# Gerenciamento de Tráfego Seguro para Redes VANETs na Presença de Ataques de Envenenamento de Dados

**Carlos Pedroso[1], Thiago S. Gomides[2], Daniel L. Guidoni[2] e Aldri Santos[1]**

[1]NR2/CCSC - Universidade Federal do Paraná - PR - Brasil

[2]DCOMP - Universidade Federal de São João Del Rei, (UFSJ) - MG - Brasil

{capjunior,aldri}inf.ufpr.br, {gomides,guidoni}ufsj.edu.br

***Abstract.*** *Systems inspired by vehicular networks generally process a large volume of data on real-time demand, being sensitive to attacks that can compromise their functioning or even interrupt them. Data Poisoning attacks (AdP) stand out among the most damaging by changing the reliability of the disseminated data. Although mechanisms exist to deal with these threats, data validation, and collaborative detection on VANETs services are often overlooked. This paper proposes an efficient and secure VANETs traffic management system against EvD attacks, called RONDA. The system has a mechanism that uses watchdog monitoring and relational consensus to detect attackers, ensuring the authenticity and availability of the data. It was evaluated on OMNET++, compared to ON-DEMAND, and attained 90% of detection rate, 4% of false negative and 10% of false positive rates, and decreased vehicle travel time by up to 40%.*

***Resumo.*** *Os sistemas inspirados em redes veiculares geralmente processam um grande volume de dados numa demanda de tempo real, sendo sensíveis a ataques que podem comprometer seu funcionamento ou mesmo interrompê-los. Os ataques de Envenenamento de Dados (EvD) destacam-se dentre os mais danosos por alterar a confiabilidade dos dados disseminados. Embora existam mecanismos para lidar com essas ameaças, a validação dos dados e a detecção colaborativa sobre os serviços de VANETs são frequentemente desconsideradas. Este trabalho propõe um sistema de gerenciamento de tráfego em VANETs eficiente e seguro contra ataques de EvD, chamado RONDA. O sistema possui um mecanismo que emprega monitoramento watchdog e consenso relacional para detecção de atacantes, assegurando a autenticidade e disponibilidade dos dados. O RONDA foi avaliado no OMNET++, junto com o sistema ON-DEMAND, e obteve 90% de taxa de detecção, 4% de falsos negativos e 10% de falsos positivos, e diminuiu em até 40% o tempo de viagem dos veículos congestionados.*

## 1. Introdução

A mobilidade urbana é um tema importante na discussão do crescimento e desenvolvimento urbano nas grandes cidades, uma vez que a mobilidade afeta diretamente a vida da população [Soriano et al. 2018]. A mobilidade das pessoas e dos veículos nos centros urbanos é importante devido às distâncias percorridas diariamente para realizar as atividades cotidianas, como ir ao trabalho, comércio, shoppings entre outras. Contudo, grandes deslocamentos e, ao mesmo tempo, deslocamentos ineficientes impactam a sociedade pela má utilização do tempo pessoal, cansaço, acidentes e congestionamentos.

O crescimento dos congestionamentos veiculares, sem nenhum ação para a minimização dos seus efeitos, pode impactar no avanço da poluição do ar, aumento do tempo e custo do transporte, com consequências financeiras e ambientais [Thakur and Malekian 2019].

Alterações na infraestrutura viária das cidades podem reduzir a influência dos congestionamentos em determinadas regiões, no entanto, possuem um alto custo de projeto e execução. Neste cenário, populariza-se o uso de soluções avançadas que através de tecnologias da informação e comunicação fornecem serviços eficientes para a diminuição dos impactos dos congestionamentos [Guidoni et al. 2020]. Utilizando a capacidade de comunicação e processamento de uma rede veicular *ad hoc* (VANETs), veículos podem monitorar e disseminar informações sobre as condições de tráfego e estimar novas rotas sem congestionamentos. Uma questão importante é a segurança na troca de informações [Lu et al. 2019, Arif et al. 2019, Lima et al. 2009]. Logo, as VANETs ficam expostas a inúmeras vulnerabilidades que visam violar atributos de segurança como, integridade e autenticidade, o que prejudica a execução de protocolos de disseminação de dados com impacto na operação dos serviços de gerenciamento de tráfego [Arif et al. 2019].

Essencialmente, entre os ataques internos ao serviço de disseminação de dados nos sistemas de gerenciamento de tráfego em VANETs, evidencia-se o ataque de Envenenamento de Dados (EvD). O ataque *EvD* também é conhecido como Injeção de Dados Falsos, um dos ataques de intrusão mais nocivos a redes orientadas a dados em virtude das inconsistências de informações e a intermitência com que ocorre [Sen and Madria 2017]. Devido a complexidade, os ataques *EvD* tornam-se complexos e trabalhosos de serem detectados, uma vez que os dispositivos maliciosos normalmente estão autenticados na rede e exercem suas funções padrão de coleta e disseminação de dados [Deng et al. 2016]. Os ataques *EvD* normalmente ocorrem em tempos variados, contínuo ou discreto, desorientado a rede. O ataque *EvD* realiza-se de duas formas: *(i)* quando um dispositivo é capturado por outro e tem seus dados manipulado e *(ii)* quando o próprio dispositivo apresenta um comportamento de má conduta. Esse comportamento dificulta a identificação de dispositivos maliciosos e aumenta o tempo de mal funcionamento da rede, gerando inconsistência nos dados. Assim, é essencial identificar e isolar a presença de dispositivos maliciosos da rede visando manter um funcionamento livre de ameaças.

A segurança em redes VANETS tem sido alvo de uma diversidade de trabalhos na literatura, seja com soluções em veículos ou na proteção dos dados [Lu et al. 2019, Arif et al. 2019]. As voltadas à proteção de dados avaliam a confiabilidade, consistência, e plausibilidade em relação aos dados recebidos. As soluções voltadas a veículos avaliam a fonte emissora com o objetivo de validar seu comportamento. Entretanto, elas têm falhado ou não são adequadas ao contexto de sistemas de gerenciamento de tráfego, visto que normalmente empregam entidades centralizadoras, geram alto consumo de recursos e ignoram a detecção colaborativa entre os veículos. Dessa forma, novas formas de lidar com ameaças em VANETS devem ser consideradas e, entre elas, destaca-se a detecção colaborativa [Li et al. 2017], onde cada dispositivo desempenha as suas funções-padrão e a de agente colaborativo de detecção de atacantes. Uma maneira de empregar a detecção colaborativa está na combinação das estratégias de monitoramento *watchdog* [Santos et al. 2019] e consenso relacional [Pedroso et al. 2019], que possibilitam os sistemas atuarem entre os veículos. Assim, as VANETS demandam por serviços eficientes de gerenciamento de tráfego, seguros, aptos a atuarem de maneira distribuída e

capazes de detectar e isolar a presença de ameaças de veículos maliciosos.

Este trabalho propõe um sistema de gerenciamento tráfego seguro para redes veiculares chamado RONDA (*Ge**R**enciamento de Tráfego Seguro C**O**ntra ataques de EN**v**enenamento de **DA**dos*). O RONDA, além de coletar informações de trânsito e criar novas rotas com melhores tempo de viagem em cenários de congestionamento veicular, ele mitiga os ataques de *EvD* através de monitoramento *watchdog* e realiza um consenso relacional distribuído entre os veículos vizinhos para detectar possíveis intrusos na rede. Durante a disseminação de informações sobre as condições de tráfego nas vias, realizada utilizando apenas a comunicação entre veículos, o RONDA assegura a autenticidade e disponibilidade de dados verdadeiros para a criação de uma base de dados distribuída em cada veículo sobre tráfego nas vias. Utilizando a sua base de dados, os veículos verificam as condições do tráfego nas vias adjacentes a sua para analisar se existe uma nova rota com menos congestionamento. Numa análise comparativa com o sistema de gerenciamento de tráfego ON-DEMAND [Gomides et al. 2020], o RONDA obteve 90% de taxa de detecção, 4% de falsos negativos, 10% de falsos positivos e atingiu 86% de acurácia, além de diminuir em até 40% o tempo de viagem dos veículos.

O restante deste artigo está organizado da seguinte maneira. A seção 2 descreve os trabalhos relacionados. A Seção 3 apresenta o sistema de gerenciamento de tráfego seguro. A Seção 4 detalha as avaliações realizadas. A Seção 5 apresenta as conclusões.

## 2. Trabalhos Relacionados

Diferentes trabalhos na literatura abordam soluções para sistemas de gerenciamento de tráfego utilizando uma rede veicular. Essas soluções visavam reduzir os congestionamentos de tráfego com menor impacto na infraestrutura urbana, principalmente com soluções utilizando novas tecnologias de comunicação e computação. As soluções propostas em [Wang et al. 2016] e [Pan et al. 2017] utilizam a comunicação do veículo com a infraestrutura auxiliar para a criação de uma base de dados central contendo as informações sobre o tráfego nas vias. De posse das informações, os servidores centrais notificam os veículos com novas rotas com menores engarrafamentos. Em [Wang et al. 2016], a solução também utiliza câmeras espalhadas nas vias para detectar congestionamentos. Existem soluções de gerenciamento de tráfego que utilizam apenas a comunicação do veículo e de seus sensores embarcados para verificar novas rotas pelos veículos. Em [Gomides et al. 2020], os veículos monitoram as condições de tráfego com base na distância percorrida e tempo de viagem na via para verificar se uma via está congestionada. Os veículos disseminam essas estimativas para que outros veículos e, de maneira colaborativa, distribuída e utilizando as informações que foram disponibilizadas, os veículos verificam rotas alternativas.

Os sistemas de gerenciamento de tráfego podem utilizar dados de diferentes fontes, tais como sensores a bordo dos veículos (aceleração, frenagem, GPS, distância percorrida, tempo na via etc), câmeras instaladas nas vias e veículos, percepção do usuário sobre o congestionamento etc. Em um ambiente distribuído, um protocolo de comunicação é utilizado para que os veículos realizem a troca das informações e, nesse contexto, questões de segurança surgem como uma ameaça ao correto funcionamento do sistema [Arif et al. 2019, Khan et al. 2019]. Por exemplo, um veículo malicioso pode interceptar, modificar, deletar ou injetar mensagens falsas. Os possíveis ataques enume-

rados no contexto de redes veiculares em [Khan et al. 2019] envolvem os ataques sobre a disponibilidade, confidencialidade, autenticação, integridade, e não repúdio.

Vários trabalhos em redes veiculares abordam o problema de segurança em protocolos de disseminação de dados, especialmente ataques *EvD*. As soluções podem ser dividias em soluções centrada nos veículos ou soluções centradas nos dados. Aquelas centradas nos veículos examinam a fonte do dado, observando seu comportamento ou alguma solução de segurança sendo executada para definir se o veículo pode ser considerado como uma entidade segura de comunicação. Por outro lado, as soluções centradas em dados avaliam a confiabilidade dos dados, verificando a sua consistência e viabilidade em relação aos dados recebidos. Em [Zhang et al. 2018], um mecanismo para detecção de dados falsos utilizando o classificador SVM (*Supported Vector Machine*) verifica o conteúdo das mensagens e os atributos do veículos para classificar uma mensagem como falsa ou um veículo como uma entidade confiável. Quando o veículo verifica se uma mensagem/veículo não são confiáveis, ele notifica uma autoridade central para a disseminação da informação. Em [Kamel et al. 2020], um *framework* para a detecção de comportamento incorreto de veículos que utilizam a comunicação V2X (Veículo-para-veículo, Veículo-para-infraestrutura e veículo para qualquer dispositivo de comunicação). O trabalho utiliza uma um servidor central como autoridade de comportamento inadequado para se ter uma detecção global do comportamento dos veículos.

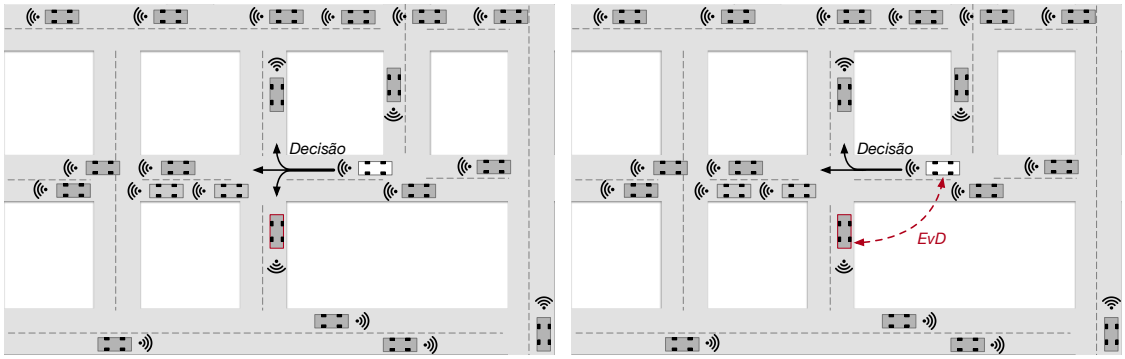
Uma maneira efetiva de alcançar uma detecção colaborativa é através do uso de Consenso entre dispositivos de uma rede. Em [Toulouse et al. 2015], um sistema distribuído para detecção de anomalias, baseado em um protocolo de consenso médio entre participantes, busca identificar anomalias que possam gerar ataques DDoS. Assim, ele realiza análises em cada ponto de coleta de dados usando um classificador *Bayes*. Esta análise ocorre de forma redundante, paralelo ao nível de cada ponto de coleta de dados, o que evita o ponto único de falhas. Em [Pedroso et al. 2019], o mecanismo CONFINIT para detecção de ataques de injeção de dados falsos em uma rede IoT industrial fixa emprega agrupamentos por similaridade para lidar com densidade de dispositivos na rede. Ele combina *watchdog* para o monitoramento entre participantes e consenso colaborativo na tomada de decisão sobre atacantes. Contudo, ignora-se as questões de mobilidade.

Os trabalhos que abordam ataques *EvD* em redes veiculares utilizam uma entidade centralizada e confiável para a detecção de veículos atacantes na rede. Dessa forma, o estudo e proposição de soluções distribuídas para mitigar o ataque de envenenamento de dados no serviço de gerenciamento de tráfego possui grande importância quando apenas a comunicação entre veículos é utilizada na rede veicular.

## 3. Gerenciamento de Tráfego Seguro Contra Ataques EvD

Esta seção descreve o sistema de *Ge**R**enciamento de Tráfego Seguro C**O**ntra ataques de EN**v**enenamento de **DA**dos* (RONDA) para redes veiculares. O RONDA coordena o fluxo do tráfego veicular levando em conta a participação de veículos maliciosos na rede que executam ataques de envenenamento de dados disseminados entre os veículos. Durante o seu percurso, os veículos verificam as condições do tráfego em suas vias e, a cada intervalo de tempo pré-definido, o veículo verifica a necessidade de estimar novas rotas. Utilizando um protocolo de comunicação, o veículo requisita as informações de tráfego das vias adjacentes a sua com o objetivo de criar uma base de dados distribuída

sobre as condições de tráfego nas vias. A partir das informações recebidas, os veículos verificam a existência de rotas com menores tempo de viagem. Entretanto, veículos maliciosos/atacantes realizam ataque de envenenamento de dados *(EvD)* onde informações erradas sobre as condições de tráfego são encaminhadas como resposta a uma requisição. O RONDA foi projetado para identificar e excluir os veículos atacantes do processo de requisição-resposta de informações sobre o tráfego das vias. A Figura 1 ilustra uma visão geral do funcionamento do RONDA. Utilizando as informações sobre congestionamento nas vias vizinhas, o veículo verifica se existem caminhos com menos congestionamentos (Figura 1(a)). Entretanto, ao verificar a existência de dados falsos devido a um ataque *EvD*, as opções de melhores caminhos podem ser alteradas (Na Figura 1(b)). Para o desenvolvimento do sistema RONDA, foram considerados os modelos dos dispositivos veiculares, rede, comunicação e ataques, descritos a seguir.




(a) Gerenciamento de tráfego (b) Comportamento do RONDA sob ataques EvD

**Figura 1. Visão geral do RONDA**

**Modelo dos dispositivos veiculares:** Cada veículo em nosso ambiente VANET é capaz de processar, analisar, comunicar e tomar decisões distribuídas. Todos os veículos são equipados com unidade de bordo (OBU), interface de comunicação IEEE 802.11p, a variedade de sensores, receptor do sistema de posição global (GPS) e o mapa da malha viária da cidade contendo informações sobre as vias (dimensões, quantidade de vias, preferências, velocidade máxima), semáforos, junções etc. Além disso, os veículos podem atuar na rede como membros ou líderes de agrupamentos, onde agrupamentos são formados em cada via contendo os veículos que estão nela e compartilham medições semelhantes de tráfego. O líder é o veículo com maior tempo de permanência na via.

**Modelo da rede:** Um ambiente VANET representado por um grafo direcionado e ponderado $G = (V, E)$, em que $V$ e $E$ representam, respectivamente, as interseções entre as vias (esquinas) e os segmentos de vias (vias entre duas ou mais interseções). O conjunto $V$ (vértices) e $E$ (arestas) é descrito por: $V = \{v_0, v_1, \ldots, v_n\}$ e $E = \forall(v_i, v_j)$. Cada aresta $e_{ij} = (v_i, v_j)$ representa o segmento da estrada que liga as interseções $v_i$ e $v_j$. O custo para percorrer o segmento $e_{ij}$ é um custo associado $w_{ij}$. O conjunto de ponderação é representado por $W = \{w_{ij}, i \neq j\}$ e $w_{ij} \rightarrow R^*_+$. Adicionalmente, $N$ representa o um conjunto de veículos em que $N = \{n_0, n_1, \ldots, n_{m\text{-}1}\}$ e $m$ é o número de veículos.

**Modelo de comunicação:** A comunicação ocorre através do meio sem fio utilizando um canal assíncrono com perda de pacotes devido a ruídos e posição dos veículos. O modelo proposto compreende dois tipos de mensagens disseminadas entre os participan-

tes da rede: as mensagens de alerta/controle, utilizadas para o controle, gerenciamento, formação dos agrupamentos e exclusão de veículos atacantes; as mensagens de disseminação de Níveis de Congestionamento (NC), que são responsáveis pela propagação das informações utilizadas no gerenciamento de tráfego.

**Modelo dos ataques:** A ameaça a rede caracteriza-se por ataques de Envenenamento de dados (EvD), onde os atacantes uma vez intruso na rede iniciam a disseminação das falsas informações de congestionamentos. O ataque pode ser lançado na rede de três maneiras diferentes: a primeira é o ataque *EvD – Inverso* cujo os atacantes sempre enviam dados de trânsito inverso ao verdadeiro coletado pelos veículos. A segunda é o ataque *EvD – Nível Máximo* onde os atacantes enviam sempre a maior aferição de dados de trânsito aos demais veículos. E a terceira é o ataque *EvD - Aleatório* onde os ataques enviam sempre as medições de tráfego com valores aleatórios. Considera-se que os ataques *EvD* ocorrem pela exploração de vulnerabilidades resultantes de outros ataques ou por falhas na rede; e que o atacante *EvD* possui conhecimento da rede [Deng et al. 2016, Pedroso et al. 2019].

### 3.1. Arquitetura do RONDA

A arquitetura do RONDA compreende quatro módulos principais, denominados de **Análise de Deslocamento (AD)**, **Disseminação de Níveis de Congestionamento (D-NC)**, **Decisão de Novas Rotas (DR)** e **Segurança (SR)**, como ilustrados na Figura 2. Os módulos do sistema RONDA atuam de maneira coordenada para assegurar a comunicação de dados eficiente e segura na rede. O módulo AD monitora as condições de deslocamento na via onde o veículo realiza o seu percurso ao longo do tempo. Este módulo desempenha um papel importante, fornecendo as informações de tráfego aos módulos de segurança e de disseminando os níveis de congestionamento. O módulo *D-NC* encaminha as análises fornecidas pelo módulo AD aos veículos que viajam em vias adjacentes, para que seja possível criar um banco de dados de NC das vias adjacentes de cada veículo. O módulo *DR* leva em conta as informações armazenadas na base de dados para verificar a existência de novas rotas com menor incidência dos congestionamentos de tráfego, ou seja, DR atua na tomada de decisões. Observe que durante a execução do *D-NC*, veículos maliciosos/atacantes podem fornecer dados falsos sobre as condições das vias em que eles estão. Nesse cenário, as decisões tomadas pelo módulo DR podem ser realizadas considerando informações recebidas através dos ataques de envenenamento de dados.

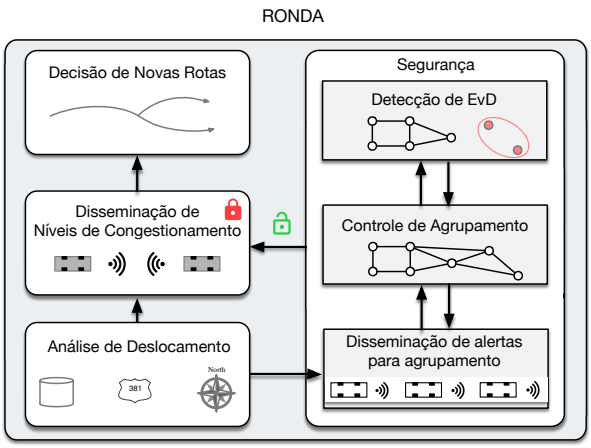



**Figura 2. Arquitetura do RONDA**

O módulo de **SR** controla a segurança dos dados de tráfego disseminados entre os veículos da rede tal que apenas dados autênticos estejam disponíveis. Ele consiste em três submódulos denominados de *Disseminação de Alertas de Agrupamento (DAA)*, *Controle de Agrupamento (CA)* e *Detecção de EvD (DA)*. O *DAA* atua na disseminação de mensagem de controle entre os veículos participantes da rede contendo as informações sobre a análise de deslocamento realizadas pelos veículos. O *CA* opera na criação de agrupamento de veículos na via e no monitoramento e verificação dos veículos que não respeitam o limiar de similaridade entre as informações tráfego disseminadas pelos veículos de uma determinada via. O *DA* atua na tomada de decisão e isolamento de ataques na rede, para isso ele emprega o consenso relacional e desvio padrão na detecção de veículos *EvD*. Assim, ao detectar um atacante os veículos participantes da detecção enviam um alerta ao líder do agrupamento. A mensagem enviada contém o $id_v$ do atacante *EvD* bem como sua medição de tráfego.

### 3.2. Gerenciamento de Tráfego

Esta seção apresenta como o RONDA realiza o gerenciamento de tráfego veicular. O modo de gerenciamento é baseado na solução proposta em [Gomides et al. 2020]. Durante o seu percurso nas vias da cidade, o veiculo constantemente monitora as condições do tráfego da via em que ele se encontra com base nas características do seu deslocamento e da via em questão. Esse monitoramento é realizado pelo módulo **AD**. Ao começar a se deslocar em uma via, o veículo monitora a Distância Percorrida (DP) e o Tempo de Viagem Verificado (TVV) na via. Considerando a velocidade permitida e o TVV, é possível estimar a Distância Esperada (DE) que deveria ter sido percorrida se a via possuir transito livre. Assim, se o veículo verificar que a DP for igual a DE, consideramos que o veículo realizou seu deslocamento em trânsito livre. Nesse caso, o nível de congestionamento da via é definido como 1. Entretanto, quando DP $<$ DE, o veículo verifica congestionamento em seu deslocamento e, quanto maior a diferença entre DP e DE, maior o nível de congestionamento verificado. Os níveis de congestionamentos variam de 1 (trânsito livre) até 10 (completamente congestionado). Mais detalhes sobre o cálculo dos níveis de congestionamento podem ser encontrados em [Gomides et al. 2020].

Cada veículo possui uma base de dados composta por tuplas $< via_{id}, valor >$, onde $via_{id}$ representa um $id$ único para cada via da malha viária da cidade e $valor$ representa uma de duas possibilidades: *(i)* valor desconhecido e *(ii)* valor do congestionamento da respectiva via. A atualização da base de dados ocorre em intervalos pré-definidos $t$, onde após cada $t$ segundos o veículo verifica quais vias adjacentes em sua base de dados estão marcadas como valor desconhecido. O veículo envia uma mensagem de $requisio$ com o destino $via_{id_i}$ a cada via $i$ com valor desconhecido em sua base de dados. Dentre os veículos que receberem a mensagem, aquele a mais tempo na via responde a requisição com a sua percepção do nível de congestionamento. Verificou-se que o veículo a mais tempo na via possui uma percepção estável do nível de congestionamento, desconsiderando rápidas acelerações ou desacelerações. A mensagem de resposta é recebida por todos os veículos dentro do raio de comunicação do veículo que enviou, inclusive o veículo requisitante. Assim, os veículos atualizam as suas respectivas bases de dados com o nível de congestionamento $< via_{id_i}, nivelCongestionamento >$. Uma requisição sem resposta é tratada como valor desconhecida na base de dados. As etapas para a criação da base de dados nos veículos são executadas no módulo **D-NC**.

Após a realização das requisições necessárias para obter as informações sobre o tráfego de veículos nas vias adjacentes, o veículo utiliza o modelo de rede baseado no grafo $G = (V, E)$ definido na Seção 3 para verificar se existem rotas com menores tempo de viagem. O módulo **DR** coordena essa etapa. Cada tupla $< via_{id}, valor >$ na base de dados é associada com uma aresta $e_{ij} = (v_i, v_j)$ e $w_{ij}$. Para valores de $via_{id}$ com valor desconhecido de congestionamento, considera-se um nível de congestionamento de 1. Isso acontece para que valores desconhecidos não interfiram nos valores recebidos. Após o ponderamento do grafo $G$, os veículos calculam o caminho de menor custo de congestionamento. Caso o novo caminho seja diferente do atual, existe uma rota alternativa a seguir, do contrário, o veículo já está no caminho de menor congestionamento.

A Figura 1(a) ilustra a execução do sistema de gerenciamento sem considerar a existência do ataques *EvD*. Utilizando os dados solicitados e recebidos dos veículos em vias vizinhas, o veículo verifica a existência de novos caminhos alternativos com menores congestionamentos. Entretanto, os veículos maliciosos podem responder a uma requisição com dados falsos (como ilustrado na Figura 1(b)), ocasionando que outros veículos, inclusive o requisitante, usem uma base de dados com informações incorretas na verificação de novos caminhos. A seguir, descreve-se o módulo de segurança do RONDA.

### 3.3. Gerenciamento de Segurança

A segurança da rede leva em conta as trocas de mensagens de controle entre os veículos a fim de identificar quais valores não respeitam ao limiar de similaridade das informações sobre o tráfego na via. O RONDA utiliza listas de atacantes para armazenar os veículos maliciosos que disseminam informações falsas. O uso das listas possibilita uma melhor avaliação sobre os veículos atuantes na rede, o que viabiliza uma detecção mais assertiva de atacantes *EvD*. Os agrupamentos formam-se a partir de veículos confiáveis na rede. Cada agrupamento é coordenado por um veículo líder, onde o líder é o veículo a mais tempo na via. Assim, apenas os veículos considerados honestos participam dos agrupamentos. O líder do agrupamento atua na exclusão de atacantes *EvD*, a partir das informações enviadas pelos outros veículos na rede. O Algoritmo 1 especifica o funcionamento dos procedimentos para detecção de falhas na rede diante dos ataques de *EvD*. A detecção inicia a atuação juntamente com as primeiras trocas de mensagem de controle, uma vez que os veículos necessitam de outras informações para executar a comparação entre os dados de tráfego das vias.

As mensagens de controle são enviadas pelo submódulo *DAA* por meio da utilização de *beacons* periódicos. Ao receber uma mensagem de controle $(msg)$, o veículo executa o procedimento **Controle de Agrupamentos** e ele tem como objetivo determinar quais veículos fazem parte do agrupamento da via e quais veículos fazem ou não parte da listas de suspeitos e atacantes. Assim, ao receber uma mensagem de controle, o veículo receptor verifica as informações enviadas e confere se veículo $(EmitterVehicle)$ faz parte ou não de sua vizinhança de via $(NeighborList)$ (*l*.2). Caso o emissor faça parte da vizinhança, ou seja, o veículo previamente já enviou uma informação dentro do *Thresholdconsensus*, ele armazena as informações de tráfego $(NeighborTraffic)$ e o tempo de viagem na lista $(NeighborTravelTime)$. O tempo de viagem é utilizado para a definição do líder do agrupamento. Caso o emissor não faça parte da vizinhança, realiza-se a verificação na lista de $(SuspectList)$ ou $(AttackerList)$ (*l*.5). Se a informação enviada respeita o *Thresholdconsensus* pré-estabelecido, a lista de vizinhos e o conjunto

**Algoritmo 1:** Segurança Contra Ataques EvD

```
1  procedure CONTROLE DE AGRUPAMENTO (msg)
2      if msg.EmitterVehicle ∈ NeighborList then
3          NeighborTraffic ⟵ NeighborTraffic ∪ msg.TrafficMeasure
4          NeighborTravelTime ⟵ NeighborTravelTime ∪ msg.TravelTime
5      else if msg.EmitterVehicle ∉ AttackerList, SuspectList then
6          if msg.TrafficMeasure ≤ Thresholdconsensus then
7              NeighborList ⟵ NeighborList ∪ msg.EmitterVehicle
8              NeighborTraffic ⟵ NeighborTraffic ∪ msg.TrafficMeasure
9          else
10             SuspectList ⟵ SuspectList ∪ msg.EmitterVehicle
11 end procedure
12 procedure DETECÇÃO DE ATAQUES EVD (msg)
13     if msg.EmitterVehicle ∈ SuspectList then
14         SuspectsList[msg.EmitterVehicle] + +
15     if SuspectsList[msg.EmitterVehicle] > thresholdattack then
16         AttackerList ⟵ AttackerList ∪ msg.EmitterVehicle
17         BroadcastMessage("DetectedAttacker", Attacker = msg.EmitterVehicle)
18 end procedure
19 procedure EXCLUSÃO POR CONSENSO (msg)
20     if AmILeader then
21         if msg == "DetectedAttaker" then
22             AttackerListLeader[msg.Attacker] + +
23             if AttackerListLeader[msg.Attacker] > thresholdattack then
24                 BroadcastMessage("Attackerbyconsensus", msg.Attacker)
25 end procedure
```

de informações recebidas são atualizadas (*l*.7 e *l*.8), caso contrário, a lista *SuspectList* é atualizada.

O procedimento **Detecção de Ataques EvD** também é executado sempre que um veículo recebe uma mensagem de controle $(msg)$. O procedimento verifica quais veículos estão atuando como atacantes na rede. Se o veículo que enviou a mensagem pertence a lista de suspeitos do veículo que recebeu (*l*.13), é feito um incremento no contador de quantas vezes aquele veículo foi classificado como suspeito. Se o contador de verificação for maior que o $thresholdattack$ pré-definido (*l*.15), o veículo é classificado como atacante e uma mensagem de alerta é enviada para os veículos do agrupamento (*l*.16 e *l*.17). O procedimento **Exclusão por Consenso** realiza a exclusão dos veículos atacantes do agrupamento realizado na via. O líder de um agrupamento é o veículo que está a mais tempo na via, e essa verificação é realizada utilizando a lista de tempos de viagens dos veículos na via ($NeighborTravelTime$). Como o líder é dinâmico e varia com o tempo, o veículo verifica se ele é o veículo líder naquele instante (*l*.20). Sendo líder, o veículo verifica se a mensagem recebida é do tipo "$DetectedAttacker$" e, em caso afirmativo, o veículo atualiza a quantidade de vezes que esse tipo de mensagem foi recebida devido ao mesmo atacante (*l*.22). Se a quantidade de mensagens recebidas for superior a $thresholdattack$, o veículo líder notifica todos os vizinhos na via que um atacante *EvD* foi descoberto por consenso. É importante ressaltar que a lista $NeighborTravelTime$ é inicializada a cada intervalo de envio de mensagens *beacons*. Assim, se um veículo mudar de via, ele enviará sua mensagem de controle $(msg)$ em uma nova via e não participará

do agrupamento da via anterior, uma vez que cada veículo está presente em apenas um agrupamento em um dado momento.

$$DP = \sqrt{\frac{\sum_{i=1}^{n} (X_i - M_A)^2}{N}} \leq Thresholdconsensus \quad (1)$$

A Equação 1 aplica-se para computar o consenso relacional considerando os valores aferidos pelos veículos. Dessa forma, usam-se os dados de leituras coletados pelos veículos participantes da rede para formar o consenso e compará-las entre eles. Assim, utiliza-se um conjunto de dados $D = (d_i, d_{i+1}, ..., d_n)$, que representa as amostras a serem verificadas. O cálculo do consenso, indicado por $\sum_{i=1}^{n}$, compreende o somatório dos valores do conjunto $D$, da primeira posição $(i = 1)$ até posição $n \in N$. O valor de $X_i$ é referenciado na posição $i$ do conjunto $D$ de dados. $M_A$ representa a média aritmética dos dados. A quantidade de dados avaliadas na formação do consenso representa-se por $N$. O limiar consensual denominado ($Thresholdconsensus$), expressa o valor pré-definido, e que pode variar conforme o tipo de dados avaliados e a aplicação onde ele atua. Neste sentido, o consenso relacional abrange a concordância, relação e uniformidade de opiniões que os veículos estabelecem por meio de troca de informações entre eles. Estas informações relacionam-se aos dados disponíveis em cada veículo e são associadas aos demais veículos para validação sobre ataques *EvD*.

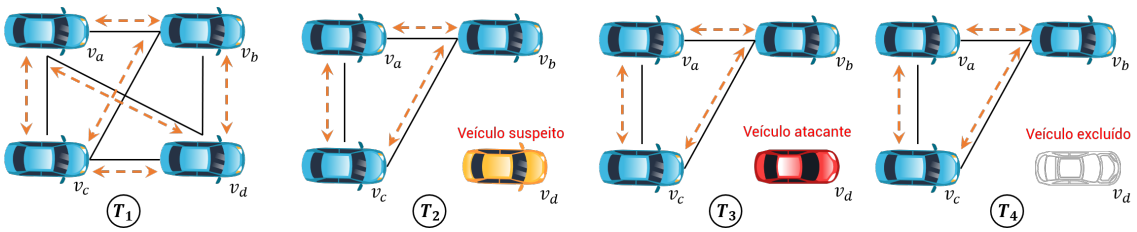



**Figura 3. Formação de consenso relacional entre os veículos**

A Figura 3 ilustra a atuação do consenso relacional entre os veículos para a detecção um atacante *EvD*. As setas pontilhadas representa a comunicação entre os veículos. No instante $T1$, os veículos $v_a$, $v_b$, $v_c$, $v_d$ realizam a troca de informações de controle. No instante $T_2$, apenas os veículos ($v_a$, $v_b$, $v_c$) agrupam-se, visto que eles respeitam o limiar de similaridade das informações sobre o tráfego contidas na mensagem de controle. Entretanto, a informação enviada pelo veículo $v_d$ não respeita este limiar, fazendo com que ele seja classificado como veículo suspeito. Em $T_3$, o veículo $v_d$ envia novamente mensagens de controle para tentar fazer parte do agrupamento. O conjunto formado pelos veículos ($v_a$, $v_b$, $v_c$) executam o cálculo da Equação 1 e classificam o veículo $v_d$ como atacante, já que ele novamente possui leituras divergentes em relação às leituras dos veículos do conjunto. Por fim, em $T_4$ ilustra a situação onde as mensagens do veículo $v_d$ são desconsideradas, uma vez que ele não participará do agrupamento. Assim, a segurança é mantida de forma distribuída pelos próprios participantes sem a necessidade de entidade externas.

Durante toda a viagem, o módulo **AD** é executado fornecendo informações aos módulos **D-NC** e **SR**. **D-NC** permite os veículos solicitarem os níveis de congestionamentos dos veículos que viajam em vias adjacentes. *SR* possibilita aos veículos se agruparem para detecção e exclusão de veículos atacantes. Os dados obtidos por *D-NC*, após a

exclusão das informações provenientes dos veículos atacantes, são utilizados pelo módulo *DR* para o cálculo de novas rotas.

## 4. Avaliações

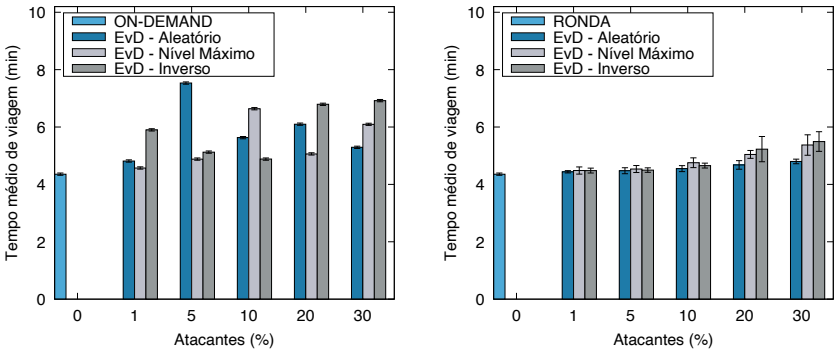
Esta seção descreve a avaliação de desempenho do RONDA em detectar e mitigar ataques *EvD* para proporcionar um ambiente seguro ao gerenciamento de tráfego. Para validar a eficiência de segurança, o sistema foi comparado ao sistema de gerenciamento de tráfego ON-DEMAND [Gomides et al. 2020]. Ambos foram implementados utilizando um conjunto de ferramentas que permitem a simulação da comunicação veicular, mobilidade urbana e também o modelo de ataque *EvD*. O SUMO 0.25 (*Simulation of Urban Mobility* gerencia e executa a mobilidade veicular, o OMNET++ 5.1.1 e Veins 4.6 auxiliam na simulação da comunicação. A operação do sistema é realizada num mapa com 120 vias com um *layout* de *Manhattan grid* em uma região de 1 km$^2$ e, para cada simulação, foram avaliados uma densidade de 1000 veículos/km$^2$. Cada veículo possui uma rota formada por uma via origem e uma via destino escolhidas de maneira aleatória em cada simulação. Além disso, o RONDA considera a disseminação de mensagens periódicas em intervalos de 2 segundos e, para os limiares $thresholdattack$ e $thresholconsensus$, o valor 3.

As avaliações foram executadas para diferentes tipos de porcentagens de veículos atacantes *EvD* e três variações de ataques. As porcentagens avaliadas foram 0%, 1%, 5%, 10%, 20% e 30% de veículos atacantes e os tipos de ataques *EvD Aleatório*, *Nível Máximo* e *Inverso* foram implementados, seguindo o modelo descrito em [Deng et al. 2016], onde os atacantes alteram os dados de leitura de uma matriz de energia. Assim, são inseridos dois tipos de dados, um visando pequenas alterações e outro com alteração inversas. Buscando uma melhor adequação ao nosso cenários foi acrescido o modelo aleatório que pode atuar de ambas as formas descritas acima e também injetando dados mais próximos aos coletados, dificultando sua detecção. Assim, são selecionados veículos específicos para agirem como atacantes na rede. Para fins de comparação, as avaliações incluíram métricas de desempenho, relacionadas à capacidade dos sistemas de minimizar os efeitos do congestionamento de tráfego e, métricas de segurança, que descrevem como o RONDA identifica e gerencia os invasores. No entanto, as avaliações de segurança têm como objetivo estimar somente o comportamento do RONDA. As métricas aplicadas foram: **Tempo de Viagem (TV)**, **Taxa de Detecção de Atacantes (TD)**, **Acurácia (AC)**, **Falsos Positivos (FP)**, **Falsos Negativos (FN)**, **Taxa de Detecção de Atacante por Consenso (TDC) Consenso Positivo (CP)** e **Consenso Negativo (CN)**. Os gráficos apresentados foram obtidos a partir de 33 simulações de cada cenário com um intervalo de confiança de 95%.

### 4.1. Resultados

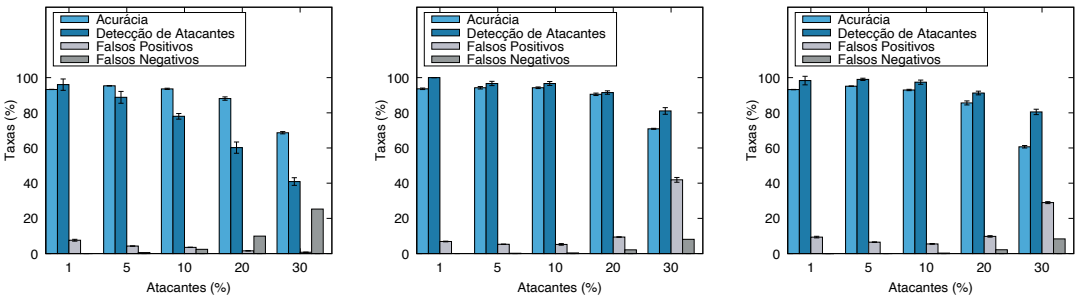
Os gráficos da Figura 4 descrevem o desempenho através da análise do deslocamento, contemplando as soluções RONDA e ON-DEMAND. Os eixos x e y representam a variação da porcentagem de veículos atacantes e o tempo médio de viagem em minutos, respectivamente. As duas soluções têm comportamento semelhantes para 0% de atacantes, pois ambas derivam do mesmo modelo proposto em [Gomides et al. 2020]. A medida que o número de atacantes aumenta, os sistemas apresentam comportamentos diferentes. Destaca-se que para todos os ataques e porcentagens avaliadas, o RONDA apresenta um desempenho superior. Além disso, nota-se uma redução no desempenho à medida que

o número de invasores aumenta e, consequentemente, a frequência com que o envenenamento de dados é realizado. Para 5% de atacantes, o RONDA apresenta redução dos tempos de viagens comparado com o ON-DEMAND em 40%, 7% e 12% em relação aos ataques *EvD* aleatório, nível máximo e inverso, nessa ordem. Considerando 20% de atacantes, o RONDA reduz em 23% para o aleatório, 1% para nível máximo e 24% para inverso, em comparação com o ON-DEMAND.




(a) ON-DEMAND (b) RONDA

**Figura 4. Eficácia no gerenciamento de tráfego com ataque EvD**

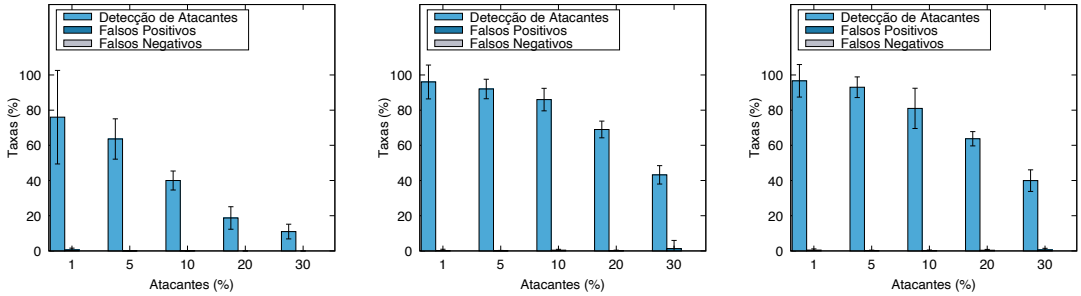



(a) Aleatório (b) Nível Máximo (c) Inverso

**Figura 5. Detecção de atacantes EvD**

Os gráficos da Figura 5 apresentam os resultados relacionados a detecção, acurácia, falsos positivos e falsos negativos obtidos pelo RONDA considerando os três tipos de ataques *EvD*. Observa-se que a solução proposta alcançou uma média de 87% de detecção para alguns cenários e atingindo uma média de 100% para alguns casos. Essa boa taxa detecção corrobora-se com as baixa taxas de falsos positivos e negativos, onde o sistema obteve em média 4% para falso positivos e 10% para falsos negativos. Além disso, os valores de acurácia alcançados pelo sistema variou entre 0,85 e 0,89, demonstrando a alta capacidade de detectar atacantes corretamente. As detecções erradas também são decorrentes de erros no cálculo de consenso entre os veículos monitores de um atacante, que pode apresentar baixo desvio de suas leituras. Em um primeiro momento eles são considerados suspeitos, porém conforme as novas interações e troca de mensagens entre os veículos acontecem, os novos cálculos identificam os valores corretos. A efetividade na detecção deve-se a o monitoramento *watchdog* entre todos os participantes da rede. Além disso, a utilização das listas de suspeitos e atacantes *EvD* garantem uma detecção asser-

tiva sobre todos os três tipos de ataques *EvD*. Também observa-se que até com 20% de veículos atacantes, o comportamento do sistema manteve-se estável à todas as avaliações.




(a) Aleatório (b) Nível Máximo (c) Inverso

**Figura 6. Exclusão de atacantes por consenso**

Os gráficos da Figura 6 apresentam os resultados da eficácia do consenso relacional para a exclusão dos três tipos de atacantes *EvD*. Este tipo de exclusão visa considerar as informações de atacantes que foram detectados por pelo menos três veículos na rede ($thresholconsensus$). Assim, para ambos os cenários são avaliadas as taxas de exclusão, falsos negativos e falsos positivos obtidas pelo RONDA. Observa-se que para os ataques de nível máximo e inverso, o sistema se manteve estável com uma taxa de exclusão entre 75% e 80% e alcançando 97% em alguns casos. Destaca-se que o ataque *EvD* aleatório apresentou os piores resultados entre os demais devido ao fato de seu comportamento ser imprevisível em relação aos outros. Evidencia-se que os taxas de consenso positivo e negativo variaram entre 0,4% e 9%, demonstrando que apenas os verdadeiros atacantes são excluídos da rede. Essa eficiência na exclusão dos atacantes ocorre pela aplicação do consenso relacional entre os veículos da rede e que considera as interações entres o veículos que detectaram algum dos tipos de atacante *EvD*.

## 5. Conclusão

Este trabalho apresentou o sistema RONDA para gerenciamento de tráfego eficiente e seguro na presença de ataques *EvD* em VANETS. O sistema coleta e dissemina informações de trânsito a fim de criar novas rotas com melhores tempos de viagem em cenários de congestionamento. O sistema apoia-se no uso de monitoramento *watchdog* para vigiar os veículos na rede e no consenso relacional distribuído por similaridade entre os veículos vizinhos para detectar ataques *EvD*. Os resultados demonstram e eficácia do RONDA na detecção, mitigação e isolamento de veículos atacantes *EvD*, assegurando que apenas dados de tráfego autênticos estejam disponíveis à criação da base de dados, e um tempo de viagem similar ao ON-DEMAND. Como trabalhos futuros, pretende-se aprimorar a propagação de alertas e disseminação de NC sem que os ganhos alcançados pelo RONDA sejam minimizados. Além disso, pretende-se avaliar o desempenho do sistema proposto considerando *traces* veiculares realísticos como o de Colônia e Luxemburgo.

## Referências

Arif, M., Wang, G., Zakirul Alam Bhuiyan, M., Wang, T., and Chen, J. (2019). A survey on security attacks in vanets: Communication, applications and challenges. *Vehicular Communications*, 19:100179.

Deng, R., Xiao, G., Lu, R., Liang, H., and Vasilakos, A. V. (2016). False data injection on state estimation in power systems—attacks, impacts, and defense: A survey. *IEEE Trans. on Industrial Informatics*, 13(2):411–423.

Gomides, T. S., De Grande, R. E., de Souza, A. M., Souza, F. S., Villas, L. A., and Guidoni, D. L. (2020). An adaptive and distributed traffic management system using vehicular ad-hoc networks. *Computer Communications*, 159:317 – 330.

Guidoni, D. L., Maia, G., Souza, F. S. H., Villas, L. A., and Loureiro, A. A. F. (2020). Vehicular traffic management based on traffic engineering for vehicular ad hoc networks. *IEEE Access*, pages 45167–45183.

Kamel, J., Ansari, M. R., Petit, J., Kaiser, A., Jemaa, I. B., and Urien, P. (2020). Simulation framework for misbehavior detection in vehicular networks. *IEEE Transactions on Vehicular Technology*, 69(6):6631–6643.

Khan, M. A., Sheikh, M. S., and Liang, J. (2019). A comprehensive survey on vanet security services in traffic management system. *Wireless Communications and Mobile Computing*, 2019:1 – 23.

Li, B., Lu, R., Wang, W., and Choo, K.-K. R. (2017). Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. *Journal of Parallel and Distributed Computing*, 103:32–41.

Lima, M. N., dos Santos, A. L., and Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks. *IEEE Communications Surveys and Tutorials*, 11(1):66–77.

Lu, Z., Qu, G., and Liu, Z. (2019). A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. on Intelligent Transp. Sys.*, 20(2):760–776.

Pan, J., Popa, I. S., and Borcea, C. (2017). Divert: A distributed vehicular traffic re-routing system for congestion avoidance. *IEEE Trans. on Mobile Computing*, 16(1):58–72.

Pedroso, C., Gielow, F., Santos, A., and Nogueira, M. (2019). Mitigação de Ataques IDFs no Serviço de Agrupamento de Disseminação de Dados em Redes IoT Densas. In *Anais SBSeg 2019*, Porto Alegre, RS, Brasil. SBC.

Santos, A. L., Cervantes, C. A., Nogueira, M., and Kantarci, B. (2019). Clustering and reliability-driven mitigation of routing attacks in massive iot systems. *JISA*, 10(1):18.

Sen, A. and Madria, S. (2017). Risk assessment in a sensor cloud framework using attack graphs. *IEEE Transactions on Services Computing*, 10(6):942–955.

Soriano, F. R., Samper-Zapater, J. J., Martinez-Dura, J. J., Cirilo-Gimeno, R. V., and Martinez Plume, J. (2018). Smart mobility trends: Open data and other tools. *IEEE Intelligent Transportation Systems Magazine*, 10(2):6–16.

Thakur, A. and Malekian, R. (2019). Fog computing for detecting vehicular congestion, an internet of vehicles based approach: A review. *IEEE Intelligent Transportation Systems Magazine*, 11(2):8–16.

Toulouse, M., Minh, B. Q., and Curtis, P. (2015). A consensus based network intrusion detection system. In *2015 5th International Conference on IT Convergence and Security (ICITCS)*, pages 1–6. IEEE.

Wang, S., Djahel, S., Zhang, Z., and Mcmanis, J. (2016). Next road rerouting: A multiagent system for mitigating unexpected urban traffic congestion. *IEEE Transactions on Intelligent Transportation Systems*, 17:1–12.

Zhang, C., Chen, K., Zeng, X., and Xue, X. (2018). Misbehavior detection based on support vector machine and dempster-shafer theory of evidence in vanets. *IEEE Access*, 6:59860 – 59870.