhan. NS notes and documents. The VINT Project, UC Berkeley, LBL, USC/ISI, and Xerox PARC. Disponível em: <www.isi.edu/nsnam/ns/nsdocumentation.html>. Acesso em: 17 Ago. 2011.

[80] A. Vargas. Objective Modular Network Testbed in C++ (OMNET++), version 4.0. Disponível em: <www.omnetpp.org>. Acesso em: 17 Ago. 2011, 2010.

[81] M. Piorkowski, M. Raya, AL Lugo, P. Papadimitratos, M. Grossglauser, and J-P Hubaux. TraNS:Realistic Joint Traffic and Network Simulator for VANETs. *ACM SIGMOBILE Mobile Computing and Communications Review*, 12, 2008.

[82] Christoph Sommer, Reinhard German, and Falko Dressler. Bidirectionally coupled network and road traffic simulation for improved IVC analysis. *IEEE Transactions on Mobile Computing*, 2010.