UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São José do Rio Preto

Edivaldo Pastori Valentini

Um Mecanismo de Detecção de Ataques para Sistema de Transporte Inteligente

São José do Rio Preto
2020

Edivaldo Pastori Valentini

Um Mecanismo de Detecção de Ataques para Sistema de Transporte Inteligente

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Ciência da Computação, junto ao Programa de Pós-Graduação em Ciência da Computação, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Orientador: Prof. Dr. Rodolfo Ipolito Meneguette

São José do Rio Preto
2020

V161m

Valentini, Edivaldo Pastori

Um mecanismo de detecção de ataques para sistema de transporte inteligente / Edivaldo Pastori Valentini. -- São José do Rio Preto, 2020

114 f. : tabs., mapas

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto

Orientador: Rodolfo Ipolito Meneguette

1. Sistemas de Transporte Inteligente. 2. Redes ad hoc veiculares. 3. Computadores Medidas de segurança. 4. Sistemas de detecção de intrusão. 5. Ataques de negação de serviço. I. Título

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Edivaldo Pastori Valentini

Um Mecanismo de Detecção de Ataques para Sistema de Transporte Inteligente

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Ciência da Computação, junto ao Programa de Pós-Graduação em Ciência da Computação, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Comissão Examinadora

Prof. Dr. Rodolfo Ipolito Meneguette
UNESP – Câmpus de São José do Rio Preto
Orientador

Profª. Drª. Kalinka Regina Lucas Jaquie Castelo Branco
USP – São Carlos

Profª. Drª. Renata Spolon Lobato
UNESP – Câmpus de São José do Rio Preto

São José do Rio Preto
3 de setembro de 2020

Dedicatória

Dedico este trabalho a Deus.
Aos meus amáveis e queridos pais, José Edivaldo e Eudite Maria.
À minha amada esposa, Ligiane.
Ao meu carinhoso e divertido filho, Vítor.

AGRADECIMENTOS

A Deus Pai criador, sagrada Família e a luz do Espírito Santo.

Aos meus pais, José Edivaldo Valentini e Eudite Maria Pastori Valentini, obrigado pelo dom da vida.

À minha esposa e amiga, Ligiane Cristina Pereira Valentini, obrigado pelo seu amor, carinho e força nesta caminhada.

Ao meu pequeno, Vítor Pereira Valentini, obrigado pelos seus divertidos e fortalecedores desenhos. Perdoe-me pelos momentos que não pudemos jogar futebol.

À minha querida irmã, Giovana Pastori Valentini, pelo seu carinho.

Ao meu orientador e amigo, Prof. Dr. Rodolfo Ipolito Meneguette, pelos grandes ensinamentos, confiança e paciência. E, também, pela grande força para que eu pudesse realizar este sonho. Meu eterno obrigado.

Ao IFSP Câmpus Catanduva, pelo grande apoio e possibilidade deste aprendizado.

Ao IBILCE/UNESP, Servidores e Professores(as), pelo acolhimento e magnífica oportunidade pela busca do saber.

Aos meus doces e carinhosos avós, Valdir e Gilda Valentini e Domingos e Ilma Pastori.

Aos meus queridos familiares, sogra Maria Helena, Tios José Roberto e Zilda, e sogro Lidio. Pequenas e lindas Maria Clara e Laura. Tia Nice, Valdemar, Fer e Dani. Cunhado Rodrigo. Tia Vilma, Toninho, Gabi e Rafa. Tia Maria, Eurides, Ana, Lucas, Alícia e Ben. Tio Lique, sempre animado. Tia Darlene, Moisés, Fabiane e Gabriel. Primão Marcelo, doce Gislâine e inteligentes Luiz Marcelo e Guzão.

Aos grandes amigos, Toninha e Zé Flores, Camões e Rafa Pelarin.

Aos meus primeiros professores de informática, Silmara Xavier, Anderson Perez, Osvaldo Perez (Dico) e José Manoel Lima (Zeca).

Ao grande Professor Júlio Lieira, pela amizade, força e sempre muito atencioso.

Às pessoas queridas e amáveis, Scott E Carpenter (EUA), Adil Alsuhaim (EUA), Giovana Sampaio e Maria Célia Guilan. Minha eterna gratidão.

À Caio Pena, Chris Sanders, Daniel Lobato, Joahannes Costa, Jason Brownlee, Márcio Andrey Teixeira, Marcos Silveira, Matthew Kirk (Matt), Milena Brito, Osvaldo Severino Jr, Pradeep Kumar, Rodrigue Tchamna e professor Vilmar Pedro Votre, muito obrigado.

“[...] apesar de sua condição divina, ele não reivindicou seu direito de ser tratado como igual a Deus. [...] Por seu aspecto, reconhecido como homem, humilhou-se, fazendo-se obediente até a morte, e morte de cruz. Por isso Deus o elevou acima de tudo e lhe deu o Nome que está acima de todo nome, de modo que ao nome de Jesus todo joelho se dobre nos céus, na terra e debaixo da terra, e toda língua proclame que Jesus Cristo é o Senhor, para a glória de Deus Pai.”

Filipenses 2, 6-11

RESUMO

O aumento das tecnologias computacionais aos meios de transportes, principalmente nos veículos, tem proporcionado grandes benefícios através dos Sistemas de Transporte Inteligente (STI). Condutores, passageiros e pedestres, usufruem de aplicações computacionais dirigidas à proteção da vida humana, entre agilidades na prestação de socorro, melhorias no trânsito e até recursos de lazer e entretenimento. A comunicação e a troca de dados, entre veículos, aplicações e dispositivos de transmissão, são realizadas pela arquitetura de rede *ad hoc* veicular (VANET). No entanto, este tipo de rede difere das tradicionais, pois opera em um ambiente altamente dinâmico, originado pela rápida mobilidade entre seus nós e com curtos intervalos de conexões. A comunicação sem fio adota o padrão IEEE 802.11p, a qual permite que os veículos operem fora de um conjunto básico de serviços. Na presença destas características, surgem inúmeras superfícies de ataques, ameaças e exploração de vulnerabilidades. Buscando melhorar a segurança e a proteção da vida humana, envolvidas neste ambiente, justificamos nosso estudo em proporcionar melhorias aos sistemas de transporte inteligente. Motivados a desenvolver um mecanismo de segurança para detecção de intrusão e ameaças, inerentes aos recursos computacionais do cenário de transporte. Levando em consideração as limitações de hardware e software, empregou-se a técnica de detecção de anomalias por meio de modelos estatísticos. Veículos identificados como suspeitos serão armazenados em uma lista de reputação, para finalidades informativas. A implementação, análises e validação dos resultados são realizadas por meio do processo de simulação. Neste trabalho utilizou-se o simulador de redes - *Network Simulator* 3.30, para implementação da rede veicular. Para simulações reais da mobilidade e do tráfego urbano, foi aplicado o simulador SUMO 1.5.0.

Palavras–chave: Sistemas de Transporte Inteligente. Redes Veiculares. Segurança da Informação. Sistema de Detecção de Intrusão. Ciberataques.

ABSTRACT

The increase of computational technologies to the means of transport, mainly in vehicles, has provided great benefits through Intelligent Transport Systems (STI). Drivers, passengers and pedestrians enjoy computer applications aimed at protecting human life, including agility in the provision of assistance, improvements in traffic and even leisure and entertainment resources. Communication and data exchange between vehicles, applications and transmission devices are carried out using the vehicle ad hoc network architecture (VANET). However, this type of network differs from traditional ones, as it operates in a highly dynamic environment, originated by the rapid mobility between its nodes and with short connection intervals. Wireless communication adopts the IEEE 802.11p standard, which allows vehicles to operate outside a basic set of services. In the presence of these characteristics, numerous surfaces of attacks, threats and exploitation of vulnerabilities arise. Seeking to improve the safety and protection of human life, involved in this environment, we justify our study in providing improvements to intelligent transport systems. Motivated to develop a security mechanism for intrusion and threat detection, inherent to the computational resources of the transport scenario. Taking into account the limitations of hardware and software, anomaly detection technique using statistical models was used. Vehicles identified as suspicious will be stored on a reputation list for informational purposes. The implementation, analysis and validation of the results are carried out through the simulation process. In this work, the network simulator - Network Simulator 3.30 was used to implement the vehicular network. For real simulations of mobility and urban traffic, the SUMO 1.5.0 simulator was applied.

Keywords: Intelligent Transport Systems. Vehicle Networks. Information Security. Intrusion Detection System. Cyberattacks.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

ARP	Address Resolution Protocol
BSS	Basic Service Set
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSRC	Dedicated Short-Range Communication
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GPS	Global Positioning System
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.11p	Protocolo padrão de redes sem fio veiculares
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITS	Intelligent Transport System
MAC	Media Access Control
MANET	Mobile ad hoc Network
OBU	On-Board Units
OICA	International Organization of Motor Vehicle Manufactures
OLSR	Optimized Link State Routing Protocol
OMS	Organização Mundial de Saúde
OSI/ISO	Open System Interconnection / International Organization for Standardization

OWASP	Open Web Application Security Project
PCAP	Packet CAPture
RSU	Road Side Units
SDI	Sistema de Detecção de Intrusão
STI	Sistema de Transporte Inteligente
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to all
VANET	Vehicular ad hoc Network
WAVE	Wireless Access Vehicular Environments
XML	Extensible Markup Language

SUMÁRIO

1 INTRODUÇÃO

Os meios de transporte sempre serão um dos principais requisitos para que a sociedade moderna continue a crescer, evoluir e inovar-se. Necessitamos de meios de transportes ágeis, econômicos e, principalmente seguros. Diversas inovações, como por exemplo, sistemas embarcados, comunicação sem fio, condução autônoma, entre outras, são aplicadas em um simples carrinho de bebê até em carros, navios e aviões modernos. Este avanço também inclui as infraestruturas de rodovias, vias urbanas e todos os elementos que constituem o campo do transporte.

Diante de constantes modernizações nos deparamos com o paradigma do Sistema de Transporte Inteligente (STI), ou *Intelligent Transport System* (ITS), que se institui, gradativamente, em um ecossistema cooperativo e colaborativo, realizando a comunicação de informações entre veículos, veículos e infraestruturas de estrada e infraestruturas de serviços de nuvem e Internet. Redução de congestionamento, eficiência do tráfego, sustentabilidade, segurança e respeito com o meio ambiente, são alguns dos benefícios favorecidos pelo STI (ALAM; FERREIRA; FONSECA, 2016).

Uma pesquisa realizada pela Organização Mundial de Saúde (OMS, 2016), verificou-se que o número de óbitos ocorridos no trânsito, no ano de 2016, chegou em aproximadamente 1,4 milhão de pessoas. Infelizmente, esse número encontra-se na oitava posição dentre as dez principais causas de mortes mundialmente. Desta totalidade, 74% estão entre homens jovens e adultos.

Outros dois fatores que necessitam de atenção – é o aumento da quantidade de veículos (OICA, 2015) e a crescente incorporação de novas tecnologias no meio automotivo (STATISTA, 2020a). Fatores preocupantes que poderão trazer inúmeras consequências sociais e ambientais, como exemplo o descarte de veículos inutilizados e a má utilização insconsciente destas novas tecnologias, elevando o índice de acidentes, perigos no trânsito e novas trágicas consequências.

Os recursos do STI também evidencia o emergente campo das Cidades Inteligentes (CI), ou *Smart Cities*. Trata-se de outro paradigma que proporciona inúmeros sistemas que buscam melhorar a vida dos cidadãos do âmbito urbano. Uma grande integração entre diferentes dispositivos e tecnologias interconectadas pelos processos da Internet das Coisas (*Internet of Things* – IoT), favorecendo a execução de diferentes serviços. Por exemplo, a coleta de informações, por meio de

sensores climáticos, dispositivos móveis, semáforos inteligentes, veículos conectados entre outros, que possibilitarão o gerenciamento e análises de dados por pessoas, órgãos municipais e organizações. Plataformas de nuvens são utilizadas tanto para o armazenamento dos dados coletados, quanto para ofertar inúmeros serviços e aplicações dentro do âmbito urbano (FERRAZ & FERRAZ, 2014).

A abstração operacional e funcional desses dois emergentes paradigmas STI e CI é estruturada com base na integração de tecnologias da informação e comunicação (TICs) (ALAM; FERREIRA; FONSECA, 2016). Entretanto, quanto mais tecnologias interconectadas e informações compartilhadas dentro do aspecto urbano, maiores serão os riscos da segurança da informação (FERRAZ & FERRAZ, 2014).

Independente da natureza dos dados (pessoais, públicos, privados), estes poderão ser expostos por uma ampla gama de ataques, vulnerabilidades e ameaças. Um exemplo infelizmente culminado em morte, inerente ao cenário de transporte urbano, ocorreu na cidade de Niterói-RJ, Brasil (G1; VEJA, 2015). Causado por falhas e a má operação da tecnologia do sistema de posicionamento global (GPS), que orienta o motorista a conduzir seu veículo por melhores rotas por meio de informações fornecidas pela aplicação, acabou colocando o veículo de um casal em situações de perigo e levando uma mulher à morte.

Outra situação real, que foi praticada pelos pesquisadores Miller e Valasek (2015), na qual executam um ataque a um veículo Jeep por meio da injeção de um programa computacional malicioso (*malware*). Este fato também ocorreu em um cenário urbano, em que pesquisadores “atacantes” controlaram o veículo remotamente, executando operações e comandos através da internet. Bloqueios nas ações do condutor, manipulação da central multimídia, aceleração do automóvel, manuseio da direção e até mesmo frear o veículo, foram algumas das consequências decorrentes do ataque (GREENBERG, 2015).

Tais situações de perigo podem aumentar em um breve futuro, caso não sejam estabelecidos sistemas e ferramentas de segurança.

Países como Estados Unidos, Japão, União Europeia, Canadá, entre outros estão fortemente incumbidos em estudos e pesquisas direcionadas para o campo de transportes, especificamente aos sistemas de transporte inteligente. Melhorar somente infraestruturas de construções de tráfego, como vias expressas, inclusão de novas avenidas e viadutos etc, não resolverão os problemas primordiais e, ainda,

poderão gerar problemas maiores (AN; LEE; SHIN, 2011). A interação destes dispositivos e elementos entre si, considerando as arquiteturas existentes dos países acima, é um dos desafios pela busca da padronização dos sistemas de transporte inteligente (MENEGUETTE; GRANDE; LOUREIRO, 2018).

No ambiente do STI a transmissão de informações é realizada de modo cooperativo, distribuído e, ao longo do trajeto, implementa-se uma rede classificada como rede veicular *ad hoc*. Conhecida também como VANET (*Vehicular ad hoc Network*), sua comunicação será de veículos entre veículos, veículos e infraestruturas de estrada, e infraestruturas de serviços de nuvem e Internet (ALAM; FERREIRA; FONSECA, 2016; HASROUNY et al., 2017; MENEGUETTE; GRANDE; LOUREIRO, 2018). Por meio da tecnologia de comunicação sem fio de curto alcance, os veículos e infraestruturas trocam informações entre si, seguindo por uma topologia de rede dinâmica, com alta mobilidade e sem a necessidade de uma entidade centralizadora. Tais características peculiares e aplicações em tempo real, específicas ao domínio de transporte, tornam as VANETs distintas das tradicionais redes de computadores, surgindo assim, inúmeros desafios na implementação da segurança em VANETs (HASROUNY et al., 2017; MENEGUETTE; GRANDE; LOUREIRO, 2018).

A existência de nós mal-intencionados ou denominados intrusos poderá exercer inúmeras atividades maliciosas prejudicando o sistema de transporte como, por exemplo, congestionamentos da rede, envio de falsos alertas, roubos de identidades, falsificações de localização e exploração de vulnerabilidades de protocolos de roteamento, que são resultantes de ameaças e ataques (HASROUNY et al., 2017; SAKIZ; SEN, 2017). Além disso, um ataque de negação de serviço resultaria em trágicas consequências, em aplicações que demandam tempo real, implicando atrasos nas operações de socorro e resgates de acidentes.

1.1 Justificativa e Motivação

Buscando melhorar a segurança e a proteção da vida humana dos ocupantes de veículos e dos pedestres, a justificativa deste estudo é contribuir e proporcionar melhorias aos sistemas e tecnologias computacionais direcionados ao transporte inteligente.

Mediante a esses fatos graves, ocorridos no trânsito, fortalecem o motivo de propor um mecanismo de segurança para detectar ataques e ameaças direcionados às VANETs e aos dispositivos do STI. Assim sendo, criar possibilidades para minimizar perigos e riscos de mortes, mitigando ações maliciosas dos atacantes.

1.2 Objetivo

O objetivo geral deste trabalho é implementar a segurança e proteção dos nós pertencentes ao ambiente STI, direcionados ao tráfego urbano, no qual a densidade de veículos é maior e mais propenso a reencontros diante da rotina cotidiana.

Baseado na análise da troca de informações entre veículos e/ou infraestruturas da rede veicular, a detecção de ataques é realizada no próprio veículo individualmente, ou seja, baseada em *host*.

1.2.1 Objetivos específicos

Este trabalho busca atingir os seguintes objetivos específicos:

(i) Desenvolver um mecanismo de segurança para o sistema de transporte inteligente direcionado à rotina do tráfego urbano;

(ii) Detectar ameaças e ataques, baseado na técnica de detecção por anomalias localmente, pelos próprios veículos em trânsito;

(iii) Estabelecer, gerenciar e armazenar, no próprio veículo, uma lista de reputação contendo os dados dos veículos maliciosos;

(iv) Implementar o processo de detecção e classificação dos ataques e ameaças, buscando melhor eficiência com base nas limitações e restrições do software e hardware dos veículos. Aplicar algoritmos, por meio de modelos estatísticos.

(v) Alcançar mínimas taxas de falsos positivos e falsos negativos.

1.3 Organização do trabalho

Este trabalho está organizado de acordo com os seguintes capítulos:

- No Capítulo 2 é apresentada a fundamentação teórica do sistema de transporte inteligente, redes veiculares e a sua segurança, sistemas de detecção de intrusão e o método de detecção por anomalias por meio de modelos estatísticos.

- No Capítulo 3 reúne os trabalhos e estudos, correlacionados com os sistemas de detecção de intrusão e a segurança em redes veiculares e STI.

- No Capítulo 4 é apresentada uma visão geral da proposta do mecanismo de segurança, juntamente com suas funcionalidades, operações e os algoritmos de monitoramento e classificação de ataques.

- No Capítulo 5 são descritas as etapas relacionadas com os processos de simulações da mobilidade urbana e implantação da rede veicular. Também são apresentadas análises, validações do mecanismo de segurança e os resultados obtidos durante os experimentos.

- No Capítulo 6 finaliza o trabalho proposto, apresentando as dificuldades encontradas, conclusão e direcionamentos para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo descreve os princípios dos sistemas de transporte inteligente (STI) juntamente com seus dispositivos e serviços. Entre eles, estão a rede *ad hoc* veicular, padrões e protocolos de comunicação, arquiteturas e modelos de STI. As principais ameaças e ataques direcionados ao ambiente de tráfego e as principais funcionalidades dos sistemas de detecção de intrusão (SDIs) tradicionais e para redes veiculares. Técnica de detecção por anomalias e abordagens estatísticas também serão descritas.

2.1 Sistemas de Transporte Inteligente

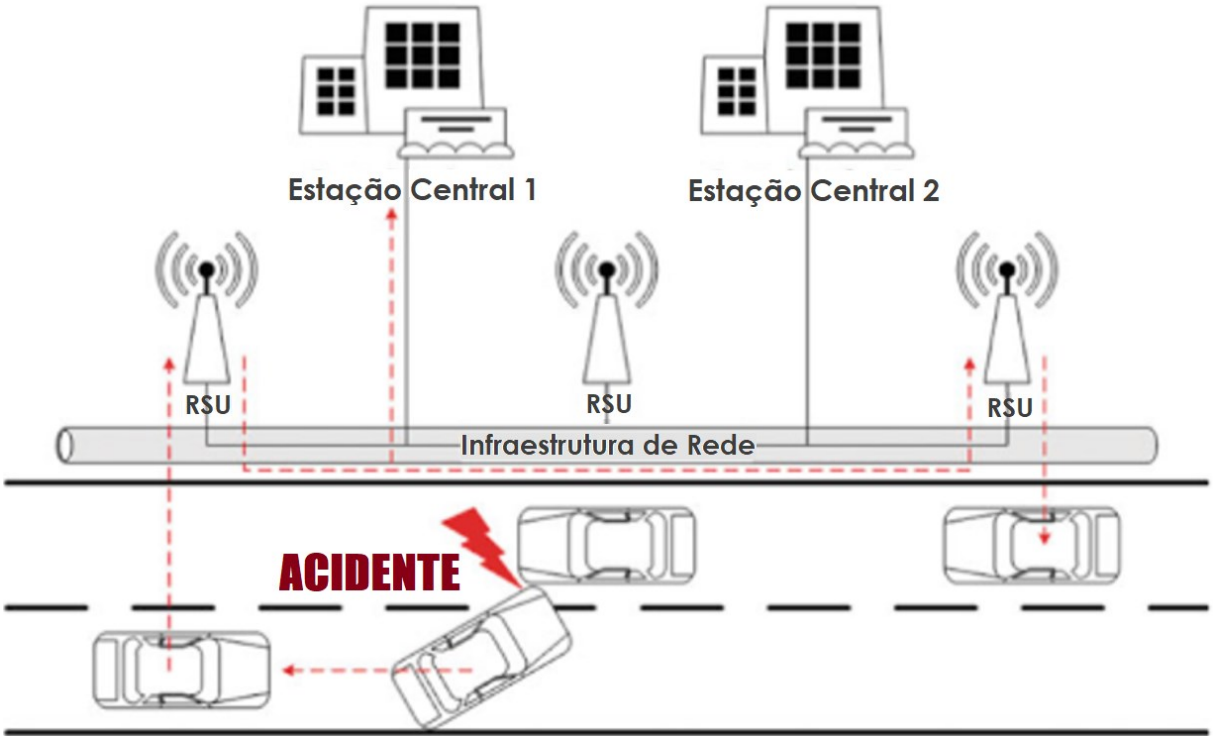
Os meios de transportes são essenciais e prioritários em uma sociedade moderna. Vivenciamos cada vez mais uma rotina diária na qual exige-se que tarefas cotidianas sejam realizadas em mínimos intervalos de tempo. Além disso, a alta densidade de veículos tem aumentado a cada ano, ocasionando sérios problemas no trânsito, transtornos sociais e a degradação do meio ambiente. São necessárias mudanças e inovações diante desse pressuposto. Adições de novas infraestruturas e a criação de regras para controles (semáforos e sinais de trânsito) não resolverão tais problemas contemporâneos. Nem sempre estas soluções são sustentáveis, pois são exigidos altos investimentos financeiros e ainda geram consequências drásticas ao meio ambiente, como por exemplo, desmatamentos, erosões etc (ALAM; FERREIRA; FONSECA, 2016).

Sendo assim, expectativas são almejadas quanto ao paradigma dos sistemas de transporte inteligente (STI), ou *Intelligent Transportation Systems* (ITS), que é constituído pela integração de tecnologias da informação e comunicação (TICs), direcionadas ao cenário de transporte. São inúmeros os serviços aplicados à proteção, segurança e conforto de pessoas (motoristas, passageiros e pedestres), bem como melhorias no gerenciamento e na eficiência do trânsito, evitando possíveis congestionamentos e a otimização da mobilidade urbana. Nesse sentido, serviços de acesso à Internet, multimídia, lazer e vagas disponíveis em sistemas de estacionamentos poderão ser acessadas pelos dispositivos pessoais. Exemplos de serviços de segurança, tais como informações das condições do trágefo, avisos de

emergências e automatização na prestação de socorro, colaboram e ajudam a evitar acidentes e minimizar os riscos de mortes.

Na Figura 1 é ilustrado um exemplo de arquitetura de STI cooperativo, que integra diversos elementos, como por exemplo, serviços de avisos de acidentes, aplicações em tempo real, a rede veicular e infraestruturas de estrada. Uma rede veicular, cujo modelo de comunicação é baseado em uma rede ponto-a-ponto (P2P - P*eer-to-Peer*), é apropriada para a troca de informações no campo de transporte. Este tipo de rede realiza conexões distribuídas, sem a necessidade de um elemento centralizador e favorece operações cooperativas entre seus nós (ALAM; FERREIRA; FONSECA, 2016; MENEGUETTE; GRANDE; LOUREIRO, 2018).

Figura 1 - Arquitetura STI com serviços cooperativos



Fonte: adaptado de Alam; Ferreira; Fonseca (2016)

O conceito dos STIs iniciou-se em meados de 1970 (AN; LEE; SHIN, 2011), originado do esforço de estudos e pesquisas entre governo, indústria automotiva e academia. A busca em estabelecer padrões e inovações, como sendo uma das grandes necessidades inerentes ao cenário de transporte, foi iniciada nos Estados Unidos em 1970. Na União Europeia, representada por Alemanha, França e Reino Unido, entre os anos de 1980 e 1985, foi implantada a Organização Européia de

Coordenação de Implementação Telemétrica de Transporte Rodoviário (EUREKA - *European Road Transport Telemetric Implementation Coordination Organization*). Em destaque ao Japão, por meio de grandes investimentos do governo, foram adquiridas experiências por volta do ano de 1990. Resultante da evolução do primeiro sistema de comunicação de informações veiculares (VICS – *Vehicle Information Communications System*), tornando-se, assim uma referência mundial. Na Coréia do Sul foi estabelecido desenvolvimentos por volta do ano de 1999.

Devido ao aumento da inclusão de novos recursos tecnológicos (computação e comunicação), o grande desafio desses sistemas é a necessidade de estabelecer padrões e implantar uma arquitetura geral. A combinação de demandas crescentes e uma variedade de requisitos, com as quais a integração de diferentes dispositivos e serviços poderão interargir entre si.

Na Tabela 1 são apresentadas arquiteturas STI pioneiras por diversos países.

Tabela 1 - Arquiteturas STIs existentes

País	Setor(es)	STI / STI-Cooperativo
EUA	Departamento de Transportes dos Estados Unidos	*Intelligent Transportation Systems Joint Program Office*[1] *Architecture Reference for Cooperative and Intelligent Transportation* (ARC-IT8.2)[2]
Europa	Organização Européia de Normalização	*European Telecommunications Standards Institute* – ETSI[3]
Japão	Organização e/ou Fundação (governo, indústria e universidades)	VICS – *Vehicle Information Communications System*[4]
Canadá	Governo, indústria e universidades	*ITS Architecture for Canada*[5]

Fonte: Autoria própria

Conforme a evolução dos STIs, são encontradas classificações, denominações e referenciais como:

[1] *United States Departament of Transportation* - https://www.its.dot.gov/index.htm
[2] *United States Departament of Transportation (ARC-IT 8.2)* - https://local.iteris.com/arc-it/
[3] ETSI (ITS) - https://www.etsi.org/technologies/automotive-intelligent-transport
[4] VICS Japão - https://www.vics.or.jp/en/
[5] ITS – STI Canadá - https://www.itscanada.ca/index.html

(i) Sistemas de Transporte Inteligente Cooperativo (*Cooperative - Intelligent Transportation Systems* – C-ITS) (ALAM; FERREIRA; FONSECA, 2016);

(ii) Referência de Arquitetura para Transporte Cooperativo e Inteligente (*Architecture Reference for Cooperative and Intelligent Transportation* - ARC-IT) (MENEGUETTE; GRANDE; LOUREIRO, 2018).

A comunicação de dados entre os elementos que compõem um sistema de transporte inteligente é realizada por uma arquitetura de rede denominada rede veicular *ad hoc*. Conhecida também como VANET (*Vehicular ad hoc Network*), cuja funcionalidade principal é a troca de informações entre veículos, infraestruturas de estradas, sensores e aplicações de pagamentos de serviços (pedágios) e entretenimento (multimídia) dentro do cenário de transporte. Além disso, possibilita o acesso às outras redes e serviços, como plataforma de nuvem, nuvem veicular (*Vehicular cloud*) e a Internet.

Além dos desafios anteriores, campos como das Cidades Inteligentes e Internet das Coisas, serão direcionados ao estabelecimento da integração entre as diferentes arquiteturas de STI e incentivados pelo intermédio de diversos países. Sistemas de transporte inteligente favorecem um campo aberto para futuras pesquisas, inovações e desenvolvimento de novos protocolos de comunicação e roteamento. Também surge a necessidade de estabelecer-se novas regulamentações, padrões e leis necessárias à proteção social e ambiental.

Outro campo importante de estudo é a preocupação com a segurança das informações transmitidas entre os dispositivos do STI. Dados de aplicações, veículos e pessoas necessitam de técnicas de segurança, como criptografia, métodos de autenticação e mecanimos para detectar e mitigar vulnerabilidades, ataques e ameaças.

2.2 Redes veiculares *ad hoc*

As redes veiculares *ad hoc*, ou VANETs (*Vehicular ad hoc Networks*) são um dos principais elementos que constituem os sistemas de transporte inteligente. Responsável pela troca de informações entre as estações do STI é um tipo de rede originária das redes móveis *ad hoc* (*Mobile ad hoc networks* – MANETs).

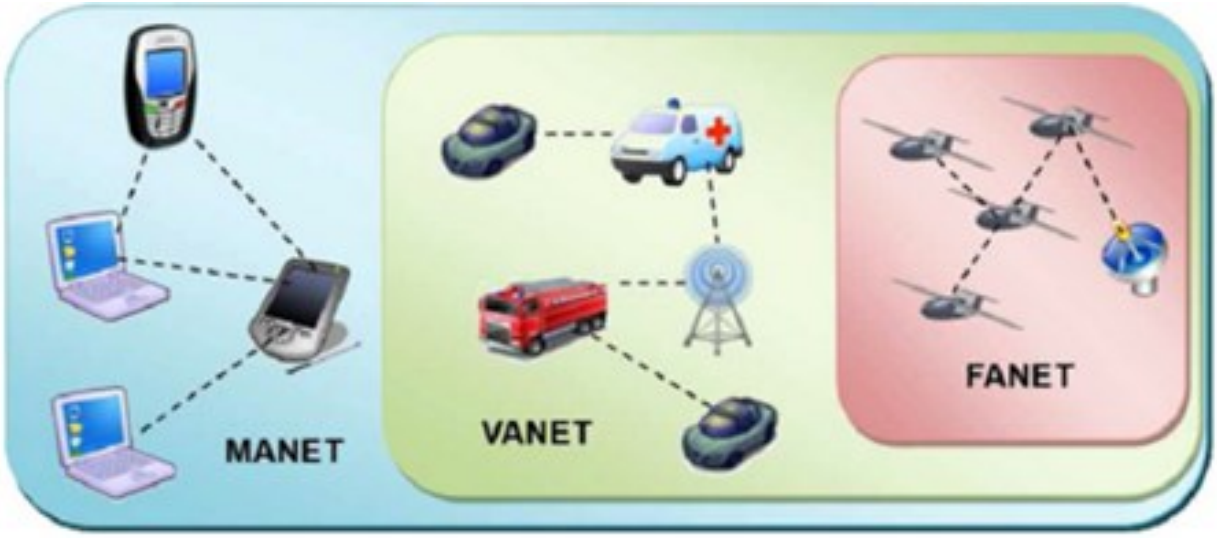
O termo *ad hoc* originado do latim, - significa “para este fim particular” (DICIONÁRIO MICHAELIS, 2020). Redes do tipo *ad hoc* geralmente funcionam como redes sem fio sem a necessidade de *layout* organizado. Considerando tipos de ambientes limitados ou topologias menores, podendo ser implementadas para veículos em comboio ou em uma pequena rede para *notebooks* e/ou *tablets* sem a utilização de fios.

Exemplificada por Branco *et al.* (2015, p.147), as redes *ad hoc* são “excelentes meios de formar uma rede temporária, não estruturada, que dispensa o uso de equipamentos adicionais além dos nós interessados”. Em uma mesma região de dados os nós se conectam, sem a necessidade de uma topologia fixa, ou seja, os nós se movem e, logo em seguida, novamente se configuram por melhores caminhos. Dentro da área de cobertura, entre os hosts, porém localizados por meio de uma distância limite, as mensagens serão encaminhadas por nós intermediários até o *host* destino. Outro fator importante em redes *ad hoc*, se o primeiro nó ou qualquer outro cair, subsequentemente, outro poderá assumir como um nó central e, assim, garantir que os serviços de comunicação não sejam interrompidos.

A abstração dos seus funcionamentos são similares a um tipo de sistema autônomo, pois são compostas por nós móveis, independentes de uma infraestrutura centralizadadora ou da existência de pontos de acesso. A troca de informações entre emissor e receptor, primordialmente, será realizada dentro da área de abrangência dos seus próprios nós (BRANCO *et al.,* 2015). Na Figura 2 é demonstrada uma variação hierarquizada da família de redes *ad hoc*, composta por: MANETs, VANETs e FLANETs. Nesta última variação, denominada como *Flying Ad Hoc Networks*, atualmente vem sendo explorada como redes aéreas *ad hoc*.

As redes veiculares permitem flexibilidades no compartilhamento de dados em ambientes altamente móveis e dinâmicos, como por exemplo, o campo de transporte automobilístico (CUNHA et al., 2016; HASROUNY et al., 2017; MENEGUETTE; GRANDE; LOUREIRO, 2018).

Figura 2 - Variação e composição da família de redes *ad hoc*



Fonte: adaptado de Branco *et al*. (2015)

Em VANETs, a comunicação é sem fio sendo favorecida por funcionalidades dedicada e de curto alcance, cuja nomeação é atribuída por DSRC[6] (*Dedicated Short-Range Communication*). Este padrão de comunicação sem fio, estabelecido por Kenney (2011), é utilizado entre os nós da VANET, favorecendo a conexão entre veículos, infraestruturas de estrada, sensores, câmeras e até mesmo outras arquiteturas de redes. Descritos por Cunha *et al.* (2016), Meneguette, Grande e Loureiro (2018), são encontradas três combinações nos modos de comunicação entre os nós da rede veicular:

(i) **Veículo para Veículo (*Vehicle-to-Vehicle* – V2V):** responsável pela comunicação direta entre veículos e não necessita de uma infraestrutura para distribuição e/ou compartilhamento das informações. Suas principais funcionalidades é prover aplicações de segurança, proteção e distribuição de mensagens de alertas (emergência, congestionamentos e rotas alternativas);

(ii) **Veículo para Infraestrutura (*Vehicle-to-Infrastructure* – V2I):** responsável pela comunicação do veículo com infraestruturas localizadas nas margens da rodovia. Suas principais funcionalidades são executar

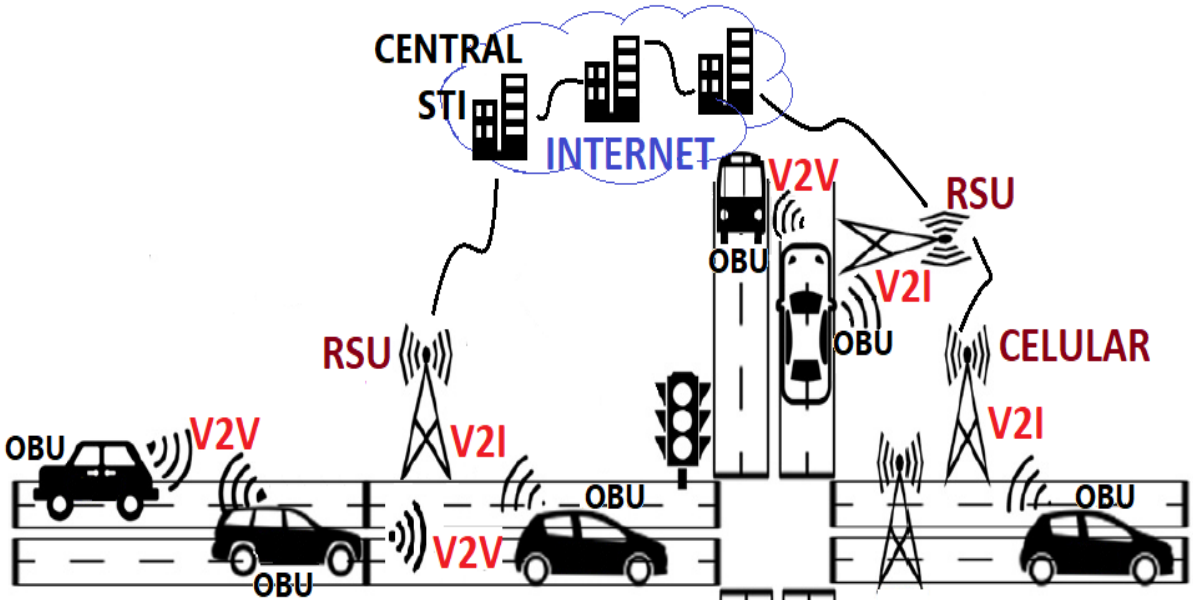
[6] DSRC (*Dedicated Short-Range Communications*) - https://ieeexplore.ieee.org/document/5888501

aplicações para coleta de informações do meio rodoviário, dados operacionais dos veículos e acesso à Internet;

(iii) **Arquitetura híbrida:** composta pela combinação entre ambos, os modos (V2V e V2I) são responsáveis pela comunicação do veículo para infraestrutura em um salto (*single-hop*) ou vários saltos (*multi-hop*), para alcançar seu destino. Suas principais funcionalidades são o compartilhamento de informações para os veículos em movimento, informações de trânsito, dados que necessitam trafegar por inúmeros nós entre abrangências distintas e prover serviços de Internet.

Na Figura 3 é ilustrado um típico ecossistema de comunicação veicular estabelecendo uma arquitetura STI. Pode-se observar, nesse cenário, que uma rede de acesso STI pode ligar seus nós da estrada a uma autoestrada interconectada com uma central STI (por exemplo, centro de gerenciamento de tráfego rodoviário ou entidades certificadoras), serviços de nuvem e a própria Internet (ALAM; FERREIRA; FONSECA, 2016; MENEGUETTE; GRANDE; LOUREIRO, 2018).

Figura 3 - Ecosistema de uma rede veicular



Fonte: adaptado de Hasrouny et al. (2017)

Os veículos são equipados com dispositivos de comunicação a bordo (OBU – *On-Board Unit*) para conexões com infraestruturas instaladas nas estradas (RSU –

Road Side Unit). As redes de acesso STI são redes dedicadas, geralmente implantadas por operadores de estradas privadas, que fornecem acesso a serviços e aplicações STI específicos, sendo interligados entre estações STI na estrada. Os veículos também se comunicam entre si através de infraestruturas interconectadas, em vez de usarem a comunicação direta pela rede *ad hoc* (ALAM; FERREIRA; FONSECA, 2016; MENEGUETTE; GRANDE; LOUREIRO, 2018).

2.2.1 Padrões e protocolos de comunicação veicular

A tecnologia de comunicação DSRC trata dos modos de comunicação inerentes ao cenário de tráfego (ALAM; FERREIRA; FONSECA, 2016; CUNHA *et al*., 2016; MENEGUETTE; GRANDE; LOUREIRO, 2018). Como as redes veiculares permitem uma comunicação direta entre veículos (V2V), veículos entre infraestruturas rodoviárias (V2I) e entre ambas (híbrida), foram definidos dois tipos de modos de operação:

(i) **modo *ad hoc***, estabelece uma rede de vários saltos distribuídos, geralmente a comunicação é realizada entre veículos (V2V);

(ii) **modo de infraestrutura**, estipulado por uma rede móvel centralizada por um salto, por exemplo, a comunicação entre um veículo e um roteador de acesso (*gateway*) à outra rede (V2I).

Os ambientes de comunicação veicular buscam a segurança e eficiência do tráfego, como a troca de informações entre as estações sobre avisos de acidentes, serviços de socorro, congestionamentos, velocidades e localização. Considerando tais fatores, as aplicações, quase sempre, serão executadas em tempo real, de modo cooperativo e distribuído.

Abstrações das funcionalidades são implementadas em níveis de camadas, sendo estas responsáveis por inúmeras operações e serviços (roteamento, criptografia, comunicação, alertas etc) e representadas por seus protocolos.

2.2.2 Camadas física e MAC

A comunicação DSRC utiliza o protocolo de comunicação sem fio padronizado pelo IEEE 802.11p (ALAM; FERREIRA; FONSECA, 2016; CUNHA *et al*., 2016; MENEGUETTE; GRANDE; LOUREIRO, 2018). Protocolo pertencente à família IEEE 802.11 (2016) para padrões Wi-Fi[7], atuando nas camadas física e de controle de acesso ao meio (MAC – *Media Access Control*). Suas funcionalidades e serviços gerenciam operações para cenários com alto dinamismo e a troca de mensagens sem a necessidade de ingressar em um Conjunto Básico de Serviço (BSS - *Basic Service Set*).

O IEEE 802.11p também define técnicas e funções de interface que são controladas pela camada MAC e adota múltiplo acesso com detecção de colisão (CSMA/CA), porém, ajusta-se aos ambientes veiculares sendo diferentes das comunicações Wi-Fi tradicionais. Portanto, este tipo de rede é limitada pelo escopo do padrão IEEE 802.11, estipulando que as camadas física e MAC funcionam dentro de um único canal lógico (ALAM; FERREIRA; FONSECA, 2016; CUNHA et al., 2016; MENEGUETTE; GRANDE; LOUREIRO, 2018).

A Comissão Federal de Comunicação dos EUA (FCC – *Federal Communications Commission*) e o Instituto Europeu de Normas de Telecomunicações (ETSI – *European Telecommunications Standards Institute*) atribuíram uma faixa de espectro de frequência dedicada para comunicações veiculares, com uma banda de 5,85 a 5,95 GHz (faixa de 5,9 GHz). Larguras de banda de 75 MHz foram reservadas para o padrão americano e 50 MHz ao padrão europeu, sendo 10 MHz para os canais de ambos padrões, favorecendo uma capacidade de comunicação sem fio para aplicações de transporte a uma distância de até 1 km (ALAM; FERREIRA; FONSECA, 2016; CUNHA et al., 2016; MENEGUETTE; GRANDE; LOUREIRO, 2018). Na Figura 4 são apresentadas as alocações dos espectros DSRC para as comunicações veiculares dos EUA (Figura 4a) e Europra (Figura 4b).

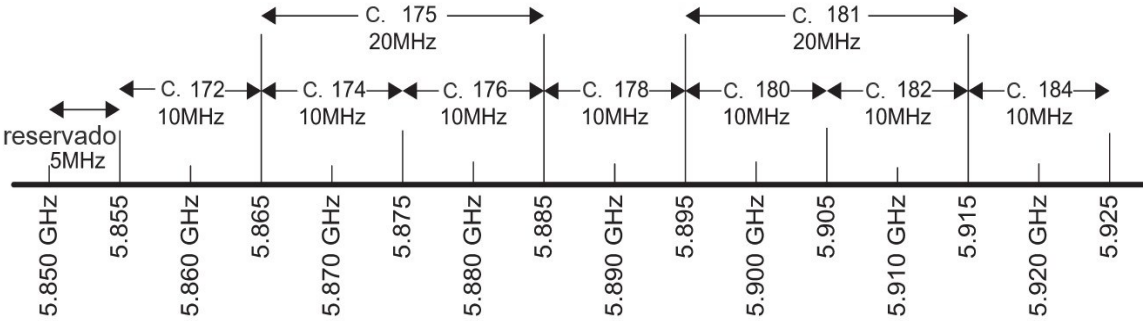
O espectro DSRC americano é estruturado em sete canais de 10 MHz (canais: 172, 174, 176, 178, 180, 182 e 184). O canal 178 é o canal de controle (CCH – *Control CHannel*), que é exclusivamente para comunicações de segurança. Apenas mensagens curtas de alta prioridade e os dados de gerenciamento são

[7] Padrão IEEE 802.11 (2016) WLAN (Física e MAC) - https://ieeexplore.ieee.org/document/7786995

transmitidas pelo canal. Os canais 172, 174, 176, 180, 182 e 184 são de serviços (SCH – *Service CHannels*), disponíveis para utilização em comunicações de serviços de segurança e conforto.

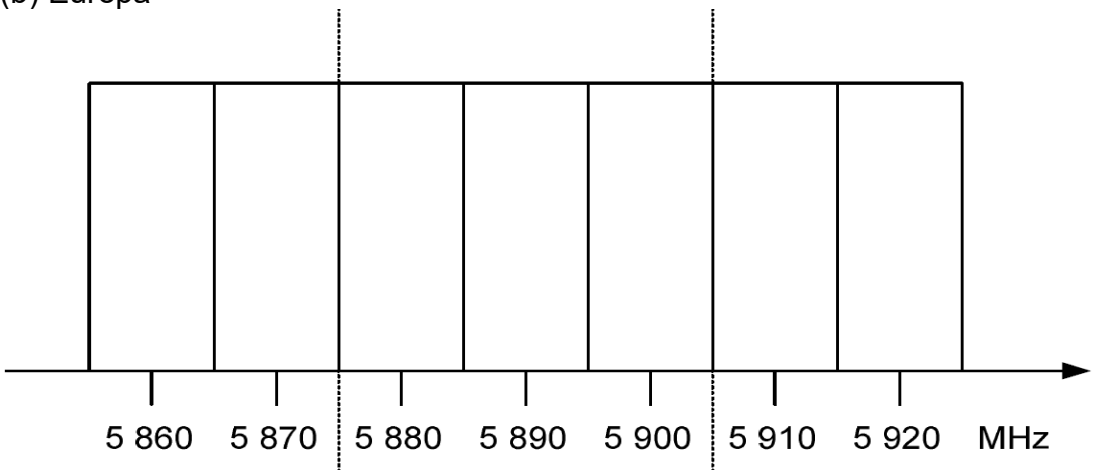
Figura 4 - Alocações de espectro DSRC para comunicações veiculares

(a) EUA



Fonte: adaptado de IEEE 1609.0 (2019)

(b) Europa



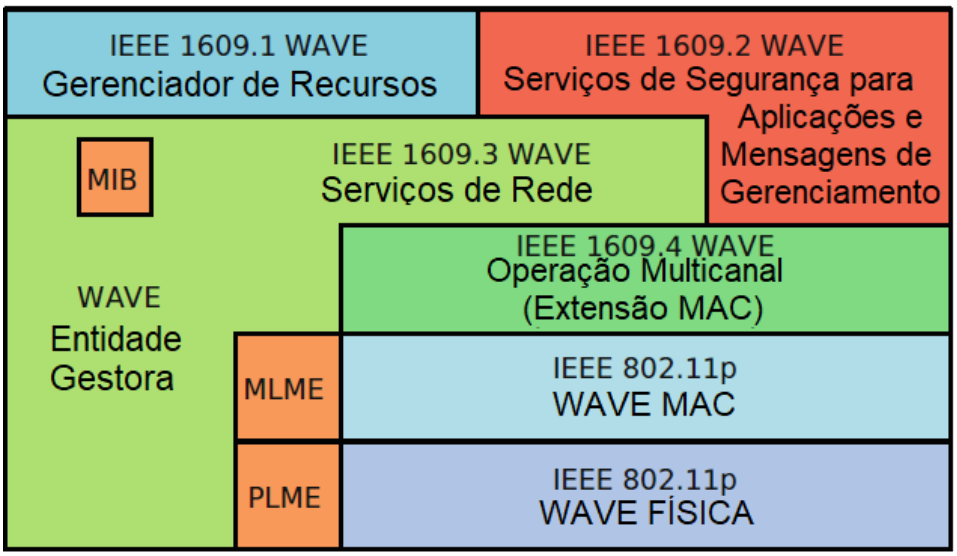
Fonte: adaptado de ETSI EN 302 571 – v2.1.1 (2017-02)

Especificamente os canais 172 e 184 são designados para aplicações de segurança envolvendo acidentes, prioridades da vida humana e prevenção de colisões em cruzamentos de rodovias (IEEE - 1609.0, 2019). Já no espectro DSRC europeu, estipulados pelos padrões ETSI EN 302 571 versão 2.1.1 (2017-02) e ETSI EN 663 versão 1.3.1 (2020-01), são definidos também sete canais diferentes, sendo dois canais de 20MHz (5.855 a 5.875 MHz) para aplicações não relacionadas à segurança, três canais de 30 MHz (5.875 a 5.905 MHz) estabelecidos para a segurança rodoviária STI e outros dois canais de 20 MHz (5.905 a 5.925 MHz) destinados para aplicações e serviços futuros para STI.

São destacadas duas conceituadas arquiteturas de STI, estruturadas em camadas de pilha de comunicação e baseadas no modelo padrão de interconexão de sistemas abertos OSI (*Open System Interconnection*). São visualizadas na Figura 5 as arquiteturas dos EUA (Figura 5a) e Europa (Figura 5b).

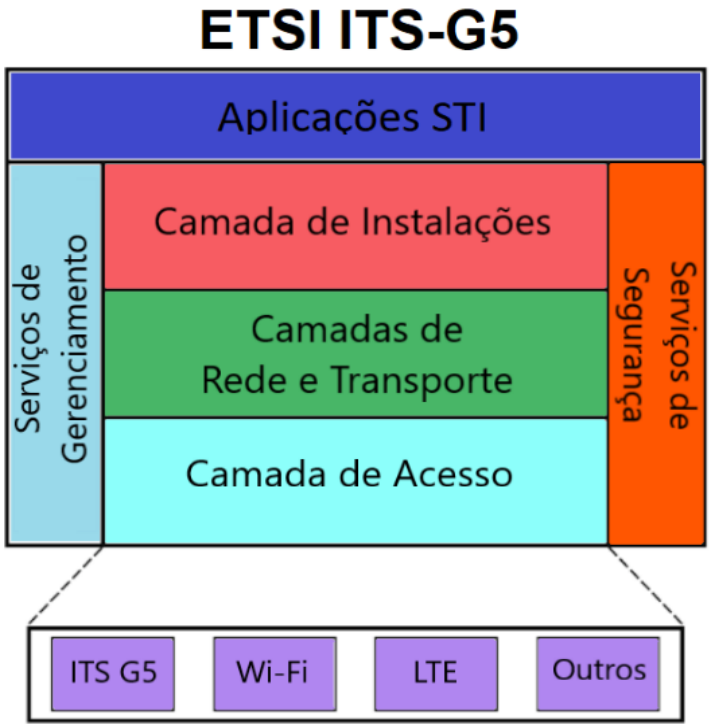
Figura 5 - Arquiteturas STI estruturadas em camadas

(a) EUA: IEEE WAVE 1609.0



Fonte: adaptado de Cunha et al. (2016) e Meneguette; Grande e Loureiro (2018)

b) Europa: ETSI ITS-G5



Fonte: adaptado de Alam; Ferreira e Fonseca (2016); ETSI EN 302 637-3 V1.3.1 (2019-02)

O padrão americano desenvolvido em 2004 pelo Instituto de Engenheiros Elétricos e Eletrônicos (IEEE), que estabelece o modelo padrão de acesso sem fio para ambientes veiculares, denominado IEEE1609.0-2019 WAVE[8] (*Wireless Access Vehicular Environments*). Já o padrão Europeu adota a arquitetura STI nomeada como ETSI ITS-G5[9].

As complexidades das camadas superiores, inerentes ao canal DSRC, são tratadas após as camadas física e MAC, implementadas pela arquitetura IEEE 1609.0 por meio dos padrões de protocolos: IEEE 1609.2, IEEE 1609.3, IEEE 1609.4, IEEE 1609.11 e IEEE 1609.12. (ALAM; FERREIRA; FONSECA, 2016; CUNHA et al., 2016; IEEE 1609.0, 2019; MENEGUETE; GRANDE; LOUREIRO, 2018). Essas camadas incluem uma camada de rede alternativa para a camada IP, recursos de segurança para aplicativos DSRC e operação multicanal de comunicação da camada IP. Suas funcionalidades são descritas a seguir:

(i) IEEE 1609.2 (2016): define formatos e processamento de mensagens seguras para aplicativos e mensagens de gerenciamento. Especifica também quando e como as mensagens de segurança devem ser processadas. A segurança é fornecida por meio da emissão e revogação de certificados de segurança, bem como da utilização de ferramentas tradicionais de segurança, como por exemplo os algoritmos que utilizam uma infraestrutura de chave pública (PKI – *Public Key Infrastructure*). Também determina um tipo específico de OBU, OBUs de segurança pública (PSOBUs – *Public Safety On-Board Units*), usadas em veículos do governo de maior prioridade (polícia e bombeiros). Vale ressaltar uma importante observação para duas alterações e correções nesta primeira versão, sendo especificadas de: (i) IEEE 1609.2a (2017), novas solicitações de setores envolvidos em melhorar o suporte para expressões compactas de intervalos de Permissões Específicas de Serviço (PES). Também revisões nas informações, para que implementadores possam obter mais confiança e correção antes mesmo de executar interoperabilidades e adição de novos manuais para apoiar

[8] IEEE 1609.0-2019 – Arquitetura WAVE: https://ieeexplore.ieee.org/document/8686445.
[9] ETSI EN 302 663 V1.3.1 (2020-01): https://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.03.01_60/en_302663v010301p.pdf

usuários e implementadores dos serviços de segurança; (ii) IEEE 1609.2b (2019), mecanismos para proteção funcional da Unidade de Dados de Protocolos individuais (do inglês, *Protocol Data Units* - PDU) do ambiente das redes veiculares, especificamente aos STIs cooperativos. No qual adicionam um campo denominado de *HeaderInfo*, para diferenciar qual o tipo de entidade funcional que receberá a PDU. Também consta uma outra importante adição para questões sobre a exportação de chave criptográfica de dados para sua posterior reutilização;

(ii) IEEE 1609.3 (2016): específica para serviços da camada de rede e de transporte, incluindo endereçamento e roteamento, definindo qual pilha a usar na camada de Controle de *Link* Lógico (LLC – *Logical Link Layer*). A camada LLC poderá escolher os seguintes protocolos: protocolo *Wave* de mensagens curtas (WSMP – WAVE *Short Message Protocol*) ou as pilhas TCP/IP ou UDP/IP. Além disso, o padrão 1609.3 define a base de informação de gestão (MIB - *Management Information Base*) para a pilha WAVE. Esse padrão é responsável pela configuração e manutenção do sistema por meio do plano de gerenciamento. Uma entidade gestora (WME - WAVE *Management Entity*), definida por este modelo, é responsável por reunir as informações das entidades de gerenciamento de outras camadas, como a entidade de gerenciamento de camada (MLME – *Layer Management Entity*) e a entidade de gerenciamento de camada física (PLME – *Physical Layer Management Entity*). O WME implementa um amplo conjunto de serviços: registro de aplicativos, gerenciamento do conjunto básico de serviço (WBSS - WAVE *Basic Service Set*), monitoramento de uso de canal e manutenção de banco de dados de gerenciamento. Além de gerenciar as camadas de rede do protocolo internet versão 6 (IPv6 – *Internet Protocol version 6*) e de transporte (TCP e UDP), o IEEE 1609.3 oferece uma alternativa ao uso dessas camadas definindo o WSMP. O motivo para usar este novo protocolo é que esse favorece uma eficiência maior no ambiente WAVE, esperando que a maioria dos aplicativos exija, entre outros requisitos, uma latência muito baixa;

(iii) IEEE 1609.4 (2016): define modificações no padrão IEEE 802.11, e especificações de funções e serviços da subcamada MAC para conectividade sem fio e operação multicanal em ambiente das redes veiculares. Para conseguir esta operação, o padrão define como a comutação entre os canais será realizada. A classificação dos pacotes indica se eles são comutados para o canal de controle ou para um dos canais de serviço. Os pacotes recebem prioridades de encaminhamento que são especificadas pelo padrão IEEE 1609.4, além de fornecer a definição de uma divisão de tempo entre canais e a sincronização de seus respectivos tempos em todos os dispositivos de rede.

(iv) IEEE 1609.11 (2010): especifica a camada e perfil des serviços e aplicações que necessitam de autenticação segura para a realização de pagamentos, identificação de dispositivos e transferências de dados por meio de aplicativos DSRC. Define um nível básico para técnicas de interoperabilidade entre equipamentos de pagamento eletrônico, por exemplo - veículos (OBU) e unidades de infraestrutura de rodovia (RSU).

(v) IEEE 1609.12 (2019): definição de identificaores para uso em séries de padrões IEEE 1609. Modelos contextuais e formais para atualizações, correções e referências do padrão WAVE.

2.2.3 Camadas de rede e transporte

A camada de rede (endereçamento do nó e roteamento de pacotes) gerencia o endereçamento lógico entre os nós por meio do endereçamento IP evitando, assim conflitos de endereços na rede. Nenhum nó poderá ter o mesmo endereço IP, ou seja, é de uso exclusivo para cada nó.

Outra funcionalidade desta camada é o gerenciamento de rotas dos pacotes trafegados entre emissor e receptor, possibilitando escolher qual será a melhor rota para que os dados sejam entregues de forma segura e eficiente. Três modelos de transmissão e recepção de informações entre os nós veiculares (CUNHA *et al*., 2016; MENEGUETE; GRANDE; LOUREIRO, 2018) são visualizados na Figura 6 e descritos abaixo:

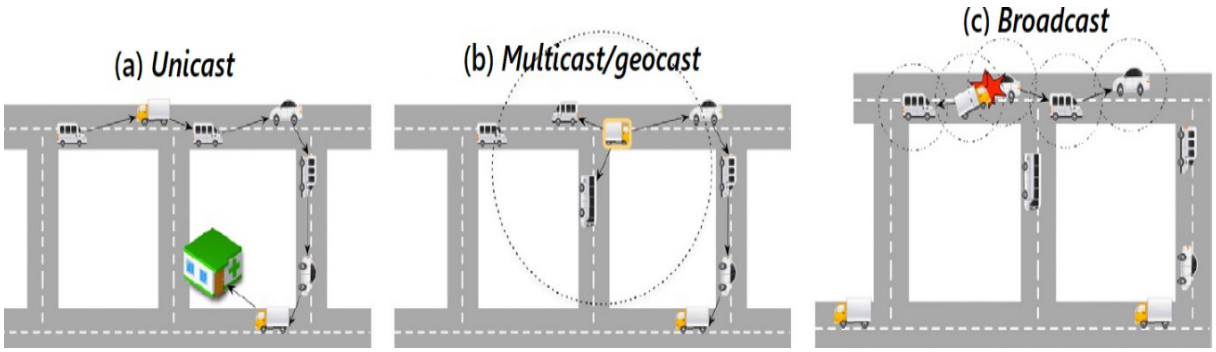
(i) ***Unicast:*** a transmissão de informações de um nó (origem) para um único nó (destino);

(ii) ***Multicast*/*geocast:*** a transmissão para todos os nós concentrados (agrupados) numa região geograficamente específica (protocolos por posição geográfica);

(iii) ***Broadcast:*** um nó origem comunica-se por difusão, de uma só vez, com todos os seus nós vizinhos. Esses, ao receberem a informação por meio de múltiplos saltos, retransmitem-na aos nós destino.

Todos os pacotes deverão ser entregues ao seu destino e, indispensavelmente às mensagens de segurança (acidentes, colisões e emergência) possuem níveis de prioridades mais altas em relação às mensagens de áudio, vídeo e entretenimento.

Figura 6 - Transmissão e recepção de informações em VANET



Fonte: adaptado de Cunha *et al*. (2016)

A camada de transporte, responsável pelos protocolos de transporte TCP e UDP e, especificamente pelo funcionamento das redes *ad hoc*, poderá encontrar duas complexidades:

(i) levar em consideração a alta velocidade automobilística dos nós ao conectarem-se em outros elementos de comunicação, porque o tempo de conectividade será de aproximadamente em milissegundos. Gerando,

assim, altas perdas de dados e implicando no baixo desempenho dos protocolos de transporte;

(ii) o protocolo TCP não poderá desempenhar seu controle de conexão confiável para a entrega das informações em um tipo de rede sem fio de alta dinamicidade e com topologias totalmente alternadas, ou seja, longa distância entre os nós. Portanto, as redes veiculares favorecem o desenvolvimento de novos protocolos de transporte ou modificações nos existentes (CUNHA *et al*., 2016; MENEGUETE; GRANDE; LOUREIRO, 2018).

Os estudos em ambientes simulados por Schmitz et al. (2006) relataram alguns testes preliminares com um protocolo de transporte veicular nomeado como VTP (*Vehicular Transport Protocol*). Sua ideia é melhorar o transporte das informações para aplicações *unicast* suprindo essas complexidades. O VTP baseia-se na estatística de características do caminho testado para controlar erros e congestionamentos e controle do congestionamento, mediada por apontamentos de informações da largura de banda, oriundas de saltos intermediários.

Em outro estudo, por Bechler, Jaap e Wolf (2005), os autores introduzem o protocolo de transporte de controle móvel, ou MCTP (*Mobile Control Transport Protocol*) tendo como base o protocolo TCP. Busca-se a otimização de acesso à Internet, para redes veiculares, por meio da combinação de sistemas de *proxys/gateways* para o aprimoramento de desempenho, dividindo a conexão TCP de ponta a ponta por arquiteturas de *proxy/gateways*.

2.2.4 Camada de aplicação

Na camada de aplicação inúmeras aplicações buscam atender dois importantes requisitos:

(i) minimizar atrasos na comunicação de ponta a ponta para os serviços de emergência, pois em alguns casos será necessário um pequeno atraso para o recebimento de informações de aplicações de entretenimento (multimídia em tempo real);

(ii) interesses futuros são esperados de aplicativos que poderão gerar negócios e *marketing*, como por exemplo, estabelecimentos comerciais, postos de combustíveis, hospedagem, lazer e turismo, transmitindo informações cujo benefício é do interesse de motoristas e passageiros. Nesse caso, mecanismos de segurança deverão garantir a confiança, privacidade e eficiência de comunicação (CUNHA *et al*., 2016).

Além das características das VANETs, Meneguette, Grande e Loureiro (2018) destacam alguns dos principais desafios: alta velocidade na mobilidade de nós e transferência de dados, fragmentação frequente de rede e a rápida mudança de topologia. Os recursos das VANETs constituem uma barreira significativa para o desenvolvimento e a implementação de aplicativos para essas redes, especialmente quando suas aplicações exigem consistência, escalabilidade no espaço-tempo e segurança dos dados trafegados.

2.2.5 Requisitos e desafios de segurança em redes veiculares

As redes veiculares fornecem vários fatores que exigem certas atenções em relação à segurança da informação. Tanto pelas características da sua arquitetura, como também das transações, informações e a privacidade de seus usuários são fatores passíveis de proteção e segurança (HASROUNY *et al*., 2017; SAKIZ; SEN, 2017). Algumas preocupações presentes e futuras necessitam de atenções que possam garantir a integridade, confidencialidade e disponibilidade das informações da rede veicular. Portanto, alguns pontos devem ser tratados e estudados:

(a) Privacidade *versus* segurança do usuário: informações dos usuários podem ser solicitadas por autoridade em casos de ocorrências, incidentes ou até mesmo para análises de fins estatísticos. Deverão prevalecer procedimentos que assegurem a privacidade do usuário, conformidades e que órgãos autorizados poderão acessá-las (HASROUNY et al., 2017; SAKIZ; SEN, 2017);

(b) Aumento do número de veículos: os veículos são os principais nós de comunicação neste tipo de rede. Evidentemente, o número de veículo

cresce a cada ano. Em todo o globo terrestre estima-se aproximadamente 1,282 bilhão de veículos em uso, segundo a OICA (2015). Considerando o Brasil, através dos números do SINDIPEÇAS (2020) em comparação ao ano de 2018, houve um aumento de 2,5% na frota de veículos em 2019, chegando a 45,9 milhões de veículos entre automóveis, caminhões e ônibus. Consequentemente o número de nós em uma VANET aumentará bruscamente, estimando que até 2023 haverá cerca de 75,4 milhões de carros conectados por meio de sistemas embarcados entre aplicações de navegação e entretenimento (STATISTA, 2020b);

(c) Criação de padrões mundiais: necessidades de governanças integradas e no envolvimento da elaboração de padrões únicos e reconhecidos globalmente (HASROUNY et al., 2017; SAKIZ; SEN, 2017);

(d) Alta mobilidade e desconexões da rede: o tempo de conectividade entre os veículos são extremamente curtos, diante de uma topologia de rede mais previsível. Dependendo do cenário (urbano ou rodoviário) situações de reencontros, entre veículos, poderão ou não surgir. Mediante a este fator, devem ser estabelecidas técnicas e processos para o gerenciamento de complexidades relacionadas a sistemas baseados em reputação (HASROUNY et al., 2017; SAKIZ; SEN, 2017);

(e) Respostas em tempo real (disponibilidade): Hasrouny et al. (2017) e Sakiz e Sen (2017) ressaltam a criticidade exigidas por aplicações de avisos de segurança rodoviária (emergências, acidentes e outros), nas quais realizam execuções em tempo real. Além de prover a proteção do transporte, é necessário que essas aplicações sejam desenvolvidas com segurança própria, ou seja, mecanismos que possam proteger suas operações, como exemplo, contramedidas a um ataque de negação de serviço (DoS – *Denial of Service*);

(f) Integridade na disseminação de mensagens: por se tratar de um ambiente totalmente cooperativo, ou seja, haja vista o alto índice de disseminação de mensagens entre os veículos, mensagens falsificadas podem ser

transmitidas nesse meio. Não se trata somente da segurança de RSUs, a complexidade maior é para com os veículos que abordam a prevenção de ameaças, mas também àqueles que são responsáveis por elaborar o ataque (HASROUNY et al., 2017; SAKIZ; SEN, 2017);

(g) Gerenciamento de congestionamento, detecção de colisões e monitoramento de atividades: sabe-se que as mensagens de avisos de segurança possuem altas prioridades. Assim sendo, é de extrema importância evitar que ataques de negação de serviço distribuídos sobrecarregam RSUs e/ou nós aos arredores, gerando grandes congestionamentos e colisões na rede. A troca intensa de dados entre a alta mobilidade dos nós dificulta o monitoramento das atividades e ações. Sistemas de detecção de intrusão (SDI) desempenham funcionalidades importantes para proteção de redes computacionais tradicionais, porém a sua implantação em VANETs torna-se complexa e desafiadora, devido às características deste modelo de rede (HASROUNY et al., 2017; SAKIZ; SEN, 2017; SHARMA; KAUL, 2018; LOUKAS et al., 2019);

(h) Mecanismos de não-repúdio: suscetíveis ataques de não-repúdio, sendo que o atacante negará que enviou tal mensagem. Mecanismos que garantem que a mensagem realmente foi transmitida por um determinado nó e impedindo que este se omita do seu ato malicioso (HASROUNY et al., 2017; SAKIZ; SEN, 2017);

(i) Abrangência e topologia da rede: altamente dinâmica, ilimitada geograficamente e com rápido crescimento. Estabelecendo-se em um cenário totalmente móvel, cria-se a necessidade de desenvolver novos protocolos de encaminhamento de mensagens, procurando a melhor rota em tempo hábil para unicast, multicast em V2V e V2I. Outro fator que pode prejudicar a comunicação são as características do meio ambiente como surgimento de barreiras naturais, (como exemplo, vegetação, prédios e posições geográficas) podem impedir a transmissão e abrangência do sinal sem fio (HASROUNY et al., 2017);

(j) Mecanismos de autenticação e verificação de dados: controle de respostas e autorizações somente entre veículos autenticados. Estabelecer esse tipo de processo ajuda a restringir e amenizar usuários mal-intencionados, identificar origem das mensagens e verificar se os dados não sofreram modificações, ou seja, se estão íntegros e válidos (HASROUNY et al., 2017; SAKIZ; SEN, 2017);

(k) Distribuição de chaves certificadoras: como descrito acima as VANETs possuem grande distribuição geográfica e não possuem um elemento centralizador. Então, surge uma complexidade desafiadora sobre (quem e quais) autoridades responsáveis poderão emitir, distribuir, gerenciar e revogar certificados e chaves públicas e privadas (HASROUNY et al., 2017; SAKIZ; SEN, 2017);

(l) Gerenciamento e tempo de durabilidade de senha: autenticações em canais que implementam segurança, exigem senhas de tempo duradouro. Porém, ao tratarmos da volatilidade e dinamismo do ambiente de tráfego, cuja comunicação entre os nós é estabelecida de maneira rápida num pequeno período de tempo, torna-se complexo e quase impossível a implementação de senhas com períodos de tempo duradouros (HASROUNY et al., 2017).

2.2.6 Ameaças e ataques

Ao desenvolver mecanismos de segurança se faz necessário conhecer quais são as possibilidades de ataques, consequências, vulnerabilidades e superfícies envolvidas. Sendo assim, são consideradas as peculiaridades funcionais e operacionais da VANET e os dispositivos interconectados pelas aplicações STI. Estes fatores favorecem diversas superfícies de ataques, vulnerabilidades e ameaças.

Hasrouny et al. (2017) categorizaram quatro grupos principais de ataques:

(i) riscos inerentes à interface sem fio;

(ii) ameaças ao hardware e softwares tanto dos veículos como das infraestruturas;

(iii) ataques em OBUs (sensores e dispositivos eletrônicos no interior do veículo);

(iv) problemas oriundos do mau gerenciamento do acesso sem fio e dos dados trafegados na rede.

Sakiz e Sen (2017) apontam para dois grupos de superfícies e/ou geradores de ameaças e ataques, tendo como base a localização do alvo pelos atacantes:

(a) ataques entre veículos: envolvem as informações trocadas entre veículos e do próprio ambiente do percurso. Informações como avisos de emergência, acidentes, condições da estrada e congestionamentos são altamente prioritárias para a eficiência do transporte e necessitam de integridade e disponibilidade. A falsificação dessas informações críticas poderá gerar grandes transtornos e graves consequências entre os veículos;

(b) ataques intra-veículo: cuja comunicação é realizada entre os dispositivos instalados no interior do próprio veículo (OBUs), como por exemplo, sensores de distância, temperatura, velocidade e aceleração, detecção de obstáculos e incêndio. Enganar esses sensores de forma intencional e maliciosa interfere no próprio veículo e no ambiente do percurso, como por exemplo um ataque direcionado a um veículo, conectado pelos dispositivos emergentes da IoT e integrado pelas TICs. Com o aumento da conectividade dos veículos, distintos tipos de ataques poderão ocorrer, e principalmente ataques remotos. Por exemplo, a disseminação de *malwares* infectando e comprometendo o veículo e, assim, possibilitando que ele venha a ser acessado e controlado remotamente pelo atacante (MILLER; VALASEK, 2015; GREENBERG, 2015).

Alguns tipos de ataques, juntamente com suas explorações maliciosas, métodos e conseqüências são descritos abaixo:

(a) Ilusão: influencia por engano o comportamento de outros condutores, manipulando a entrada ou saída dos sensores dos veículos por meio de informações falsas, e assim criando cenários ou situações não reais inerentes ao tráfego. Por exemplo, mensagens de um falso acidente fazendo com que os veículos, dentro da abrangência do atacante, reduzam a velocidade (SAKIZ; SEN, 2017);

(b) *Sybil*: cria várias identidades falsas de veículos, simulando múltiplos nós na rede, ou seja, falsificação de identidades. Por exemplo, simulações de veículos com identidades falsas (nós *Sybil*) apresentando-se em diversas posições geográficas, subversão de reputação, clonagem de identidades e mensagens ilusórias (HASROUNY et al., 2017; SAKIZ; SEN, 2017; SHARMA; KAUL, 2018; LOUKAS et al., 2019);

(c) *Blackhole:* também conhecido como o ataque do buraco negro. Ganha esse nome porque sua ação maliciosa é capturar (“roubar”) o pacote do nó origem para si próprio. O veículo malicioso adquire autoridade em manipular os pacotes dos seus veículos vizinhos e, ao mesmo tempo, esses recebem do atacante direcionamentos para rotas falsificadas por meio de violação da rota de dados e mensagens inválidas. Geralmente são exploradas falhas nos protocolos de roteamento localizado na camada de rede, causando a perda dos dados que complementam o roteamento do pacote (HASROUNY et al., 2017; SAKIZ; SEN, 2017; SHARMA; KAUL, 2018; LOUKAS et al., 2019);

(d) *Wormhole:* em comparação ao ataque *blackhole,* nele será constituído por dois ou mais nós maliciosos. Através de um túnel privado, criado entre suas extremidades, é realizado o desvio da rota dos pacotes originados pelos nós vítimas, também conhecido como ataque “buraco de minhoca”. Como exemplo de abstração, uma rede privada maliciosa sendo controlada por dois nós atacantes, separados geograficamente, mas ao

alcance de seus rádios. Aprisionando os veículos vítimas, capturando o tráfego da rede, modificando-o e, assim, retransmitindo-o pela extremidade de origem (maliciosa) para a extremidade destino (maliciosa). Consequências podem ocorrer também nos modos de transmissão (*multicast* e *broadcast*), que serão interrompidos, ficando restritos pela conexão privada e sem o encaminhando dos pacotes. Quando estabelecido o túnel oculto, as informações nele trafegadas, ficarão restritas e disponíveis somente entre as suas extremidades, ou seja, pelos nós maliciosos (HASROUNY et al., 2017; SAKIZ; SEN, 2017; SHARMA; KAUL, 2018; LOUKAS et al., 2019);

(e) *Man-in-the-Middle:* conhecido também como o ataque do “Homem do Meio” em que o atacante toma posse do canal de comunicação (MORENO, 2016, p. 178). De forma oculta, o atacante estará no meio da conexão, entretransmissor e receptor, capturando os dados trafegados neste canal. Sua abstração poderá ser realizada por um atacante estando em seu veículo, situado entre a comunicação V2V ou V2I, e coletando informações dos veículos em trânsito. Esse ataque executa a técnica denominada *sniffing*, que o atacante interceptará a conexão e disponibilizará a outros nós vítimas simulando um ponto de acesso falso, por exemplo (HASROUNY et al., 2017; SAKIZ; SEN, 2017; SHARMA; KAUL, 2018; LOUKAS et al., 2019);

(f) *Replay:* neste tipo de ataque os endereços IP e MAC podem ser clonados e falsificados. O atacante de posse desses dois tipos de endereços poderá reproduzir ou retransmitir informações válidas, porém já enviadas anteriormente. Ações maliciosas como a manipulação das tabelas de roteamento e localizações dos nós atingidos, poderão criar falsas ilusões de eventos ocorridos anteriormente. Por exemplo, congestionamentos e acidentes, causando confusões aos veículos que trafegam naquele dado momento (HASROUNY et al., 2017; SAKIZ; SEN, 2017; LOUKAS et al., 2019);

(g) GPS *spoofing*: o funcionamento do GPS é realizado via satélites de comunicação, em que são efetuados cálculos das rotas (coordenadas geográficas) em questão da localização do veículo. Tal tecnologia já se faz presente nos novos veículos e, também, pode ser utilizada por meio de *smartphones* ou adquiri-los como um dispositivo eletrônico separado. Porém, esse sistema não está livre de sofrer ataques maliciosos, o qual é chamado de *GPS spoofing*, ou seja, falsificação/simulação de posição. O atacante, por meio de um simulador de GPS, poderá subverter as coordenadas de localização do veículo. O simulador estando próximo dos alvos ultrapassará o sinal íntegro do satélite, fazendo com que o receptor do GPS do veículo passe a visualizar as falsas coordenadas pelo sinal malicioso. Os condutores passarão acreditar que estarão em outros locais diferentes e seguirão para rotas inadequadas. Esse ataque pode estender-se para os ataques do túnel (*tunnel attack*) e veículo oculto (*hidden vehicle*) (HASROUNY et al., 2017; SAKIZ; SEN, 2017; SHARMA; KAUL, 2018; LOUKAS et al., 2019);

(h) Ataque do túnel e veículo oculto: no ataque do túnel o atacante poderá utilizar de áreas suscetíveis de interferências no sinal real do GPS, como por exemplo – entradas ou saídas de túneis e/ou garagens/estacionamentos subterrâneos, ou até mesmo criando uma área de interferência simulando a ausência do sinal íntegro do GPS (HASROUNY et al., 2017; SAKIZ; SEN, 2017; SHARMA; KAUL, 2018). Já o ataque do veículo oculto (HASROUNY et al., 2017; SHARMA; KAUL, 2018) consiste em um veículo atacante manipular a posição real de um veículo acidentado convencendo-o de que a posição manipulada é a correta. Ao mesmo tempo interferindo em seu sinal de aviso e impossibilitando-o de transmitir o seu acidente. Os veículos próximos não receberão os avisos e poderão causar graves acidentes;

(i) *Malware:* ocorre no cenário interno ou externo da rede VANET, quando usuários mal-intencionados do próprio sistema (*insider*) ou usuários externos (próximos das vias de transportes e/ou infraestruturas de comunicação) infiltram programas maliciosos (*worms* e *malwares*) no

momento em que a OBU e/ou RSU estão recebendo seus dados (HASROUNY et al., 2017; SHARMA; KAUL, 2018; STALLINGS; BROWN, 2014, cap. 6);

(j) Ataques de escuta e análise de tráfego: são considerados tipos de ataques envolvendo a confidencialidade e privacidade dos usuários da rede veicular (HASROUNY et al., 2017; SAKIZ; SEN, 2017; ARSHAD et al., 2018). Permite ao atacante, por meio de mecanismos de espionagem, escuta e análise dos dados trafegados, obter informações sensíveis dos condutores e veículos. É utilizado para diversos fins, como roubo de IDs, invasão da rede, dados de localização para rastreio dos veículos e gerar novos ataques. Sua ocorrência é passiva, não gerando impactos à rede e sem o consenso dos usuários (SAKIZ; SEN, 2017).

2.2.7 Ataque de negação de serviço no ambiente veicular

Com o aumento exponencial do número de dispositivos conectados no âmbito urbano, e com a chegada dos modernos veículos com dispositivos de comunicação sem fio, evidenciam-se o surgimento de novas vulnerabilidades e ameaças a estes dispositivos interconectados (FERRAZ & FERRAZ, 2014, OWASP API Security Project, 2019). Diante deste pressuposto, originam-se diversas possibilidades e superfícies para que o ataque de negação de serviço seja explorado e direcionado, tanto ao hardware e software destas inúmeras tecnologias. Este tipo de ataque é um dos ataques mais conhecidos e frequentes nos diversos modelos de redes e principalmente na Internet (MORENO, 2016).

Conhecido também, do inglês, como *Denial of Service* (DoS), é uma técnica que consiste em mandar uma sobrecarga muito alta de informações para determinado servidor/serviço, gerando, desse modo, indisponibilidades nas funcionalidades e serviços de uma ou várias redes alvo e acarretando uma série de problemas graves a vítma. Outra vertente de exploração é forçar a vítma a executar operações que possam consumir recursos da rede, largura de banda ou responder a inúmeras requisições de protocolos de forma intensiva e desequilibrada, forçadas pelo atacante (BRANCO et al., 2015; STALLINGS; BROWN, 2014, cap. 7).

Somente no Brasil, durante o ano de 2019, o ataque de negação de serviço foi o segundo mais reportado ao Centro de Estudos, Resposta e Treinamento de Incidentes de Segurança no Brasil (CERT.br). Adquiriu um percentual de 34,42% em relação aos outros tipos de ataques, conforme estatísticas realizadas pelo CERT.br (2019). Existem diversas vertentes de execução do DoS e duas destas são destacadas:

(i) Inundação e tempestade de pacotes (do inglês, *Flooding* e *Packet Storm*): ação maliciosa do atacante em enviar grandes quantidades de dados a uma ou mais vítimas, assim excedendo o limite de informações da sua capacidade de processamento (BRANCO et al., 2015);

(ii) Negação de serviço distribuída ou *Distributed Denial of Service* (DDoS): com o passar dos anos o ataque de negação de serviço adquiriu inovações, podendo ser executado e controlado por meio de diversos atacantes. Inúmeros *hosts* são “sequestrados”, tornando-se maliciosos, manipulados remotamente pelo atacante direcionam inúmeros ataques DoS a uma rede alvo ou vítma (BRANCO et al., 2015; STALLINGS; BROWN, 2014, cap. 7).

Quando considerado no ambiente das VANETs, o ataque de negação de serviço poderá causar inúmeras e grandes consequências, como por exemplo, a indisponibilidade da comunicação sem fio entre veículos (V2V e OBUs) e com RSUs (V2I ou híbrido). Outro impacto previsto é a degradação do atraso permitido durante os avisos de acidentes ou emergências, ocorridos ao longo da estrada. Esses dados poderão receber um *delay* muito alto e não chegarão ao seu destino e não receberão o prévio aviso (HASROUNY *et al*., 2017; SAKIZ; SEN, 2017. Suas execuções podem ser feitas por nós maliciosos internos ou atacantes externos, como no caso de inundar o canal de uma RSU e tornando-a fora de operação, exemplo de DDoS. Assim, inúmeros atacantes poderão executar um ataque em massa convergindo numa sobrecarga excessiva dos veículos vítmas (SHARMA; KAUL, 2018; LOUKAS *et al*., 2019).

Descritas por Moreno (2016, 2018), são encontradas diversas ferramentas que possam explorar com facilidade a superfície de uma rede sem fio e executar

diversas ações maliciososas do DoS/DDoS. Vale ressaltar que algumas configurações e políticas de segurança, aplicadas ao meio sem fio, divergem-se das utilizadas em uma rede tradicional cabeada. Entre estas distinções, são elencadas as limitações da abrangência de comunicação, largura de banda, manejos na potência do sinal de transmissão, como interferências e perdas de propagação. Dois exemplos de ataques de negação serviço para redes *wireless*, podem ser vistos a seguir, por meio da falsificação e manipulação de quadros MAC e do protocolo ARP:

(i) *Deauth* ou Desassociação: processo pelo qual o atacante envia pacotes falsos fingindo ser um AP (*Access Point,* ou Ponto de Acesso), forçando as estações vítmas desconectar-se da rede (MORENO, 2016, 2018);

(ii) Envenenamento de *cache* ARP: também conhecido por ARP *cache poisonning*, estação maliciosa convence os *hosts* alvos que ele é o novo *gateway* da rede, e assim fazendo com que as vítimas encaminhem seus pacotes ao falso *gateway* para que possam ser interceptados (SANDERS, 2017; SEITZ, 2015);

Ataques DoS quando direcionados a serviços essenciais como prestação de socorro, aplicações em tempo real, avisos de congestionamentos e acidentes, em um cenário de transporte, podem ocasionar riscos de vida e até mortes.

2.2.8 Perfil dos atacantes

Analisar e conhecer comportamentos maliciosos dos atacantes, possibilita o desenvolvimento de novas contramedidas (como exemplo, políticas de segurança, mecanismos de reputações, criptografia etc), e possivelmente mitigar determinadas ameaças descritas nas subseções 2.2.6 e 2.2.7. São descritos abaixo alguns perfis de atacantes encontrados na literatura (HASROUNY et al., 2017):

(a) Motorista egoísta: neste perfil, o atacante poderá realizar um redirecionamento do tráfego;

(b) Bisbilhoteiros: tentativa de coletar dados dos dispositivos;

(c) Condutores gananciosos: motoristas com o perfil de ataque em benefício próprio, como induções de mensagens falsas sobre acidentes ou liberação da via;

(d) Atacante mal-intencionado: este atacante é mais direcionado em seus alvos, causando danos por meio de aplicações da rede. São mais racionais e perigosos, podem ocultar e/ou atrasar a transmissão de informações prioritárias;

(e) Infiltrantes industriais: são os próprios funcionários dos fabricantes ou mecânicos da indústria automobilística (infiltrados) que realizam alterações no software ou firmware do hardware (V2V ou V2I), adulterando atualizações e abrindo possibilidades para invasões ou coleta de informações;

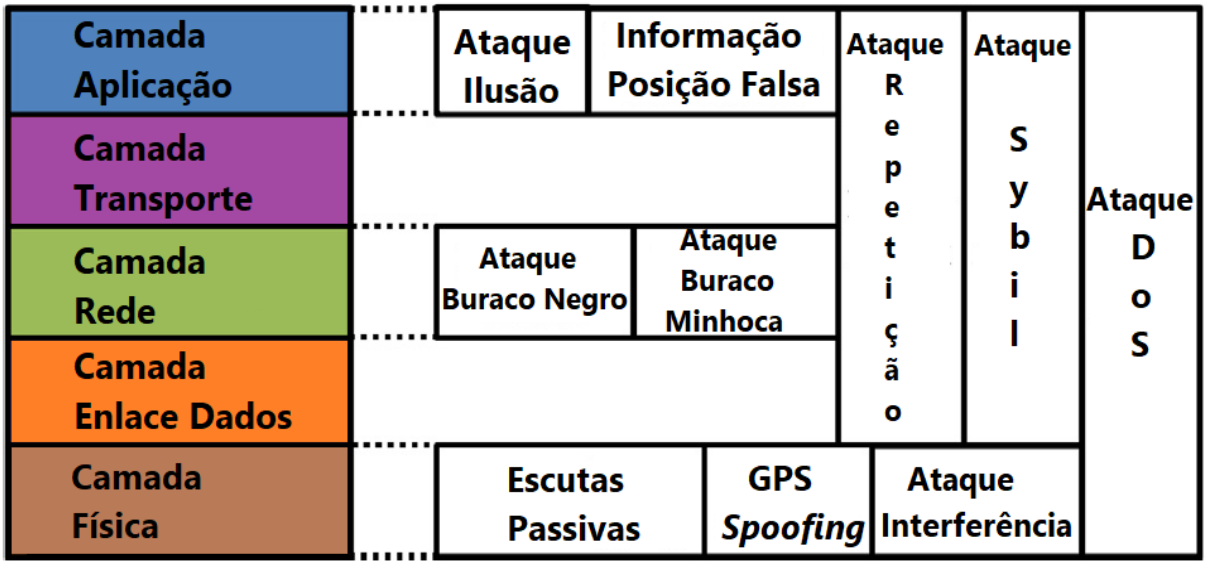
(f) Infiltrados (*insiders*): este atacante pertence à rede, estando conectado através de uma chave pública autenticada. Assim, terá acesso a todos os dados inerentes à rede, possibilitando disseminar inúmeras maliciosidades;

(g) Brincalhões: incentivados por motivos de prazer e diversões prejudicam os veículos ou equipamentos da rodovia utilizando DoS, sobrecarga da rede ou disseminando mensagens adulteradas sobre emergência ou acidentes de alguma região geográfica específica, cujo transtorno culminará no congestionamento daquele local;

(h) Estranhos: este atacante não necessariamente está autenticado na rede, porém pode capturar dados dos veículos e de seus usuários conforme transita pela localidade do atacante. Podem também efetivar ataques do tipo DoS congestionando a rede com falsas informações e, até mesmo, interromper o seu funcionamento, porém possuem limitações de acesso à rede limitando o leque de ataques.

Na Figura 7 é apresentada a sumarização dos principais tipos de ataques, exibindo a relação entre os principais ataques com a pilha de camadas TCP/IP.

Figura 7 - Ataques relacionados com as camadas da arquitetura TCP/IP



Fonte: adaptado de Sakiz e Sen (2017)

2.3 Sistemas de detecção de intrusão

Os sistemas de detecção de intrusão (SDI), ou *Intrusion Detection Systems* (IDS) podem operar como um hardware, software ou integração de ambos. Sua funcionalidade é monitorar atividades das redes ou sistemas computacionais, buscando por operações não autorizadas ou subversões das políticas de segurança da informação (SANTOS; BARCELOS, 2016; STALLINGS; CASE, 2016).

Pilli *et al*. (2017) definem um SDI como uma ferramenta de segurança defensiva que captura e monitora o tráfego de rede, logs do sistema e verifica o sistema e/ou a rede pela busca de atividades suspeitas. Ao encontrar uma atividade considerada maliciosa emitirá avisos e alertas (alarmes) ao administrador do sistema.

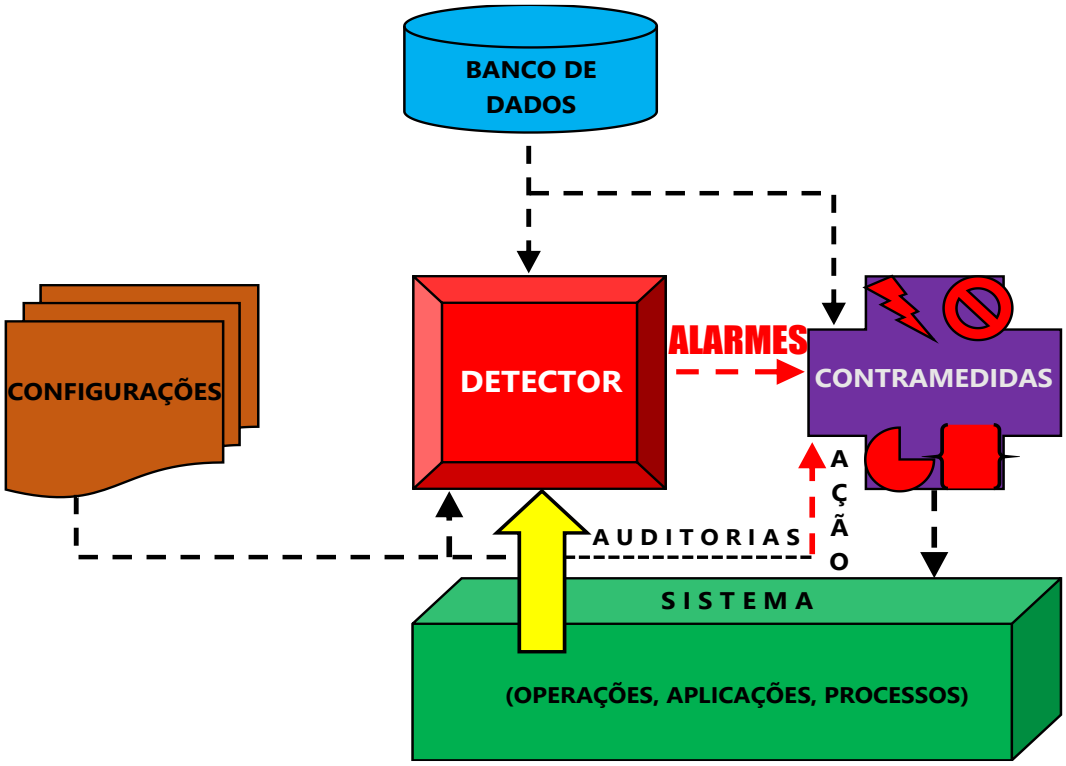
Stallings e Case (2016) conceituam um SDI elencando duas importantes definições do glossário de segurança da internet, descritos na RFC 4949 versão 2 (IETF, 2007):

(i) **Intrusão de segurança:** um ou vários eventos de segurança constituem um incidente de segurança, que o intruso obteve (ou tentou obter) acesso a um sistema (ou recurso) sem a autorização;

(ii) **Detecção de Intruso:** serviço de segurança para **monitorar** e **analisar eventos** originados no sistema, cuja finalidade é encontrar e emitir avisos em tempo real (ou possivelmente) de tentativas de acessos aos recursos do sistema sem a autorização devida.

Um SDI pode ser constituído por diversos componentes lógicos e conceituais, sendo apresentados na Figura 8.

Figura 8 - Componentes e ações de um SDI tradicional



Fonte: adaptado de Dewanjee e Vyas (2017)

Estes componentes são responsáveis por diversas funcionalidades e ações inerentes às configurações, locais de implantação, operacionalidades, métodos de detecções de ataques e o armazenamento destes.

Na Tabela 2, são descritos estes componentes devidamente com suas ações, operações, processos e sequências do fluxo de dados.

Tabela 2 - Componentes lógicos e conceituais de um SDI

Componentes	Descrição
DETECTORES OU SENSORES	- responsáveis pela coleta e monitoramento dos dados gerados; - a entrada do sensor poderá ser qualquer parte do sistema contendo operações de evidência intrusa; - tipos de entrada: pacotes de rede, arquivos de log e vestígios de chamada de sistema.
CONTRAMEDIDAS E ALARMES	- recebem entrada de um ou mais sensores ou por outros analisadores; - responsável por determinar se a intrusão ocorreu; - sua saída cria uma indicação que ocorreu a intrusão; - tipos de saída: evidências são as bases de conclusão que a intrusão ocorreu; - fornece orientações de quais ações poderão ser tomadas inerentes ao efeito da invasão.
BASE DE DADOS	- armazena eventos, resultados processados e assinaturas de padrões reconhecidos como anormais.
CONFIGURAÇÕES	- permite ao administrador visualizar a saída do sistema ou controlar o comportamento do sistema; - ações: finalizar um processo, reiniciar conexões e emitir notificações; - em alguns sistemas essa interface poderá ser um gerente, diretor ou componente de console.

Fonte: adaptado de Santos e Barcelos (2016) e Stallings e Case (2016)

O local de implantação do SDI é um dos requisitos importantes para sua atuação. Como descrito anteriormente, esse tipo de mecanismo de segurança poderá atuar como software, hardware ou pela integração de ambos. Sendo assim, um SDI poderá ser implantando com base em dois locais diferentes (STALLINGS; CASE, 2016):

(i) **Baseados em rede:** estrategicamente posicionados na rede de computadores (podendo ser segmentos específicos ou dispositivos da rede) para que possam monitorar e analisar todo o tráfego, protocolos e aplicativos de rede, seguindo os padrões estabelecidos pelas assinaturas conhecidas e os comportamentos suspeitos. Podem ser nomeados por NIDS (*Network Intrusion Detection System*);

(ii) **Baseados em host (*host-based*):** monitora as características e os eventos que ocorrem em máquinas individuais, ou seja, no host em si. Nomeado também como HIDS (*Host-based Intrusion Detection System*), estando conectado a uma rede, seus pacotes de entrada e saída, e comportamentos são monitorados e analisados, emitindo avisos de alertas ou executando contramedidas reativas em casos de atividades suspeitas ou maliciosas.

Outro requisito crucial é para com a técnica que será utilizada para detectar ataques e ameaças (eventos identificados como maliciosos). Duas destas técnicas são descritas:

(i) **Anomalias (comportamental):** monitora o tráfego da rede ou operações do sistema, comparando-as com o comportamento normal esperado. Utiliza como base a banda “normal” de operação, protocolos de comunicação, endereços IP e portas de conexões, processos do sistema operacional (SO), chamadas de sistemas e outros. O desvio do comportamento normal é considerado um ataque, emitindo avisos e alertas. Nesse caso, considera-se amplamente a dependência de atividades que regem a rede ou o SO em si. Esse método, em alguns SDIs, pode ser denominado de estatístico. Assim, análises de resultados estatísticos, baseados nas operações e atividades de um sistema, ajudam a estabelecer limites normais e anômalos. Porém, podem ser geradas altas taxas de falso-positivos se o sistema for parametrizado incorretamente e o tempo de detecção é maior;

(ii) **Assinaturas (padrões de ataques):** nesta metodologia o monitoramento do tráfego de rede ou das operações do sistema é comparado com assinaturas ou atributos de ataques já conhecidos (padrões). Esses padrões são armazenados em um banco de dados de assinaturas de ataques conhecidos pelo próprio SDI. Porém, um dos seus maiores problemas é a existência de uma lacuna temporal, ou seja, depende do tempo da atualização do banco de dados com novas ameaças (descobertas) e da geração de novas assinaturas. Nesse sentido,

complexidade em gerir essa lacuna poderá fazer com que o sistema não reconheça uma ameaça verdadeira e a ignore, porém, o tempo para detecção é alto.

O SDI poderá operar somente com um desses métodos ou ser configurado pela combinação de ambos, assim denominando um **SDI híbrido** (SANTOS; BARCELOS, 2016; STALLINGS; CASE, 2016; DEWANJEE; VYAS, 2017).

2.4 Detecção de intrusão em redes veiculares

Após um levantamento e uma revisão da literatura atual, são descritos nesta seção os princípios de sistemas de detecção de intrusão para redes veiculares e sistemas de transporte inteligente. Metodologias de detecção, locais de implantação, classificação do sistema, meios de simulações e validações, complexidades e desafios também serão abordados.

Foram localizadas diversas propostas de SDIs para veículos, porém, com abordagens específicas ao protocolo baseado em mensagens da rede CAN (*Controller Area Network*). A rede de área do controlador é utilizada internamente pelos veículos, para a comunicação da Unidade de Controle Eletrônico (ECU – *Electronic Control Unit*) com módulos e dispositivos eletrônicos locais. Por exemplo, os dados coletados pelo sensor de temperatura são transmitidos para a ECU, sendo que esta tomará decisões e ações necessárias. Trabalhos focados na segurança da rede CAN de veículos, como a análise do quadro de mensagens do barramento CAN *bus*, foram propostos por Lee, Jeong e Kim (2017). Em outro estudo, os pesquisadores Kim, Han e Kwak (2018) utilizaram o método de análise de sobrevivência para detecções de anomalias no tempo de durabilidade específicas do campo ID no quadro de mensagens da rede CAN. Nesse tipo de pesquisa, a possibilidade de cenários mais próximos do real se torna mais efetiva. Esses dois trabalhos os autores utilizaram pequenos dispositivos computacionais (Arduino e Raspberry) e veículos reais, para a injeção de dados, execução dos ataques, coleta e validação dos resultados

Os trabalhos, anteriormente mencionados, buscam a proteção e segurança inerentes à rede de comunicação interna do veículo, que também carecem de contribuições, estudos e futuras soluções. São vários os desafios e as

complexidades, ao se estabelecer sistemas e medidas de segurança, em um modelo de rede que traz características distintas das redes tradicionais de computadores. Como descrito, os nós operam em um ambiente totalmente móvel, sua topologia é altamente dinâmica, os intervalos de conexões são curtos e, na maioria das vezes, a comunicação é sem fio.

Outra questão desafiadora é o processo de testes e do desenvolvimento de protótipos, pela pouca existência de cenários semelhantes ou compatíveis com cenários reais de tráfego e transporte.

Mediante a revisão da literatura, foi diagnosticado que, na maioria dos estudos propostos, esses foram desenvolvidos, implementados e validados em softwares simuladores (SAKIZ; SEN, 2017; LOUKAS *et al*., 2019). Os sistemas simuladores englobam simulações de redes de computadores, do tráfego veicular e da mobilidade em cenários rodoviários e urbanos.

Ao utilizar simuladores, principalmente para implementações de sistemas de segurança, é necessário a presença de conjuntos de dados (*datasets*) para efetuar testes de desempenho e para validações dos resultados gerados. A maioria dos *datasets* existentes, compostos por processos e operações maliciosas, são privados de ataques, ameaças e vulnerabilidades atuais e vigentes.

O KDD-99[10] é o conjunto de dados comumente mais utilizado para este tipo de pesquisa (SHARMA; KAUL, 2018). Porém, seu conteúdo trata de dados mais antigos (KDD CUP, 1999). Alguns trabalhos, como de Aloqaily, Otoum e Ridhawi et al. (2019), utilizaram uma versão mais aprimorada e melhorada do KDD-99, denominada de NSL-KDD[11].

Várias técnicas de detecção semelhantes com as descritas na seção 2.3, juntamente com suas vantagens e desvantagens, são abordadas pela Tabela 3.

Podem ser empregadas diversas metodologias específicas, compostas por recursos e pelas características do cenário de tráfego. Dependendo das necessidades e especificidades estas metodologias podem ser integradas, sendo classificadas como híbrida.

---

[10] KDD Cup 1999: conjunto de dados (“maliciosos” ou “normais”) utilizado para o desenvolvimento, implementações, testes e validações de sistemas de detecção de intrusão. Disponível em: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. Acesso em: 20 fev. 2019.

[11] NSL-KDD: conjunto de dados. Disponível em: https://www.unb.ca/cic/datasets/nsl.html. Acesso em: 20 fev. 2019.

Tabela 3 - Técnicas de detecção propostas para redes veiculares e STI

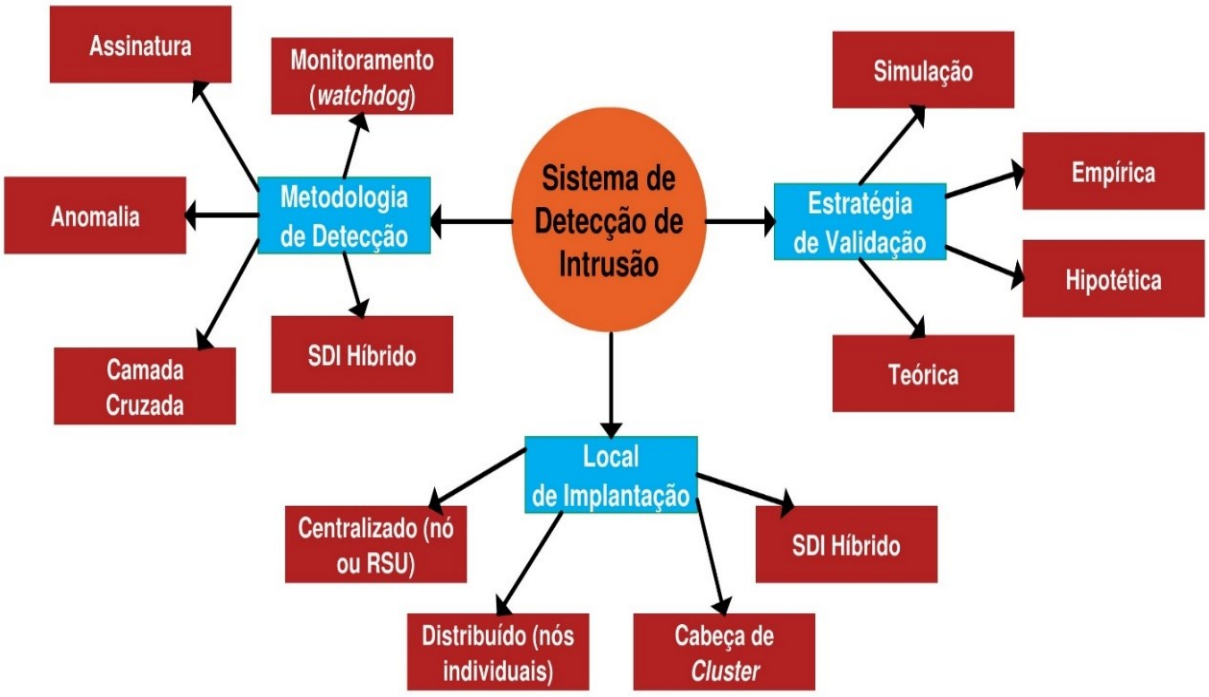
Técnica	Descrição	Vantagens	Desvantagens
Assinaturas	Conhecida por uso incorreto ou baseado em regras. Utiliza o processo de reconhecimento da identificação (assinatura), cujo padrão é gerado pela combinação do nó e do seu ataque, comparando-a com as assinaturas armazenadas num banco de dados.	Rápida detecção, tempo de detecção mínimo e baixo processamento computacional.	Dependente da constante atualização do banco de dados de assinaturas em virtude de novos padrões de ataques, não reconhece ataques de dia-zero (*zero-day*) e pequenas alterações efetuadas em padrões existentes.
Monitoramento (*watchdog*)	Baseada na vigilância das atividades maliciosas executadas pelos nós vizinhos. Opera em modo promíscuo ouvindo todo o tráfego daquela rede, como exemplo o encaminhamento de pacotes.	Reconhece nós egoístas e gananciosos (não retransmitem os pacotes aos nós vizinhos guardando-os para si).	Somente para ataques egoístas e gananciosos, exige alto processamento, implica no fator privacidade pois depende do monitoramento do tráfego e poderá causar congestionamento da rede.
Anomalias	Baseia-se na análise do comportamento das atividades do sistema buscando situações ou eventos anormais (inúmeras tentativas de logins, modificações de parâmetros etc). Eventos desviados de comportamentos normais serão considerados maliciosos e um alerta é gerado.	Reconhecimento de ataques de dia zero e desconhecidos, baixo custo computacional e o SDI poderá aprender e treinar reconhecimentos.	Alta taxa de falso positivo (poderá classificar um evento normal como anormal), altos atrasos na detecção e complexidades nas fases de treinamento e aprendizagem.
Camadas cruzadas (*cross-layer*)	Detectar operações maliciosas distintas ocorridas em diferentes camadas da rede veicular. Reunindo os resultados de detecção e logs de eventos das diferentes camadas o mecanismo de segurança formará uma decisão.	Aumento da taxa de detecção, baixa taxa de falso-positivo e detecção de vários tipos de ataques e ameaças por diferentes superfícies.	Consome mais energia, gera sobrecarga na rede, e conforme o aumento dos nós e a alta mobilidade da rede afeta o desempenho e eficiência.
Híbrida	Combinação das técnicas de assinatura e anomalias. Favorece um SDI com maior amplitude entre diversos tipos de ataques.	Reconhecer diferentes tipos de ataques (sem assinaturas e anômolos), baixas	Exige alto processamento computacional e poderá criar atrasos na detecção.

Técnica	Descrição	Vantagens	Desvantagens
	Manipulação, treinamento e aprendizagem nos padrões dos ataques existentes e reconhecidos são realizados através da técnica de anomalias, refletindo num aprimoramento do sistema.	taxas de falsos-positivos e de erros.	
Honeypots **(Potes de mel)**	Características de um mecanismo pró-ativo, ou seja, através de um pacote "isca" poderá identificar o nó considerado egoísta (malicioso) pois este não retransmitirá, aos nós origem e vizinhos, abandonando o pacote "isca" recebido.	Capaz detectar ataques de dia-zero e conhecidos, melhora a taxa de entrega de pacotese oferece amplitude para outros ataques.	Se for implantado de forma incorreta poderá ocasionar atrasos na rede e baixa taxas de detecção.

Fonte: adaptado de Sharma e Kaul (2018)

Na Figura 9 foram relacionados os diversos componentes que constituem um SDI para VANETs e STI. Métodos de validações também são demonstrados, processo este utilizado pelos pesquisadores como medida de aferir o desempenho do sistema proposto.

Figura 9 - Principais componentes de um SDI para VANETs e STI



Fonte:adaptado de Sharma e Kaul (2018)

Como base inicial, são utilizados três parâmetros: (a) metodologias de detecção; (b) locais de implantação e (c) estratégias de validação.

A correlação entre os parâmetros de metodologias de detecção e locais de implantação, permite criar diferentes abstrações relacionadas com determinadas classificações de SDIs.

A escolha correta do local de implantação do SDI possui grande importância, pois poderá implicar, vantajosamente, nas taxas de detecção, transmissão de pacotes e o desempenho da rede. Três locais de implantação são destinados para o posicionamento do SDI em uma rede veicular e caracterizados por diferentes classificações (SHARMA; KAUL, 2018; LOUKAS *et al*., 2019). Na Figura 10 são exibidos estes locais e classificações, conforme descritos abaixo:

(i) Descentralizado e distribuído: instalado em nós individuais;

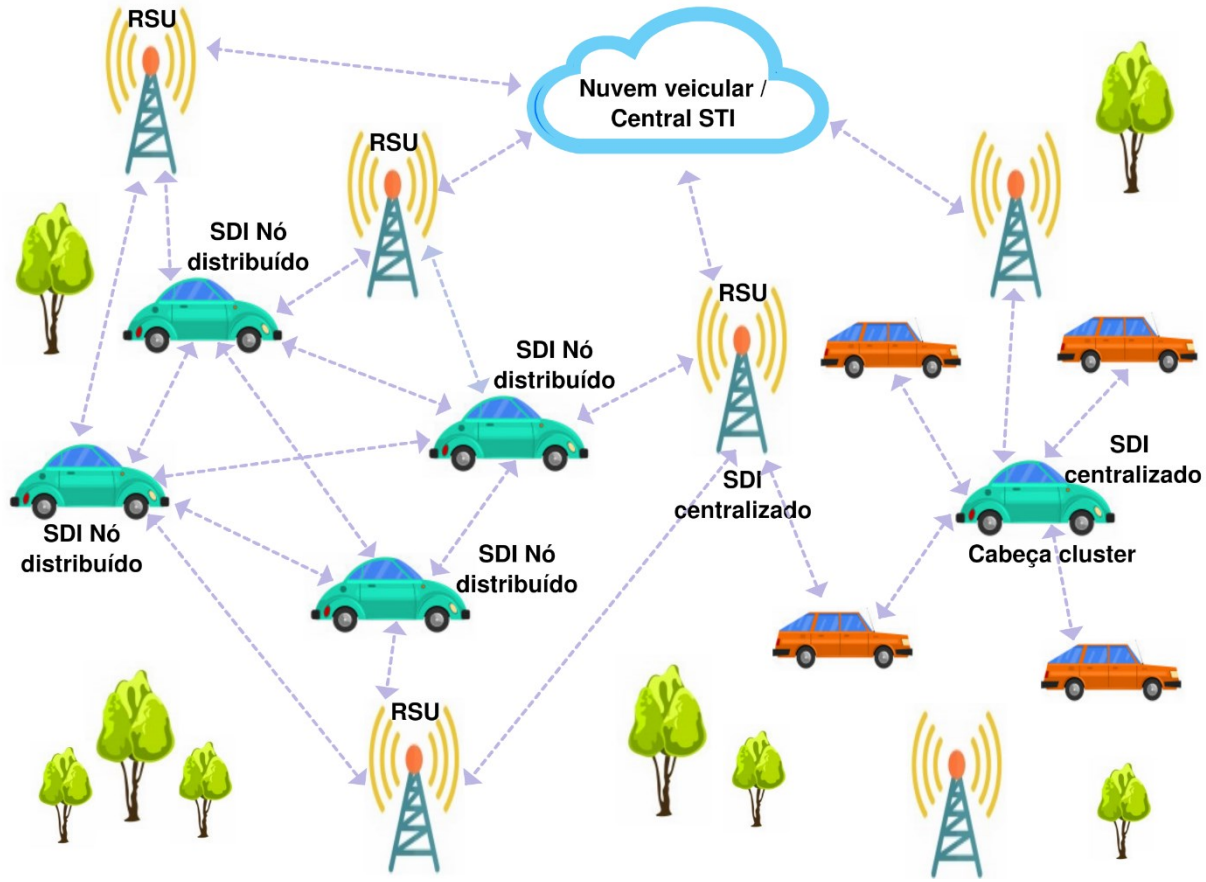
(ii) Centralizado: instalado em RSUs, cabeças de *clusters* (CHs) ou em plataformas de nuvem/nuvem veicular;

(iii) SDI híbrido: implantado em todos os nós da rede (veículos, cabeça de *cluster*, RSU e plataforma de nuvem/nuvem veicular).

O desenvolvimento de um SDI para veículos e ambiente de transporte necessita de antemão considerar diversos requisitos prioritários. Inicialmente, como base, os padrões, recursos (hardware e software) e protocolos que constituem o STI. Consequentemente, elenca-se as características operacionais, funcionais e a comunicação da rede veicular. Como disponibilizado pelas Figuras 9 e 10, verifica-se uma abstração dos elementos, composição, métodos e ações do funcionamento dos possíveis SDIs.

O fluxo de informações é o caminho percorrido pelos dados trafegados no mecanismo de segurança, sendo este tratado por diversas ações como: coleta dos dados (entrada), processo de classificação (normal, anormal, padrão de assinaturas) e ação a ser executada (saída), como alertas, bloqueios do invasor ou até mesmo a transferência/armazenamento dos dados a um local remoto para análises mais detalhadas.

Figura 10 - Locais e classificações de implantação do SDI veicular



Fonte: adaptado de Sharma e Kaul (2018) e Loukas *et al.* (2019)

Loukas *et al.* 2019, atenta-se às limitações do local que o SDI será instalado, ou seja, veículos e os dispositivos de infraestruturas. Dependendo dos dispositivos envolvidos poderão trazer certas restrições, por exemplo: limitações dos recursos computacionais como o baixo poder de processamento, mínimo espaço para armazenamento de dados, dispositivos dependentes de baterias, restrições da rede de comunicação sem fio etc.

A inclusão de serviços baseados em nuvem e/ou nuvem veicular (SHARMA; KAUL, 2018) poderão integrar tarefas de transferência, armazenamento e gerenciamento dos dados coletados pelo SDI. Aplicação de métodos de classificação de dados, descoberta de novos modelos de ameaças, implementação da lista de padrões de assinaturas de ataques, são alguns dos serviços operados por uma *VANET cloud*. Os serviços podem ser realizados por processos distribuídos, possibilitando uma série de medidas colaborativas e ações cooperativas, por diversas aplicações e sistemas, em benefício ao transporte. O emergente conceito

da computação em nuvem veicular (*Vehicular cloud computing*) conduz para novas possibilidades de serviços, como - serviços para recursos móveis, operações autônomas, flexibilidade de recursos, arquitetura de rede P2P (*Peer-to-Peer*) ou cliente-servidor, veículos como plataformas de serviços de armazenamento remoto ou local e entre outros (HE; YAN; XU, 2014; BOUKERCHE; GRANDE, 2018).

2.4.1 Técnica de detecção por anomalias e abordagem estatística

Nesta subseção serão discutidas operações e processos envolvidos pela técnica de detecção por anomalias por meio de abordagem estatística.

Quando um evento é considerado anômolo por um mecanismo de segurança, por exemplo um SDI, este emitirá alertas, logs e avisos ao administrador do sistema. Sabe-se que inúmeras situações podem ser identificadas e classificadas como anomalias, entre elas: falhas no sistema, mal formação de pacotes, conexões com hosts desconhecidos ou imensas quantidades de dados sendo transferidas por pequenos intervalos de tempo. Ao detectar uma anomalia torna-se evidente que sua ação será maliciosa, podendo ter gerado ou ainda estar gerando inúmeros eventos que são denominados de incidentes (SANDERS; SMITH, 2014).

O ponto crucial ou do instante momento em que um SDI identifica e gera um alarme em decorrência de um evento ou comportamento anormal, é denominado de técnica de detecção. Na Tabela 3, seção anterior, foram resumidas algumas destas técnicas de detecção para VANETs.

Um SDI para ser efetivo em seu monitoramento de segurança, são necessários inúmeros levantamentos, análises de processos, monitoramentos e coleta de dados gerados pelo respectivo sistema ou rede a ser protegida. Com posse destes dados o Centro de Operações de Segurança (COS), ou SOC (*Security Operations Center*), por meio de análises e aplicação de modelos estatísticos, poderá identificar padrões e comportamentos que serão estabelecidos como normais ou anormais (SANDERS; SMITH, 2014).

Antes de selecionar e aplicar um modelo estatístico aos dados coletados, é necessário realizar uma análise destas informações guiada por meio de determinados parâmetros, ou seja, indicadores. Vale ressaltar que este procedimento analítico é independente da plataforma de segurança em uso. Algumas literaturas ou aplicações de segurança descrevem estes indicadores como

- **Indicadores de Compromisso e Assinaturas**. Outras literaturas definem-o simplesmente de **Indicadores de Compromisso (IC)**, ou *Indicators of Compromise* (IOC), explica Sanders & Smith (2014). Para facilitar o uso de IC eles são classificados de acordo com o ambiente em que são executados: (i) **indicadores de rede**, e (ii) **indicadores de *host***, como exemplo:

(a) **IC de Rede:** endereçamento IPv4 e IPv6, *hash* do certificado, nome do domínio, *string* de texto, protocolo de comunicação etc;

(b) **IC de *host*:** chave de registro, nome de arquivo, processos, conta de usuário, *string* de texto etc;

Além destas duas classificações iniciais, alguns indicadores podem estar em ambos locais de execução. Sendo assim, são utilizadas duas subclassificações:

(i) **estáticas:** são utilizadas com base em valores conhecidos previamente. Para este indicador são definidas três variações (**atômica**, **computada** e **comportamental**). Exemplos: **atômico,** indicam valores menores e específicos, e não podem ser divididos (IP, nomes de *host*, endereço de email); **computado,** originado por dados de incidentes (cálculos de *hash*, expressões regulares e resultados estatísticos) e **comportamentais**, combinação dos indicadores atômicos e computados por meio de uma análise e processamento lógico (um endereço de e-mail recebe um anexo, fazendo o download de um arquivo executável, no qual este realiza conexões com um determinado servidor remoto e inicia uma transferência de dados suspeita, gerando grandes quantidades de tráfego de saída.

(ii) **variáveis:** quando valores não são conhecidos, por exemplo, a combinação de análises comportamentais (sequência de eventos que podem gerar um ataque) e a busca em encontrar valores em variáveis (quantide de pacotes gerados, por exemplo). Este indicador geralmente baseia-se no modelo conceitual do ataque, ou seja, tentando “descobrir” possivelmente uma ocorrência anormal.

Uma analogia aos ICs é considerá-los o combustível principal do COS, fazendo-o trabalhar constantemente pela busca de novas anomalias, por meio da coleta, análise e monitoramento destes. Este processo mantem o mecanismo de segurança atualizado e em plena evolução (SANDERS; SMITH, 2014).

Caberá ao COS coletar, organizar e interpretar os dados gerados pelos ICs transformando-os em novos resultados. Contudo, deverá ser estudado e entendido qual será o modelo estatístico mais apropriado para ser aplicado a estes novos valores, assim detectando-se novos padrões de normalidade ou anormalidade dos dados analisados. Em princípio, alguns exemplos podem ajudar na escolha do modelo estatístico mais apropriado:

(i) identificar quais são os *hosts* que mais geram tráfego na rede;

(ii) quais os servidores remotos que trocam dados diariamente com a rede interna;

(iii) domínios de e-mails mais recebidos e/ou enviados pela organização;

(iv) processos do servidor que mais consomem processador e memória em certos períodos do dia;

(v) quantidade de dados trafegados durante os finais de semana e em períodos com menos atividades de trabalho.

Entretando, estes exemplos são uma pequena amostra dentre inúmeros outros que deverão ser coletados, organizados e parametrizados e posteriormente serem analisados por meio de abordagens estatísticas.

Os estudos analisados por Kumar & Dutta (2016) e Muruti, Rahim e Ibrahim (2018), relatam diversas contribuições e propostas que abordam a técnica de detecção de anomalias por meio de modelos estatísticos. Sendo estes um dos primeiros modelos aplicados a detecção de intrusão. Geralmente são utilizadas as medidas de média, desvio-padrão, distribuição dos dados e probabilidades para criar modelos referenciais e padrões de comportarmentos. Este tipo de técnica de

detecção, quando aplicada a um sistema ou rede, avalia ocorrências de determinados eventos e os comparam com o modelo referencial padrão. Havendo algum desvio do modelo criado, o evento será considerado uma anomalia ou intrusão. Um dos benefícios de utilizar técnicas estatísticas é a descoberta de novas ameças e vulnerabilidades, pois não requerem conhecimento antecipado de comportamentos ou características de possíveis problemas na segurança do sistema monitorado (KUMAR; DUTTA, 2016).

Dentre os modelos existentes, Muruti, Rahim e Ibrahim (2018), elencam:

(a) Técnicas paramétricas: os dados utilizam distribuição normal e são criados como parâmetros e pontuações para detectar instâncias de anomalias. São utilizados modelos de regressão, Gaussiano, estimastivas de máxima verossimilhança, testes do qui-quadrado ou pela combinação destes modelos. São aplicados em análise de tráfego de redes, sistemas e máquinas virtuais em nuvens, entre outros;

(b) Técnicas não-paramétricas: não assume nenhum modelo dedutivo e são usadas instâncias de dados normais para criarem um modelo referencial. Desvios deste modelo, serão considerados anômolos. São utilizados histogramas, modelagem baseada em *Kernel* para calcular similaridade e instância dos dados. São aplicados para grandes conjuntos de dados com altas dimensões e em sistemas de grande escala;

Outras abordagens estatísticas, para a segurança em MANETS, avaliam: monitoramento de protocolos de roteamento, comunicação sem fio, agregação em *clusters*, camada MAC, análise da energia de baterias, entre outros. Kumar & Dutta (2016) relataram os seguintes modelos estatísticos:

(a) Teoria dos Jogos com equilíbrio de Nash;

(b) Abordagem com redes bayesianas por meio de relações probabilísticas;

(c) Detecção de valores extremos (*outliers*);

(d) Análises de componentes principais por meio de compactação de dados de altas dimensões, exemplo: tráfego de rede;
(e) Abordagens baseadas em detecção de valores extremos (*outliers*) por meio das técnicas de *clustering* (agrupamentos), similaridade predeterminada ou medidas por distâncias;

2.4.2 Análise de valores extremos ou detecção de *outliers*

Valores considerados extremos ou também conhecidos por *outliers*, são definidos por Aggarwal (2017, p. 1, tradução nossa)[12] como - "[...] um ponto de dados significativamente diferente dos dados restantes". Também podem ser visualizados como anormalidades, discordantes ou desvios encontrados em amostras de dados estatísticos.

Outro aspecto importante, considerado por Aggarwal (2017, p. 1), é:

> [..] que na maioria dos aplicativos, os dados são criados por um ou mais processos geradores, que podem refletir a atividade no sistema ou observações coletadas sobre entidades. Quando o processo de geração se comporta de maneira incomum, resulta na criação de discrepâncias. Portanto, um *outlier* geralmente contém informações úteis sobre características anormais dos sistemas e entidades que afetam o processo de geração de dados. O reconhecimento de tais características incomuns fornece informações úteis específicas da aplicação (AGGARWAL, 2017, p. 1).

Enfatizando a técnica para encontrar valores discrepantes, Kumar & Dutta (2016), descrevem três categorias que podem ser utilizadas como base neste tipo de modelo:

(i) estatística: supõe que os objetos normais acompanham um determinado padrão de geração de normalidade, quando identifica valores extremos os classificam como desvios deste padrão de normalidade;

(ii) distância: entende-se que os *outliers* estão em uma certa distância de seus vizinhos;

[12] *An outlier is a data point that is significantly different from the remaining data.*

(iii) densidade: calcula a densidade ao redor de um valor extremo e a compara com a densidade de seus vizinhos, considerando a grande diferença entre ambas.

O uso da análise e identificação da presença de *outliers*, pode ser aplicados por sistemas de detecção de intrusão, sistemas de antivírus, análises de sensores, mineração de sentimentos em mídias sociais e aplicações Web. Outras áreas de estudos, como ciências da terra, engenharia, saúde e financeiro adotam a verificação e análise de valores extremos (AGGARWAL, 2017, p. 399-416).

2.4.3 Desvio Absoluto da Mediana (DAM)

Um dos modelos estatísticos aplicado na identificação de valores discrepantes é nomeado de **Desvio Absoluto da Mediana (DAM)**. Redescoberto e divulgado por Hampel (1974 *apud* LEYS *et al.*, 2013, p. 2), o MAD (do inglês, *Median Absolute Deviation*) é um modelo estatístico simples, entretanto robusto em sua execução para o processo de identificação de valores extremos, alcançando resultados satisfatórios (LEYS *et al.*, 2013).

Este modelo utiliza o cálculo da mediana que de certa forma é mais robusto em relação a influência da presença de valores discrepantes. O valor da mediana começa a ser substancialmente influenciado quando atinge mais de cinquenta por cento (50%) de uma distribuição infinita, sendo que seu ponto de ruptura é de 0.5, definido por Donoho & Huber (1983 *apud* LEYS *et al.*, 2013, p. 2).

Para o cálculo do DAM são necessários alguns passos simples abaixo:

- Inicialmente deve-se classificar o conjunto de dados em ordem crescente para encontrar a classificação média das séries estatísticas, e depois encontrar a mediana. A próxima etapa consiste em subtrair a mediana de cada ***n*** observação da série de dados e posteriormente aplicar o valor absoluto nesta nova série. Na última etapa, consiste novamente em encontrar a mediana desse último conjunto de dados gerado e multiplicá-la pela constante ***b* = 1.4826**. Esta constante considera a normalidade dos dados, conforme descrita por Rousseeuw & Croux (1993 *apud* LEYS *et al*.,

2013, p. 2), pois sem esta operação final, o DAM estimaria somente a escala até uma constante multiplicativa (LEYS *et al*., 2013, p. 2).

O cálculo do desvio absoluto da mediana (DAM) é visto como um estimador de escala, sendo totalmente imune ao tamanho da amostra. Sua aplicação e descrição é apresentada pela equação (1).

Para o cálculo do DAM é aplicada a seguinte fórmula:

$$DAM = b\ M_i(|x_i - M_j(x_j)|) \quad (1)$$

onde:

- ✓ x_j: é a *n* observação original.
- ✓ M_j: é a mediana da série original.
- ✓ x_i : é a *n* observação original pela diferença da mediana.
- ✓ $|x_i - M_j(x_j)|$ é: o módulo da diferença entre a observação original pela mediana da observação original.
- ✓ M_i: é a mediana da série absoluta.
- ✓ b: é uma constante de valor **1.4826** supondo-se a normalidade dos dados.

Após a obtenção do resultado do DAM é preciso encontrar um limiar de rejeição, ou seja, os valores superiores a este limiar serão classificados como dados discrepantes (*outliers*).

Recomendado por Miller (1991 *apud* LEYS *et al*., 2013, p. 3), são propostos três critérios de exclusão para serem aplicados ao cálculo da obtenção do limiar de rejeição. Na equação (2) são descritos os procedimentos para encontrar este limiar l_r por meio da aplicação dos seguintes critérios de exclusão:

a) **2.0** (pouco conservador);

b) **2.5** (moderadamente conservador);

c) **3.0** (muito conservador).

Vale ressaltar que, para este processo, o pesquisador tenha um bom conhecimento sobre os dados que serão analisados e realize vários experimentos de testes com cada critério de exclusão. A definição do critério de exclusão c_e, poderá ser calculada tanto para valores discrepantes negativos como também positivos.

O limiar de rejeição é calculado pela seguinte fórmula:

$$M - c_e * DAM < l_r < M + c_e * DAM \quad (2)$$

onde:

- ✓ l_r: é o limiar de rejeição (negativo ou positivo) utilizado para identificar *outliers*.
- ✓ DAM: é o valor do desvio absoluto mediano.
- ✓ c_e: é o critério de exclusão escolhido (**2.0**, **2.5** ou **3.0**).
- ✓ M: é o valor da mediana da série original classificada.

Diante desta análise e revisão da literatura esta proposta de segurança implementa um SDI para VANETs, baseado nas seguintes vertentes:

(a) local de implantação: **descentralizado** e **distribuído**, ou seja, instalado em veículos individuais;

(b) técnica de detecção: **anomalias** com **abordagem estatística**;

(c) modelo estatístico: **identificação de valores extremos (*outliers*)**, aplicado pelo **Desvio Absoluto da Mediana (DAM)**.

No próximo capítulo são elencadas propostas relacionadas com o SDI proposto neste trabalho. Análises específicas sobre SDIs, mecanismos e técnicas de segurança para ambientes veiculares, são comparados e discutidos.

3 TRABALHOS RELACIONADOS

Este capítulo apresenta trabalhos relacionados com a proposta de segurança deste estudo. Propostas que abordam mecanismos, técnicas e SDIs específicos para segurança das operações do STI e na troca de dados dos nós conectados pela VANET. Análises e identificações de lacunas também foram descritas.

Um SDI, como visto no capítulo anterior, depende de diversos fatores para o seu desenvolvimento, funcionamento e implantação. Métricas de desempenho, como exemplo: taxas de detecção de ataques, percentuais de falso positivo e falso negativo, são alguns requisitos aplicados para a validação destes modelos de soluções de segurança (SHARMA; KAUL, 2018; LOUKAS *et al.*, 2019).

Outro fator relevante é para com as características distintas que a rede veicular apresenta em termos de operações, funcionalidades e da comunicação de dados entre seus nós. Também são encontradas dificuldades relacionadas com a mínima existência de requisitos compatíveis, utilizados nos processos de desenvolvimento e testes direcionados ao ambiente do STI. Por exemplo, complexidades na utilização de cenários reais urbanos ou rodoviários, combinação de diferentes aspectos topológicos e geográficos, e questões financeiras inerentes aos custos elevados em aquisições de elementos de comunicação de dados (veículos, RSUs e dispositivos sem fio). Todos estes parâmetros, na maioria das vezes, são desenvoldidos e aplicados por meio de eventos e processos de simulações. São utilizados softwares simuladores, específicos para a criação de cenários de mobilidade e implementação da comunicação da VANET (HASROUNY et al., 2017; SAKIZ; SEN, 2017; SHARMA; KAUL, 2018; LOUKAS *et al.*, 2019).

O estudo proposto por Lyamin *et al*. (2014), consiste em realizar a detecção em tempo real de ataques de negação de serviço (DoS) para VANETs. O protocolo de comunicação sem fio de curto alcance utilizado é o IEEE 802.11p. A proposta em questão, verifica o bloqueio de mensagens periódicas de posição (*beacons*), trocadas entre veículos, através de um pelotão constitúido por até 25 nós. Levaram em consideração as distâncias de 5 metros entre veículos e 15 metros para caminhões.

Foi considerado atacantes do tipo *Jamer*, ou seja, veículos que interferem ou corrompem os pacotes de dados transmitidos pela VANET. Dois tipos de ataques foram utilizados: a) corrupção de pacotes no canal de transmissão e b) corrupção de

beacons. Na primeira fase de execução o nó detector analisa o canal e verifica se não há colisões de *beacons* no momento da transmissão. Já na segunda fase o detector escuta o canal e registra as identificações dos veículos para os quais os *beacons* foram recebidos com sucesso. Um alerta é gerado quando pelo menos um grupo, entre um intervalo definido de tempo, não recebeu exatamente um sinalizador. Outro alarme é gerado quando é identificado perda do sinal, validando-se por meio da existência da colisão de dois nós dentro do mesmo grupo.

Foram analisados e aplicados configurações relacionadas com a camada física e MAC (categoria de melhor esforço) do protocolo IEEE 802.11p. Aplicações de modelos estatísticos como média, probabilidade e funções recursivas foram aplicadas ao estudo. Resultados como a taxa de detecção alcançou 90% e não apontaram nenhum falso positivo. Entretanto, o trabalho não detalha sobre os métodos utilizados para implementação e simulação da comunicação dos veículos no pelotão. Outro fator que limita o processo de detecção é o fato de considerar somente a análise de até 25 nós por pelotões. Este procedimento ficaria limitado, por exemplo, em identificar um ataque de negação de serviço distribuído fora do pelotão (LYAMIN *et al.*, 2014).

Um sistema de detecção de intrusão baseado em host, foi proposto por Zaidi *et al.* (2016). Os autores utilizaram técnicas estatísticas (média, desvio padrão e Teste T de *Student*), para detectar anomalias e nós invasores, classificandos-os como RNs (*Rogue nodes*). Concentraram-se na detecção de informações falsas, especificamente em mensagens de emergência. Cada veículo é capacitado para coletar dados de seus veículos vizinhos e, assim, modelarem o tráfego ao seu redor. Parâmetros entre a relação do fluxo (veículos por hora) e a densidade de veículos (veículos por quilômetro) são base de informações estatísticas. Estes parâmetros permitem que os veículos, numa distância de 500 m (atrás e à sua frente), recebam e/ou transmitam mensagens de outros veículos, calculando a densidade e a velocidade média de seus nós vizinhos. Além do valor calculado do fluxo de tráfego, em sua vizinhança, os nós compartilham entre si a localização e velocidade também. Assim, cada veículo, obtendo tais valores de parâmetros dos demais vizinhos, dentro da distância estabelecida, poderá calcular a média (estimativa) daquela região. O teste de hipótese é aplicado para detectar valores falsos e identificar o veículo como malicioso. Mecanismos de reputação e pontuações de confiança não foram adotados.

Utilizaram os seguintes instrumentais para análises, testes e avaliações: OMNET++ para simulações de rede, SUMO para geração de tráfego e VACaMobil como gerenciador de mobilidade de carros da própria OMNET. Quatro cenários rodoviários, foram analisados e avaliados, sendo o primeiro com acidentes e sem nós maliciosos, no segundo com tráfego normal e sem acidentes, no terceiro cenário, ausente de acidentes, porém com nós maliciosos, e, por útlimo, o quarto cenário, com a presença de acidentes e nós maliciosos. Os autores demonstraram, durante a simulação e ao considerarem o ataque de *Sybil*, que o SDI proposto poderá operar até com 40% de nós, cuja identidade é falsa e maliciosa. Métricas de avaliação foram iniciadas em 5% até 40% com veículos maliciosos. As taxas obtidas foram de 97.5% para detecção de ataques e 2.5% para falso positivo. Entretanto, o modelo proposto aborda somente os ataques de informações falsas e *sybil* (clonagem de identidade simulando diversos veículos falsos). Outra questão importante é melhorar o cálculo da diferença entre valores recebidos e valores obtidos, pois a técnica utilizada só reconhece valores bicaudais como muito altos ou muito baixos. Esse problema implica no reconhecimento de ataques de negação de serviço e negação de serviço distribuída, pois as informações falsas podem variar gradualmente pela densidade e localizações próximas ou distantes (ZAIDI *et al.*, 2016).

Loukas *et al.* (2017), propuseram um sistema de detecção de intrusão, especificamente a um veículo robótico, o qual possui restrições de armazenamento, processamento limitado implicando em latências nos processos de detecções. Outro fator relevante é o consumo de energia, pois o dispositivo depende de bateria para operações contínuas. Essas motivações e justificativas levaram os pesquisadores a criarem um protótipo, no qual o descarregamento computacional (*offloading*) demonstra ser um processo cooperativo e positivo às necessidades que demandam segurança e técnicas de decisões em tempo real. Os autores criaram um modelo matemático que estima o custo energético de uma detecção contínua baseando-se em aprendizagem profunda (com classificação binária), permitindo identificar o número mínimo de pontos de dados usados pelo processo de detecção. Dois fatores cruciais devem ser levados em conta: desempenho e o custo de energia. A tarefa do descarregamento considera o tempo para enviar os dados para o servidor pela rede, o servidor, para concluir o cálculo e o tempo para receber o resultado de volta do servidor.

O algoritmo de aprendizagem profunda deverá retornar 1 para ataque e 0 não ataque. Devido à classificação binária, o tempo de resposta será menor que o tempo total utilizado. Entretanto, nesse estudo de caso, os autores testaram somente o ataque de injeção de comando, por ser considerado um ataque mais complexo em detecção de aprendizagem leve. O estudo visa demonstrar que o processo de *offloading* favorece diversas operações, porém será necessário considerar a latência total (neste caso, coleta de dados, transmissão pela rede, classificação e resposta), tipo do veículo, o ambiente e outras características. Uma observação, também apontada pela pesquisa, é o tempo crítico por estar limitado pela utilização de técnicas leves de aprendizado de máquina. Sempre considerando os limites de tempo e desempenho energético. Outro desafio futuro é aplicar algoritmos de detecção de processamento alto (maiores complexidades), conciliando com a tarefa de *offloading*, não afetando a autonomia operacional do veículo e o consumo energético (LOUKAS *et al.*, 2017).

Na proposta de So, Petit e Starobinski (2019), focaram na detecção de mau compartamento dos veículos, analisando o RSSI (*Received Signal Strength Indicator*), ou Indicador de Intensidade do Sinal Recebido. Especificamente analisando comportamentos em torno da potência do sinal de rádio dos veículos. O trabalho aborda operações relacionadas com a camada física, aplicando um modelo de plausibilidade para identificar falsificações na localização dos nós. Sabe-se que os veículos na VANET, devem enviar suas localizações por meio de mensagens básicas de segurança. O procedimento de detecção é independente, ou seja, executado individualmente por cada veículo, entretando algumas etapas necessitam de RSUs confiáveis.

Os pesquisadores aprimoraram um *dataset*, denominado de VeReMi, para o processo de simulação semelhante ao cenário real. Este conjunto de dados contém cinco tipos de ataques, três tipos de densidades de veículos e variações de veículos atacantes chegando a trinta porcento. Os cinco modelos de ataques englobam alterações e randomizações do envio de posições falsas em diversas situações. Uma interessante análise é feita em torno da relação entre a potência RSSI e a distância de 800 metros de onde o veículo possa estar localizado. Este recurso foi utilizado para comparações entre cenários considerados normais e anormais, ou seja, com atacantes incluídos. Foram adotados três modelos de Plausibilidade, que verificam determinados dados como: RSSI local e abrangente de sua localização,

mensagens básicas de segurança (BSM – *Basic Security Message)* entre veículos e RSUs (confiáveis). Ao receber um sinal de rádio, o RSSI é calculado pelo receptor e comparado com o RSSI abrangente, sendo este distribuído pela RSU mais próxima. São aplicados métodos de validação cruzada para classificar se o BSM é normal ou anômalo.

Foram estabelecidas três técnicas de verificações de plausibilidade. Tais técnicas aplicam modelos estatísticos, como média e variância, para encontrar um intervalo de confiança com base nas distâncias semelhantes, enviadas pelos BSMs do cenário. O primeiro modelo de plausabilidade - *First*-BSM, verifica se o veículo está fora do intervalo de confiança. Já o segundo modelo - *Majority*-BSM, é aplicado com uma regra majoritária aos BSMs recebidos, caso este seja classificado como malicioso o veículo também o será. O terceiro e último modelo - *Weighted*-BSM, utiliza o procedimento de pontuação, sendo este calculado através da aplicação da média móvel ponderada. O veículo ao receber BSMs confiáveis atribui uma pontuação ao transmissor, caso contrário se a pontuação recebida estiver abaixo de 99,7% o veículo será classificado como malicioso (SO; PETIT; STAROBINSKI, 2019).

A ferramenta MATLAB foi utilizada para fins de validação e análise de desempenho. O simulador da rede veicular utilizado é o *VEINS*. Este mecanismo de segurança é dependente de RSU, para que os veículos recebam o valor RSSI abrangente e calculem a validação cruzada do cenário vigente. Caso ocorram perdas de comunicação entre os nós e RSUs, o sistema de segurança ficará comprometido. Diversas validações para cada tipo de ataque foram executadas e resumidamente alcançaram taxas de detecção de 93% para o modelo *Weighted*-BSM, porém com taxa de recorrência de 83%. O modelo *First*-BSM obteve a melhor taxa de recorrência em aproximadamente 84% (SO; PETIT; STAROBINSKI, 2019).

As propostas existentes escolheram diferentes arquiteturas, algumas são baseadas em RSU ou plataforma de nuvem, outras são totalmente distribuídas e ainda outras abordam diferentes modelos de classificação e detecção. Após análises dos trabalhos relacionados e compará-los com a solução de segurança proposta, são descritas as lacunas e a ausência de certas características:

(i) Na proposta de Lyamin *et al*. (2014), os pesquisadores propuseram a detecção de DoS somente quando esse tipo de ataque é direcionado à

corrupção de *beacons* e aos dados dos canais de transmissão. Não especificaram ataques de negação de serviço distribuído, ataques de inundação e o processo de detecção foi baseado em um pelotão de até 25 nós;

(ii) No SDI proposto por Zaidi *et al*. (2016) é baseado em host, porém depende do envio de parâmetros de localização e velocidade dos veículos vizinhos, para que o processo de detecção possa verificar se as mensagens de emergência recebidas são válidas ou falsas. Os autores não implementaram nenhum processo de reputação e não trataram de ataques do tipo DDoS;

(iii) No mecanismo de segurança desenvolvido por Loukas *et al.* (2017), os autores utilizaram uma arquitetura centralizada para detectar o ataque de injeção de comando. No entanto, o SDI utiliza aprendizagem profunda aplicada ao processo de classificação binária. Este fator poderá impactar na latência de recuperação de dados entre o aplicativo de segurança do veículo e a arquitetura de armazenamento remoto;

(iv) No estudo realizado por So, Petit e Starobinski (2019), é específico para a camada física, analisando a potência do RSSI. A técnica de detecção, para ser mais precisa, depende das informações compartilhadas pelas RSUs. Neste trabalho, os pesquisadores não exploraram ataques DoS/DDoS.

O sistema de segurança proposto é resumido na Tabela 4 em comparação com os trabalhos relacionados e elencados anteriormente. Locais de implantação, técnicas de detecção, modelos de classificação de ameaças, principais recursos e características também foram descritas.

No entanto, nenhum dos trabalhos relacionados abordaram a detecção de anomalias causadas pelo mau comportamento da camada de enlace de dados (MAC/LLC). Também não apresentaram a classe de ataque de negação de serviço distribuída (DDoS). Além disso, não implementaram nenhum processo que utilizasse uma lista de reputação para o gerenciamento de nós detectados como maliciosos.

Tabela 4 - Comparação dos trabalhos baseados em SDI para VANETs e STI

	Local de Implantação		**Técnica de Detecção**		**Principais Recursos e Características**	
	Distribuído (nós individuais)	Centralizado (CH, RSU, Cloud)	Anomalia	Modelo de Classificação	Mau comportamento camada MAC	Lista de Reputação
Lyamin *et al.* (2014)	✓		✓	Média, probabilidade e FDA.		
Zaidi *et al.* (2016)	✓		✓	Média, desvio padrão e Teste-t.		
Loukas *et al.* (2017)		✓	✓	Aprendizado profundo (baixo, moderado e alto).		
So, Petit e Starobinski (2019)	✓	✓	✓	Plausibilidade (média, média móvel ponderada e variância).		
Trabalho proposto	✓		✓	*Outliers* (mediana e desvio absoluto da mediana).	✓	✓

Fonte: Autoria própria

Neste trabalho foi proposto uma solução de segurança baseada nos conceitos e operações de um SDI, por meio de um modelo estatístico simples e aplicado na identificação de *outliers*. O mecanismo de segurança utiliza a técnica de detecção de anomalias, oriundas do mau comportamento do envio de *frames* MAC. Atuando no monitoramento do protocolo ARP e contabilizando o recebimento de requisições ARP REQUEST, para detecção de ataques DoS/DDoS. O SDI também implementa uma lista de reputação para o armazenamento de nós maliciosos. Suas funcionalidades, operações e recursos são apresentados no capítulo seguinte.

4 MECANISMO DE DETECÇÃO DE ATAQUES PARA STI (MDASTI)

Neste capítulo é apresentada a metodologia aplicada no desenvolvimento do Mecanismo de Detecção de Ataques para Sistema de Transporte Inteligente (MDASTI). Além da justificativa e motivação, são abordadas suas funcionalidades, operações e etapas envolvidas na implementação. Também são descritos o local de implantação do MDASTI, a abordagem aplicada ao processo de detecção e classificação de ataques, juntamente com seus algoritmos de monitoramento e análise dos dados.

4.1 Visão geral do MDASTI

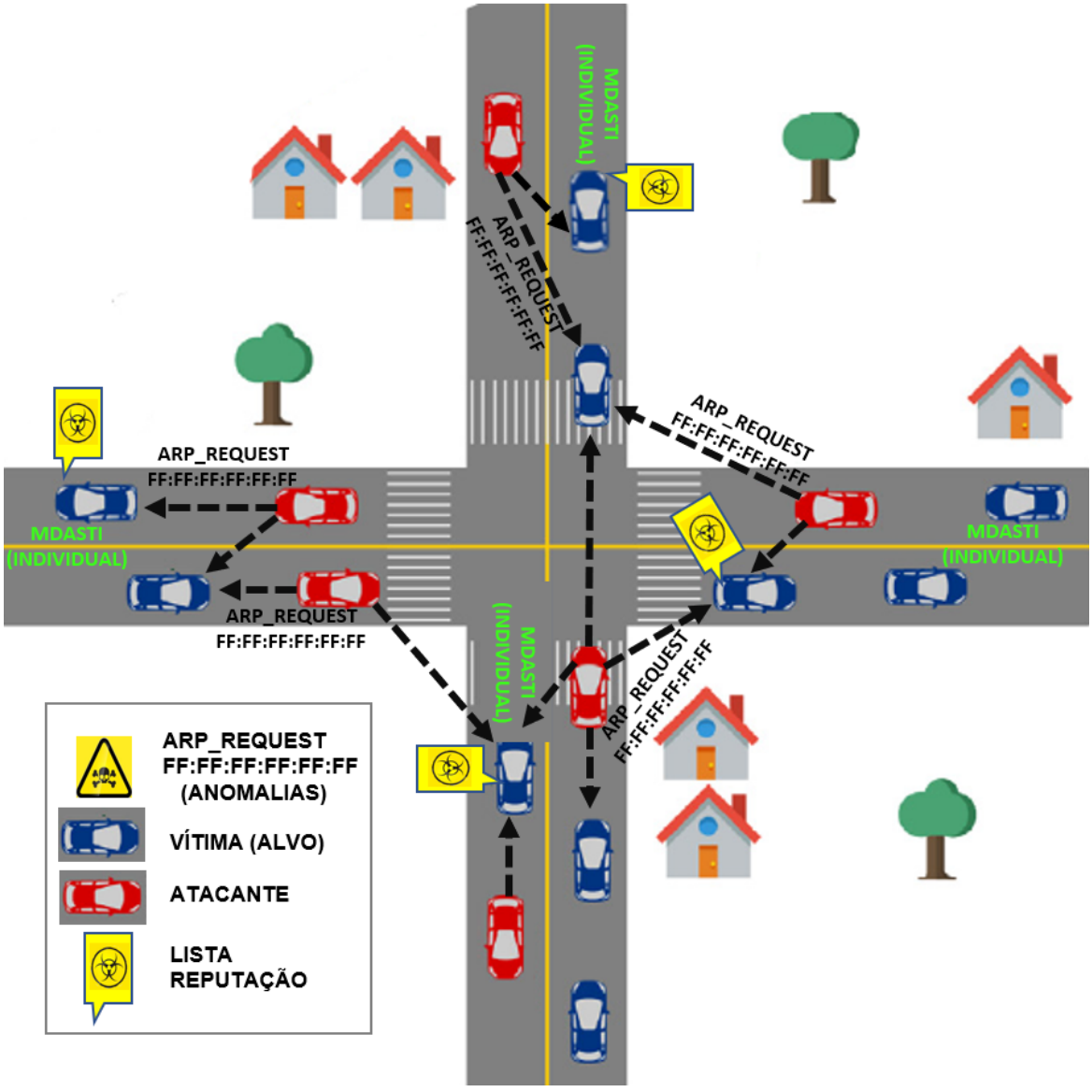
O estudo em questão visa a segurança e a proteção da vida humana envolvidas no campo de transporte terrestre, especificamente os ocupantes dos veículos (condutores e passageiros) e pedestres do âmbito urbano. Mediante os avanços dos recursos computacionais no meio automobilístico, através das redes veiculares e dos sistemas de transporte inteligente, justificam-se contribuições e propostas de melhorias a essas emergentes tecnologias e recursos.

Todas estas inovações tecnológicas, tem buscado melhorar a vida do âmbito urbano por meio de um amplo contexto social, político e econômico. Entretanto, independente destes avanços, ainda em sua maioria, os veículos e estas novas tecnologias são conduzidas por seres humanos. Assim sendo, a combinação de veículos e inovações tecnológicas necessitam constantemente de olhares vigilantes à sua segurança. São inúmeros os desafios e complexidades para que esta combinação não seja utilizada por atacantes e motoristas maliciosos, para fins prejudiciais. Inúmeras situações drásticas e até mesmo consequências fatais poderão ocorrer, devido ao envolvimento de veículos e vidas humanas. Diante destes fatores preocupantes este trabalho foi motivado a propor um mecanismo de segurança para detecção de ataques e ameaças inerentes às operações de comunicação da VANET e dos dispositivos que integram o STI.

Uma de suas funcionalidades é possibilitar que sua atuação seja independente de infraestruturas de comunicação (RSUs), pelotões de conduções e de veículos denominados cabeças de *clusters*.

Os processos de execução e processamento são atribuídos localmente, ou seja, para cada veículo individualmente. Na Figura 11 é apresentada uma abstração do funcionamento dos elementos constituintes e das operações do MDASTI. Também são visualizados veículos maliciosos efetuando o ataque de DoS/DDoS aos veículos alvos.

Figura 11 - Estrutura e elementos do MDASTI



Fonte: MDASTI

A ação maliciosa deverá ser detectada por qualquer veículo em percurso. Após a ameaça (DoS e/ou DDoS) ser detectada, informações referentes ao veículo atacante deverão ser armazenadas, pelo MDASTI, em uma estrutura de dados denominada de lista de reputação. A justificativa desta lista de reputação baseia-se

na possibilidade de que ambos veículos poderão se reencontrar novamente, durante o percurso diário. Sendo assim, o veículo vítima terá condições de consultar a sua lista de reputação e identificar se o veículo vizinho é ou não malicioso.

A implementação e geração de resultados são realizados por meio do processo de simulação. Devido às restrições de cenários para testes e prototipagem, serão utilizados softwares simuladores para o funcionamento real da rede veicular e da mobilidade dos veículos do percurso urbano. Após o término das simulações, os dados gerados foram processados e analisados, para fins de validação e desempenho do MDASTI.

4.2 Local de implantação do mecanismo

A escolha do local de implantação de um SDI é muito importante, pois dependendo de sua atuação poderá impactar nos processos de detecção e no seu desempenho.

O MDASTI é executado por **nós individuais**, seguindo o modelo **descentralizado** e atuando na **detecção de ataques locais** (baseado em *host*).

4.3 Técnica de detecção e modelo de ataque

A técnica de detecção empregada pelo MDASTI é baseada em **detecção por anomalias**, analisando o comportamento das atividades do sistema em busca de eventos ou indicadores estatísticos considerados com valores extremos. Neste trabalho são consideradas anomalias o envio de inúmeras requisições por meio do protocolo ARP (*Address Resolution Protocol*), ou Protocolo de Resolução de Endereços.

O modelo de ataque explorado é o ataque de negação de serviço. Sendo combinadas quatro características inerentes ao DoS/DDoS:

(i) **inundação (*flooding*)**: envio de solicitações **ARP *REQUEST*** em intervalos de tempo, variando entre 5 e 10 segundos;

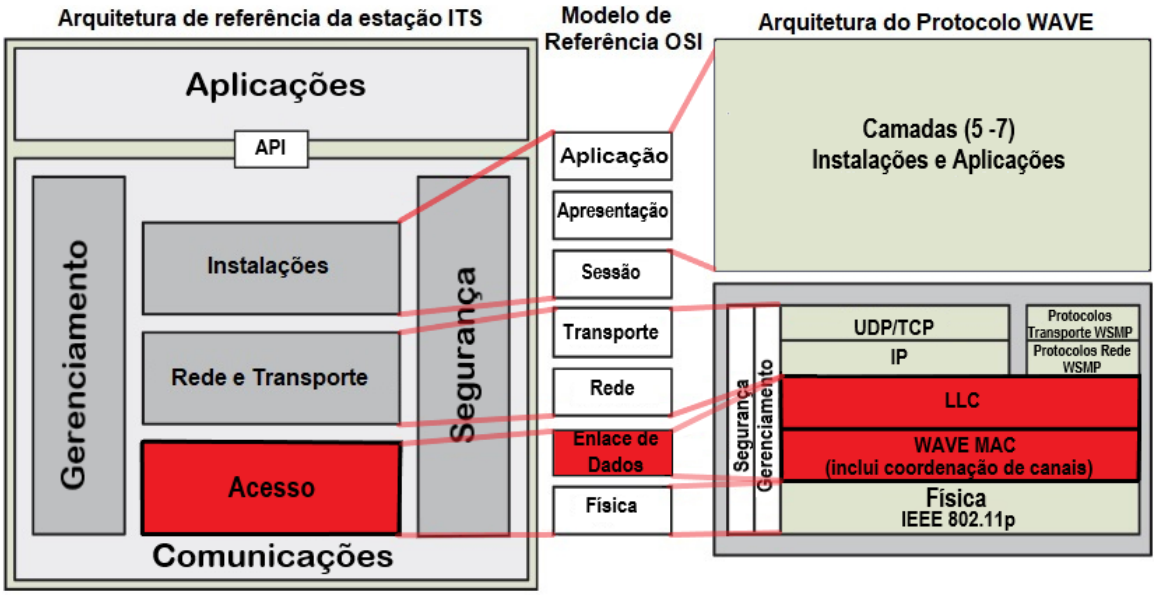
(ii) **tempestade de pacotes (*packet storm*)**: são enviados a todos os veículos da VANET inúmeros quadros **MAC;**

(iii) **negação de serviço distribuída (DDoS)**: veículos maliciosos serão injetados na rede veicular, para cada simulação, utilizando a faixa de percentuais: 5%, 10%, 15%, 20% e 25% de atacantes;

(iv) **desassociação (*deauth*)**: quadros **MAC** maliciosos, são direcionados a todos os veículos da rede. Por tratar-se de solicitações **ARP *REQUEST*** o campo endereço de destino (**MAC_DST)** do quadro **MAC**, armazenará o valor hexadecimal "**ff:ff:ff:ff:ff:ff**", sinalizando que este quadro é transmitido por *broadcast*.

Este modelo de ataque explora especificamente a camada de enlace de dados e de controle de acesso ao meio (MAC). Na Figura 12 é destacada a camada afetada, sendo referenciada pelos modelos e arquiteturas de rede OSI/ISO (*Open System Interconnection / International Organization for Standardization*) e WAVE. O padrão OSI (traduzido como, Interconexão de Sistemas Abertos) é um modelo referencial de redes de computadores estabelecido pela Organização Internacional de Padronização (IEEE 802.11, 2016, p. 231).

Figura 12 - Camada explorada pelo ataque



Fonte: adaptado de IEEE Std 1609.0 (2019)

4.3.1 Método de classificação do ataque

São descritas nesta subseção as operações e funcionalidades sobre o método abordado pelo algoritmo de detecção e classificação de anomalias, por meio de modelo estatístico.

Com o objetivo de estabelecer um equilíbrio entre as taxas de detecção, mínimas incidências de falsos positivos e falsos negativos, levou em consideração a relação entre o local de implantação e a técnica de detecção adotada. Essa justificativa é originada pelos fatores relacionados ao custo computacional, exercido pelo algoritmo de detecção. Vale ressaltar também a importância de fatores que possam interferir no desempenho do mecanismo, entre eles - restrições e limitações do hardware, espaço de armazenamento e do software operacional. Estes requisitos devem ser sempre levados em conta, pois cada veículo difere em sua arquitetura de padrão de fábrica.

Assim sendo, para o processo de detecção e classificação de anomalias o MDASTI aplica o conceito de identificação e análise de valores extremos ou *outliers*, por meio do modelo estatístico do **Desvio Absoluto da Mediana (DAM)**. Um modelo estatístico simples, entretanto, eficaz na execução de procedimentos direcionados na identificação de valores extremos (LEYS *et al.*, 2013).

Contudo, o valor obtido pelo DAM não deve ser aplicado unicamente como parâmetro de decisão, pois a identificação de valores discrepantes será ineficaz. Sendo assim, a próxima etapa, é necessário encontrar um limiar de rejeição (l_r) no qual será aplicado na etapa de identificação de *outliers*. Este limiar define no conjunto de dados, o valor limite para os dados considerados dentro de um comportamento padrão, ou seja, não anômolos. Os valores superiores ao limiar de rejeição ($l_r > outliers$) são considerados discrepantes, ou seja, anômolos.

Para o cálculo do l_r podem ser utilizados três critérios de exclusão (c_e), conforme Leys *et al.* (2013): (a) **2.0** (pouco conservador), (b) **2.5** (moderadamente conservador) e (c) **3.0** (muito conservador).

Para uma análise mais ampla e fins de validação do MDASTI, foram realizadas simulações para cada um dos critérios de exclusão mencionados acima. Após obtenção dos resultados e análises, foram observados quais os c_e exerceram o melhor equilíbrio entre as taxas de detecção, número de falsos positivos e falsos negativos.

Uma observação, não menos importante, este estudo considerou somente valores discrepantes com tendência positiva, ou seja, *outliers* com disposição $l_r > n, \ldots, n+1$.

Considerando o ambiente das VANETs, no qual as conexões entre os veículos são realizadas em mínimos intervalos de tempo, ataques DoS poderão impactar severamente o funcionamento da rede veicular e leva-lá à grandes instabilidades. Ressaltando que o modelo de ataque abordado, neste estudo, fará com que os veículos recebam enormes quantidades de solicitações ***ARP REQUEST***, gerando assim inúmeras ocorrências de eventos anômolos.

O MDASTI utiliza dois algoritmos, sendo executados diretamente no veículo individual. Neste processo foram monitorados e analisados quadros MAC, por meio dos campos: *EtherType* - identificação de protocolo na subcamada LLC[13], envio de solicitações ARP *REQUEST* e a contabilização das requisições ARP enviadas. Os algoritmos foram desenvolvidos com base nos parâmetros disponíveis e fornecidos pelo simulador, sendo referenciados pelo padrão IEEE 802 (2014).

Os processos executados por estes dois algoritmos, são descritos pelas fases:

(1) Monitorar e analisar constantemente quadros MAC recebidos dos veículos dentro de sua faixa de rádio;

(2) Identificar no campo *Ethertype* do quadro MAC recebido, o valor *0x0806*, no qual representa a identificação do protocolo ARP oriundo da subcamada LLC;

(3) Ao identificar se o quadro MAC é constituído pelo protocolo ARP, será necessário distinguir se o quadro transporta uma solicitação ARP *REQUEST* ou uma resposta ARP *REPLY*;

(4) Se for uma solicitação ARP *REQUEST*, constará em seu campo de endereço de destino o valor ff:ff:ff:ff:ff:ff (*broadcast*);

[13] LLC – *Logical Link Control*, ou Controle de *Link* Lógico. Uma subcamada (superior) da camada de Enlace de Dados que atua juntamente com a subcamada MAC, para a troca de unidades de pacotes de dados (PDU) entre camadas pares LLC (IEEE 802.11p, 2016).

(5) Nesta primeira fase e descritas no Algoritmo 1, são coletados o *TimeStamp* (registro temporal do evento), endereços MAC e IPv4 do veículo que originou o quadro MAC, e o campo *TotalArpReq*, incrementado (em +1) e adicionando a nova requisição ARP. Estes campos constituem uma estrutura de dados mantida pelo próprio MDASTI;

(6) Na segunda fase, demonstrado pelo Algoritmo 2, é executado o processo de detecção empregando o modelo estatístico do **DAM**. O algoritmo analisa, na estrutura de dados, o campo que contém o total de requisições ARP, recebidas de cada veículo vizinho, buscando identificar valores considerados extremos;

(7) Ao detectar veículos que tenham grandes quantidades de envios de solicitações ARP *REQUEST*, por meio do campo *TotalArpReq*, estes serão classificados como maliciosos, bloqueando-os na rede e armazenando-os em uma lista de reputação local.

A escolha do uso do método do desvio absoluto da mediana é devida a sua consistência e ao mesmo tempo simplicidade de processamento na identificação de *outliers*. Por tratar-se de valores extremos, ou seja, quantidades enormes de requisições oriundas de um ataque DoS/DDoS, este modelo apresenta maior solidez quando comparado com a aplicação do cálculo da média somada a dois ou três desvios-padrão.

Geralmente o cálculo da média é aplicado para encontrar medidas que indicam uma tendência central. Para conservar os dados e obter uma margem de segurança em uma distribuição bicaudal, o pesquisador soma ou subtrai o resultado da média ao cálculo de um ou até três desvios-padrão. Contudo, a média poderá ser substancialmente influenciada pelos valores discrepantes e, assim, resultando em um valor distorcido (BRUNI, 2013).

O indicador de insensibilidade de uma amostra de dados é denomiando de ponto de ruptura, no qual é baseado no número máximo de observações. Por exemplo, ao calcular a média de uma distribuição infinita, obteremos também um valor médio infinito, pois o seu ponto de ruptura será zero (0). Em contrapartida o

cálculo da mediana não sofre fortes influências pela presença de valores extremos, pois ele retorna o centro de uma série ordenada (BRUNI, 2013).

4.3.2 Descrição dos algoritmos do mecanismo de segurança

Os algoritmos utilizados pelo MDASTI são apresentados nesta subseção, utilizando a descrição pseudocódigo.

No Algoritmo 1 são realizados o monitoramento, análise e coleta dos dados dos quadros MAC, recebidos pela camada de enlace de dados (MAC/LLC). Para cada pacote da subcamada superior LLC recebido, entre as linhas 3 e 5, será verificado se o campo *EtherType* possui o valor de identificação *0x0806* correspondente ao protoclo ARP.

Se este valor existir, linha 6, verifica se o quadro MAC é uma solicitação ARP *REQUEST*, pois o monitoramento será realizado somente em requisições ARP. Caso a requisição ARP seja verdadeira, entre as linhas 7 e 10, são coletados os dados *TsArpReq* (*timestamp* do recebimento do quadro MAC), *MacOri* (MAC origem emissor), *IpOri* (IPv4 origem emissor) e declara a variável *ArpReq* (armazenará a quantidade de requisições ARP).

O mecanismo mantém uma estrutura de dados denominada de *VetorMAC*, linhas 12 e 13, que armazenará os campos coletados toda vez que houver um ARP *REQUEST.*

Entre as linhas 15 e 20, o algoritmo varre toda a estrutura, comparando se o MAC recebido encontra-se armazenado na estrutura de dados *VetorMAC*. Caso ele esteja, o campo *TotalArpReq* será incremetando com +1 e o campo *TimeStamp* será atualizado com o novo valor de *timestamp*.

Na linha 23, caso não tenha sido encontrado este novo veículo na tabela, baseando-se no endereço MAC, este será adicionado juntamente com seus dados. Todos esses procedimentos monitoram o acesso ao meio e o envio de solicitaçãos ARP *REQUEST*.

No Algoritmo 2, é analisado o campo *TotalArpReq* da estrutura *VetorMAC*, sendo a entrada deste algoritmo. Este campo armazena o total de ARP *REQUESTs* enviados por cada veículo vizinho.

Algoritmo 1 – Monitora, analisa e coleta dados do quadro MAC

```
1:  ENTRADAS: LLC_Ethertype(0x0806), FrameMAC.
2:  SAÍDAS: VetorMAC, TabelaMAC.
3:  para cada LLC recebido faça
4:      se (LLC) então
5:          se (Ethertype == 0x0806) então
6:              se (QuadroMAC == ARP_REQUEST) então
7:                  TsArpReq ← TempoAtual;
8:                  MacOri ← Mac48Address _HardwareOrigem;
9:                  IpOri ← Ipv4Address_Ipv4Origem;
10:                 declara ArpReq ← 0;
11:                 aux ← 0;
12:                 se (VetorMAC.tamanho < 1) então
13:                     VetorMAC.insere ← ({TsArpReq, MacOri, IpOri, ArpReq});
14:                 senão
15:                     para (VetorMac.início até VetorMac.fim) faça
16:                         se (VetorMac.MacOrigem == MacOri) faça
17:                             aux ← 1;
18:                             VetorMac.TotalArpReq ← +1;
19:                             VetorMac.TimeStamp ← TsArpReq;
20:                         fim se
21:                     fim para
22:                     se (aux == 0)
23:                         VetorMAC.insere ← ({TsArpReq, MacOri, IpOri, ArpReq});
24:                     fim se
25:                 fim se
26:             fim se
27:         fim se
28:     fim se
29: fim para
```

Fonte: Autoria própria - MDASTI

Dentro de intervalos estabelecidos, considerando a cada 2 segundos, são criadas duas estruturas de dados do tipo vetor estrutura (*vDados* e *vListaReputação*), nas linhas 3 e 5. Entre as linhas 6 e 10, o campo *TotalArpReq* da estrutura *VetorMAC* é varrido e todo seu conteúdo, naquele instante momento, é copiado para o novo vetor *vDados.* Este campo armazenará todos os veículos vizinhos que enviaram solicitações ARP *REQUEST* ao veículo em questão.

Neste momento é executado a detecção de anomalias, procurando por valores extremos, nesta estrutura de dados por meio do modelo estatístico DAM, descrito na linha 11. A cada $x_j, \ldots, x_j + 1$ corresponde aos valores de cada veículo armazenados no campo *TotalArpReq*, copiados para a estrutura *vDados*. A variável M_j calcula a mediana da série original $x_j, .., x_j + n$, depois calculará a diferença da série original com o resultado da mediana e encontrará o seu valor absoluto. Onde que ^{M}i calculará novamente a mediana, porém agora, na série com os valores

absolutos $x_i, \ldots, x_i + 1$. Este processo descreve a aplicação do cáculo do desvio absoluto da mediana $DAM = b\ M_i(|x_i - M_j(x_j)|)$.

Após calcular o DAM é necessário encontrar o valor do limiar de rejeição, ou seja, um valor máximo do conjunto de dados que definirá o limite máximo da normalidade dos dados. Valores superiores a este limiar, serão considerados *outliers* (anômolos).

Algoritmo 2 – Detecção de anomalias com DAM

```
1:  ENTRADAS: VetorMAC.
2:  SAÍDAS: VeículoMalicioso, vListaReputação.
3:  para cada (intervaloTempo ← 2 segundos) faça
4:      declara vDados[VetorMAC.tamanho];
5:      declara vListaReputação estrutura ListaRep (TimeStamp, MacMAL, IpMAL, TotalEnvArpREQ);
6:      Aux ← 0;
7:      para (VetorMac.início até VetorMac.fim) faça
8:          vDados[aux] ← VetorMAC.TotalArpReq;
9:          aux ← +1;
10:     fim para
11:     DAM = b M_i(|x_i − M_j(x_j)|) ← vDados.TotalArpReq;
12:     MEDIANA ← vDados.TotalArpReq;
13:     se (Ce = 2.0) então
14:         Outlier ← MEDIANA + (2.0 * DAM);
15:     senão
16:         se (Ce = 2.5) então
17:             Outlier ← MEDIANA + (2.5 * DAM);
18:         senão
19:             se (Ce = 3.0) então
20:                 Outlier ← MEDIANA + (3.0 * DAM);
21:             senão
22:                 imprima "Critério Inválido!";
23:             fim se
24:         fim se
25:     fim se
26:     para (VetorMAC.início até VetorMAC.fim) faça
27:         se (VetorMAC.TotalArpReq > Outlier) então
28:             imprima "Veículo Malicioso: " ← VetorMAC.MacOrigem;
29:             vListaReputação.insere ← VetorMAC.({TimeStamp, MacMAL, IpMAL, TotalEnvArpREQ});
30:         fim se
31:     fim para
32: fim para
```

Fonte: Autoria própria - MDASTI

Para este processo é necessário a escolha entre três critérios de exclusão Ce, que são descritos entre as linhas 13 e 25. Estes critérios são: (a) $Ce = 2.0$, (b) $Ce = 2.5$ e (c) $Ce = 3.0$, e deverão ser aplicados individualmente pela fórmula $Outlier = Mediana + (Ce*DAM)$. Soma-se a mediana da série original ordenada

$Mediana\ (vDados.TotalArpReq)$, linha 12, pelo produto entre o critério de exclusão escolhido Ce e o resultado do $DAM.$ Após encontrar o limiar de rejeição $Outlier,$ é feita uma varredura na estrutura *VetorMAC*, linha 26, comparando se o veículo que conter em seu total de requisições ARP um valor maior que o limiar de rejeição ($VetorMAC.TotalArpReq > Outlier$), então este será classificado como "*Veículo Malicioso*", linhas 27 e 28.

Na linha 29 é determinada a estrutura de dados *vListaReputacao*, sendo esta responsável em armazenar todos os veículos detectados como "*malicioso*". Sua descrição é apresentada na seção seguinte.

4.4 Lista de reputação

O MDASTI mantém uma lista de reputação local, armazenada pelo MDASTI no próprio veículo, para fins de bloqueios dos dados classificados como anômolos. Podendo consultá-la diariamente, para verificar quais veículos do percurso urbano são considerados "maliciosos". Empiricamente a lista poderá ser apagada ou reiniciada, conforme decisões do condutor (usuário).

No próximo capítulo são descritas as etapas envolvidas nas simulações e apresentação dos resultados obtidos.

5 EXPERIMENTOS E RESULTADOS

Após a execução de inúmeras etapas de simulações, informações como logs e arquivos de rastreio foram gerados para análises e validações dos respectivos resultados. Sendo assim, este capítulo foi dividido em duas seções. Na primeira são descritos os procedimentos recorrentes aos experimentos de simulação, mapa geográfico urbano utilizado, parâmetros da rede veicular e ações do modelo de ataque implementado. A partir da seção 5.4 Resultados, são apresentadas as métricas de desempenho utilizadas, validações e os resultados alcançados.

5.1 Cenário realístico urbano e simulação da mobilidade veicular

A mobilidade do tráfego veicular realístico foi realizada por intermédio do simulador de mobilidade urbana – SUMO. Uma aplicação de código aberto nomeada de *Simulation of Urban MObility* (LOPEZ *et al*., 2018). A versão utilizada foi a 1.5.0 (SUMO, 2020).

Entretanto, antes de configurar e estabelecer os parâmetros de mobilidade, se faz necessário importar o mapa geográfico que será aplicado ao processo de simulação do percurso urbano veicular.

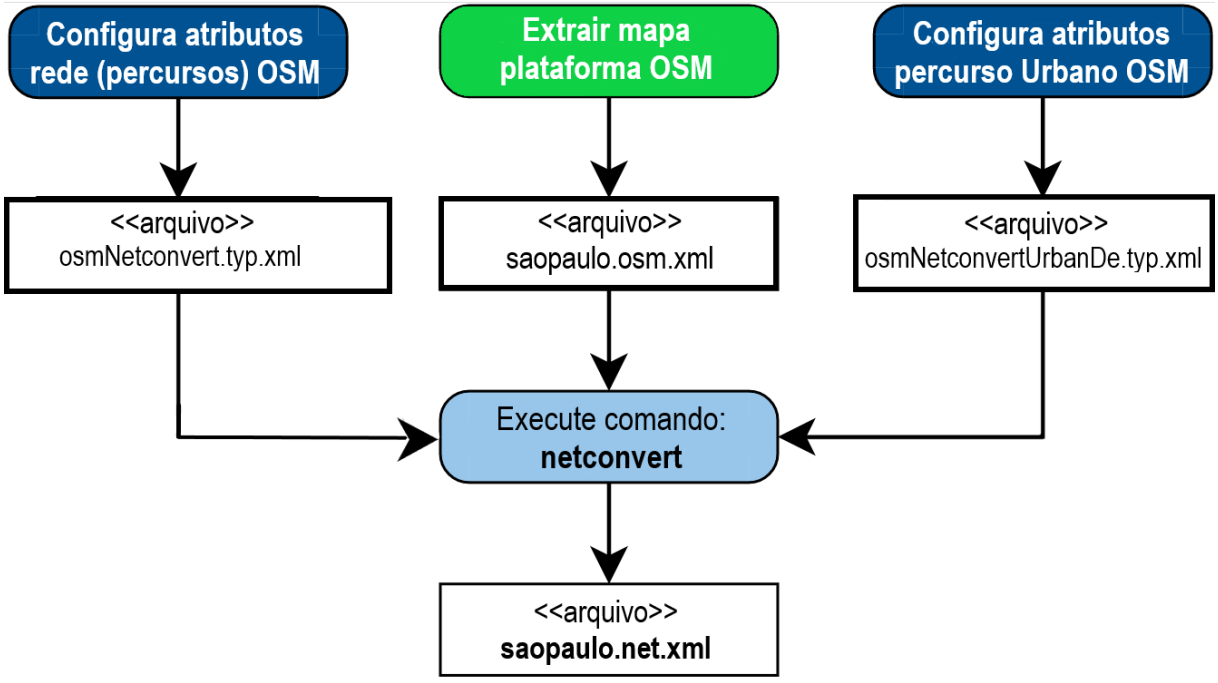
A ferramenta utilizada, nesta etapa, foi a plataforma de dados abertos de mapeamento, denominada de *OpenStreetMap* (OSM). Mantida por uma comunidade de usuários voluntários e mapeadores de diversas localizações ao redor do mundo (OSM, 2019a). O percurso urbano selecionado para o processo da simulação da mobilidade veicular foi a cidade de São Paulo, no Brasil. Trata-se de uma localização de altas densidades no fluxo de veículos, sendo constituída por diferentes aspectos topográficos (OSM, 2019b). A imagem do mapa do percurso urbano realístico é ilustrada na Figura 13.

O local selecionado foi exportado diretamente do próprio site da ferramenta OSM, gerando um arquivo no padrão XML (*Extensible Markup Language*). Após a obtenção da área do percurso urbano, foram realizadas configurações e parametrizações para que o mapa do OSM seja importado pelo simulador SUMO. Os passos utilizados pelos parâmetros de importação, próprios do SUMO, são visualizados na Figura 14.

Figura 13 – Mapa do percurso urbano realístico

Fonte: Mapa da cidade de São Paulo, Brasil, por OpenStreetMap (OSM, 2019b)

Figura 14 - Parâmetros de convesão mapa OSM para simulador SUMO



Fonte: Adaptado de SUMO (2020)

Após a conversão do mapa OSM, nesta última etapa, se faz necessário algumas parametrizações por meio do SUMO:

(a) **Polígonos:** considerado pontos de interesses através de formas geométricas (edifícios, rios, indústrias etc). Utiliza-se o comando, *polyconvert*;

(b) **Percurso Aleatório:** configura a quantidade de veículos, entradas e saídas destes e o tempo total do percurso. Utiliza-se o comando, *randomTrips.py rede.net.xml -b tempo_inicial -e tempo_final -p índice_de_cálculo_total_de_veículos -r rout.xml*. Obs: para o cálculo de 120 veículos com duração de 300 segundos de simulação, deverá ser calculado o índice do parâmetro *-p*. Operação: *-p = ((tempo_inicial – tempo_final) / número_total_de veículos)*. Exemplo: *((0 – 300) / 120))* = *2.5*, então temos *-p 2.5*;

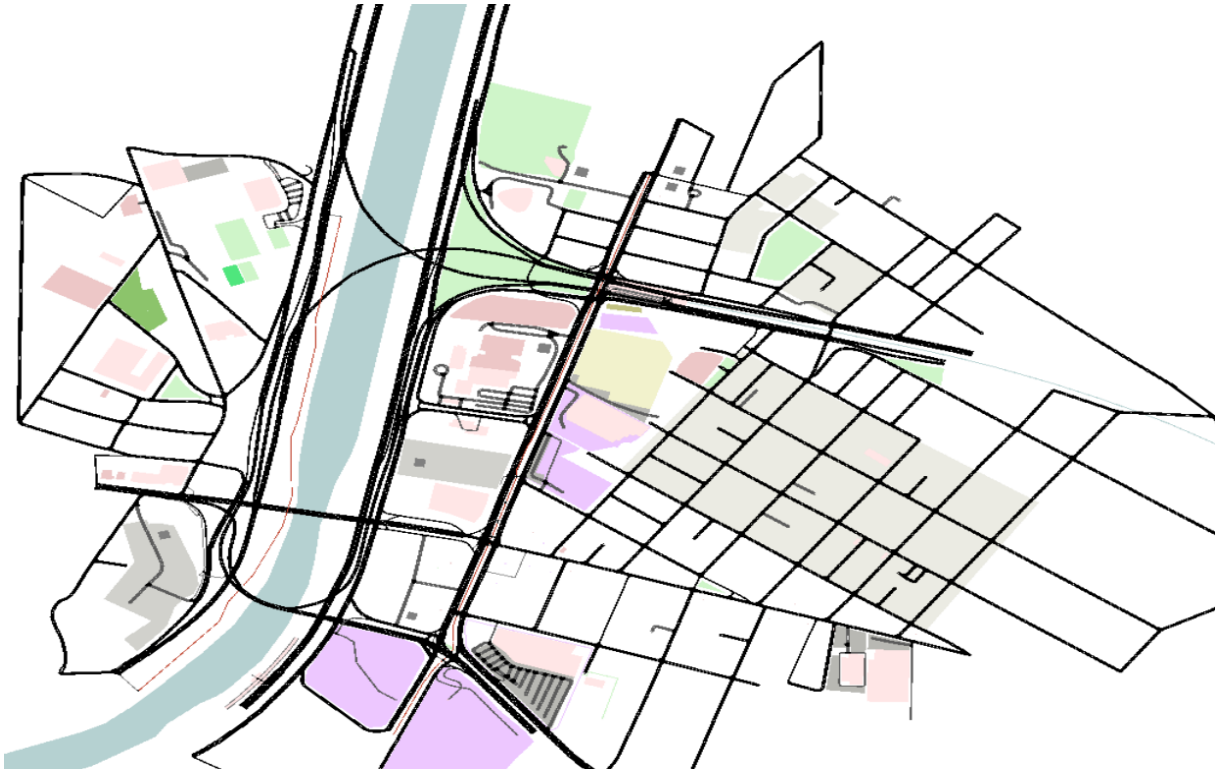
(c) **Arquivo de parâmetros SUMO:** o arquivo de configuração geral, ou seja, que agrega a rede, rotas da mobilidade, tempo de simulação e tipo de cenário é denominado de *arquivo.sumocfg*, cujo formato é XML;

(d) **Geração do *trace* (arquivo de rastreio)**: para a geração da mobilidade dos veículos juntamente com suas posições e velocidades variadas, utiliza-se o comando, *sumo -c arquivo.sumocfg --fcd-output mapa.sumotrace.xml*;

(e) **Conversão mobilidade SUMO para NS-3:** nesta última etapa será realizada a conversão de todo o percurso, rotas, total de veículos, velocidades, posições e tempo total de simulação para o simulador da rede veicular. Utiliza-se o comando:
traceExporter.py –fcd-input mapa.sumotrace.xml --ns2mobility-output mobilidade_ns3.mob.

Na Figura 15 pode ser visualizado o mapa, após ser convertido para os parâmetros de configuração e simulação do simulador SUMO. Sua execução, para fins de validação e visualização do cenário, poderá ser realizada pelo comando: *sumo-gui arquivo.sumocfg.*

Figura 15 – Mapa percurso urbano São Paulo convertido para o SUMO



Fonte: Gerado por SUMO (2020)

5.2 Comunicação e simulação da rede veicular

A implementação das funcionalidades da VANET, tais como - arquitetura da rede veicular, protocolos de comunicação sem fio, mobilidade entre os nós e a geração de pacotes de dados, foram desenvolvidos por meio do simulador de redes de computadores NS-3 (*Network Simulator*), versão 3.30. Simulador de código aberto e utiliza como base de programação o compilador C++. Sua estrutura de implementação é toda realizada por meio da programação orientada a objetos. Classes, métodos, atributos, parâmetros e uma série de exemplos de simulações, estão disponíveis em sua documentação (NS-3, 2019).

Para a comunicação sem fio e dedicada de curto alcance foi utilizada a pilha de protocolos IEEE 802.11p, com taxas de transmissão de 6 Mbps e operações de

acesso ao canal de transmissão com frequências de 10 MHz. O protocolo de roteamento empregado, para a comunicação *broadcast, unicast* e *multicast*, foi o protocolo de roteamento de estado de *link* otimizado - OLSR (do inglês, *Optimized Link State Routing Protocol*).

O NS-3 também possibilita simular aplicações cliente-servidor. Sendo assim, foram estabelecidos em alguns veículos como estações servidoras de aplicações UDP, e permitindo que os demais nós enviem datagramas de tamanho de 64 KBytes. Na implementação dos veículos maliciosos, estes foram incluídos no cenário da rede veicular a partir de intervalos de tempo entre 4 e 5 segundos de simulação. Procedendo com esta aleatoriedade até o tempo final de simulação. Foram considerados os percentuais do número de atacantes entre 5%, 10%, 15%, 20% e 25% de um total de 120 nós (veículos).

Na Tabela 5, são descritos os parâmetros devidamente com seus valores de configuração, aplicados durante os processos de simulação do MDASTI.

Tabela 5 - Parâmetros da simulação

Parâmetros	**Valores**
Simulador	NS-3.30
Tempo de Simulação	180 segundos
Mapa Geográfico	OpenStreetMap (OSM)
Cenário do Percurso	Urbano realístico
Modelo de Mobilidade	SUMO (cidade de São Paulo, Brasil)
Modelo de Propagação	*Two-Ray Ground*
Total de Veículos	120
Número de Veículos Servidores	10 – 30
Percentual de Veículos Maliciosos	5% – 25%
Tempo de Variação do Ataque	4 – 5 segundos
Protocolo Camadas Física e MAC	IEEE 802.11p
Protocolo de Roteamento	OSLR
Modulação	OfdmRate6MbpsBW10MHz
Abrangência de Rádio	1000 metros
Potência de Transmissão (TX)	33.8 dBm – 60.0 dBm
Protocolo de Transporte	UDP
Tamanho do Datagrama (*payload*)	64 KB

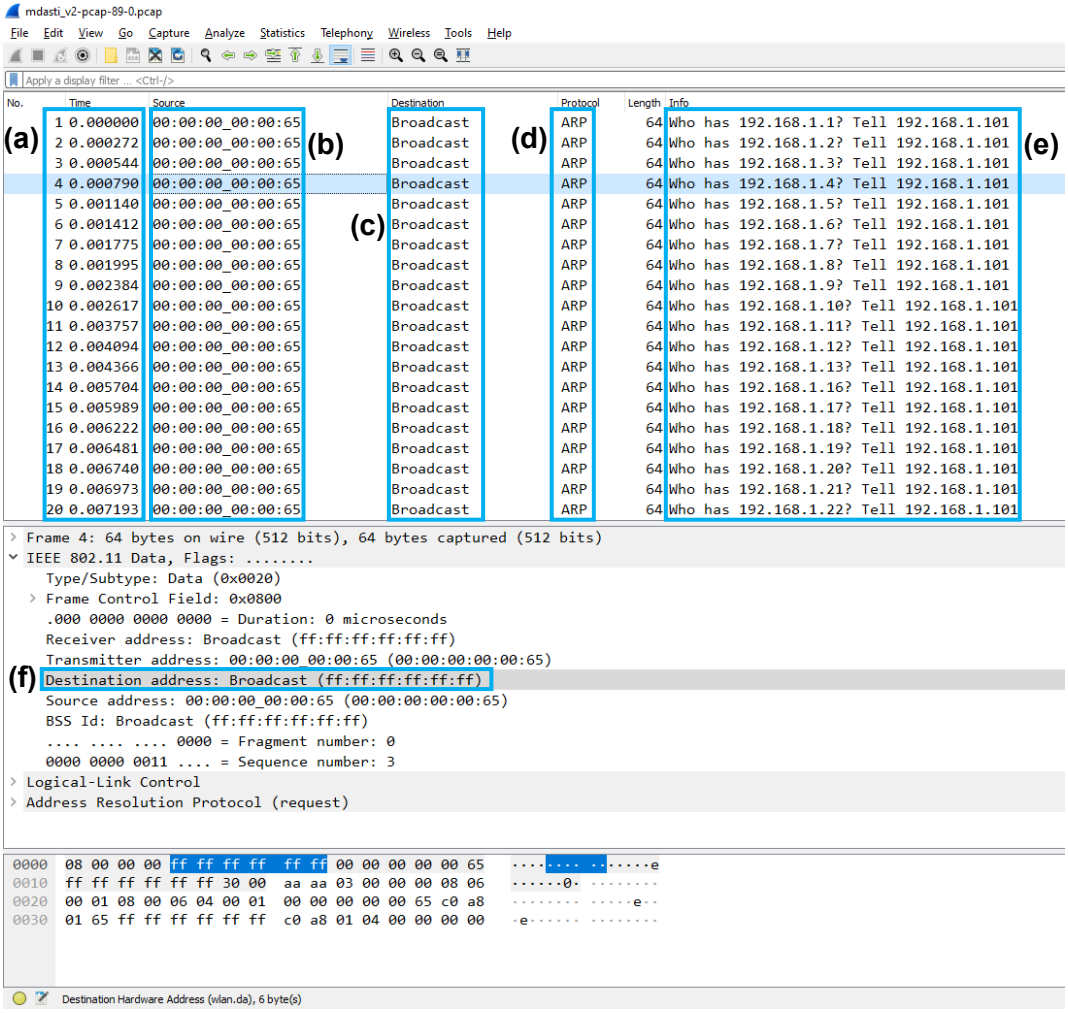
Fonte: Autoria própria – MDASTI

5.3 Implementação do ataque de negação de serviço

A execução e implementação do ataque de negação de serviço foi realizada diretamente no simulador NS-3.30. A quantidade de nós maliciosos variou entre 5% e 25% (entre 6 a 30 veículos), sendo estas informadas no início da simulação. O próprio simulador, por meio de variáveis aleatórias, realizou a seleção dos nós maliciosos entre o total de 120 veículos.

Para esta etapa, pós-simulação, foi utilizada a ferramenta de análise de pacotes - *Wireshark*[14]. Por meio da análise dos logs, gerados no formato PCAP, são observadas na Figura 16 a efetivação e realização do ataque explorado.

Figura 16 - Visualização de quadros MAC oriundos do ataque DoS/DDoS



Fonte: MDASTI - análise de log no formato PCAP pela ferramenta *Wireshark*

[14] *Wireshark* vr. 3.2.4 – ferramenta para análise de protocolos e pacotes de rede capturados em formato de arquivos (.PCAP). Disponível em: https://www.wireshark.org/. Acesso em: 18 jan. 2020.

A análise do ataque gerado, visualizados anteriormente na Figura 16, são descritos a seguir elencando características do DoS/DDoS:

(a) mínimos intervalos de tempo, em microssegundos, entre cada solicitação;

(b) endereço MAC que originou o ataque: **00:00:00:00:00:65**;

(c) transmissão no modo ***Broadcast*** para o destino;

(d) tipo de protocolo: **ARP**;

(e) solicitação **ARP** ***REQUEST*** e endereço **IP** do veículo atacante: **192.168.1.101**;

(f) presença do valor hexadecimal: ***broadcast*** (**ff:ff:ff:ff:ff:ff)** no campo ***Destination address***, solicitação enviada para todos os veículos da rede.

Estes veículos, dentro do intervalo de tempo estabelecido, injetaram na rede grandes quantidades de quadros MAC por meio de solicitações ARP *REQUEST*. Lembrando que este processo de transmissão foi realizado via *broadcast* (*ff:ff:ff:ff:ff:ff*) e fazendo com que todos os veículos, estando dentro da sua abrangência de rádio, recebam as requisições ARP em curtos intervalos de tempo.

Nesse processo da simulação, ao executar o modelo de ataque abordado, evidentemente gerou um grande desequilíbrio no desempenho da VANET. Os veículos foram forçados a responderem inúmeras solicitações do protocolo ARP *REQUEST*, gerando assim uma densa transmissão incomum de quadros MAC.

5.4 Resultados

Após a conclusão das etapas de simulações, os dados gerados foram analisados e processados para fins de validação, desempenho e eficácia do MDASTI.

Também foi analisada uma outra proposta de mecanismo de segurança (ZAIDI *et al.*, 2016) para fins comparativos. O mecanismo de segurança analisado

apresenta semelhanças em seus processos de detecção e classificação de ataques, e aplica abordagens estatísticas. Zaidi *et al*. (2016) utilizaram o cálculo da média somada com dois desvios-padrão, para verificações de mensagens de emergência entre veículos vizinhos. O modelo estatístico comparado foi adaptado aos processos de simulações, para análise e desempenho entre ambas propostas.

Sendo assim, nesta seção serão apresentados os resultados obtidos e suas devidas interpretações.

5.4.1 Métricas para análise de desempenho e eficiência

Foram aplicadas e consideradas métricas para verificar a eficiência e o desempenho do mecanismo proposto (ALHEETI; GRUEBLER; MCDONALD-MAIER, 2017; BROWNLEE, 2020). Para fins de interpretação destas métricas, na Tabela 6 são descritas suas terminologias.

Tabela 6 – Terminologias das métricas aplicadas

Terminologia	Descrição
Verdadeiro Positivo (VP)	- são eventos em que o SDI classifica corretamente o ataque.
Verdadeiro Negativo (VN)	- são eventos normais em que o SDI os classificou corretamente.
Falso Positivo (FP)	- são eventos normais em que o SDI os classificou incorretamente, considerando-os como ataques ou anormais.
Falso Negativo (FN)	- são eventos de ataques em que o SDI não conseguiu detectá-los corretamente, considerando-os normais.

Fonte: Alheeti; Gruebler; Mcdonald-Maier (2017), Brownlee (2020)

Diante destas terminologias foram aplicadas as seguintes fórmulas conforme equações:

(i) **Taxa de Detecção (TD):** definida pelo total de ocorrências verdadeiras pela proporção do total geral de ocorrências.

$$TxD = \frac{VP + VN}{VP + VN + FP + FN}$$

(ii) **Taxa de Verdadeiro Positivo (TxVP):** definida pelo número de ataques que realmente aconteceram pela proporação do total de ataques detectados.

$$TxVP = \frac{VP}{VP + FN}$$

(iii) **Taxa de Verdadeiro Negativo (TxVN):** definida pelo número total de eventos normais pela proporação do total de eventos considerados normais.

$$TxVN = \frac{VN}{VN + FP}$$

(iv) **Taxa de Falso Positivo (TxFP):** definida pelo número de eventos classificados incorretamente como ataques pela proporação do total de ataques detectados.

$$TxFP = \frac{FP}{FP + VN}$$

(v) **Taxa de Falso Negativo (TxFN)**: definida pelo número de eventos classificados incorretamente como normais pela proporção do total de eventos considerados anômolos.

$$TxFN = \frac{FN}{FN + VP}$$

(vi) **Precisão:** define o quanto o mecanismo detectou de eventos positivos em relação a totalidade da classe positiva. Seu valor tende a diminuir pelo fato do aumento de Falsos Positivos.

$$Precisão = \frac{VP}{VP + FP}$$

(vii) **Recorrência**: resume o quanto a classe positiva foi bem prevista. Seu valor tende a diminuir pelo fato da existência de Falsos Negativos, significando que o mecanismo está com deficiências no processo de detecção de eventos considerados realmente maliciosos.

$$Recorrência = \frac{VP}{VP + FN}$$

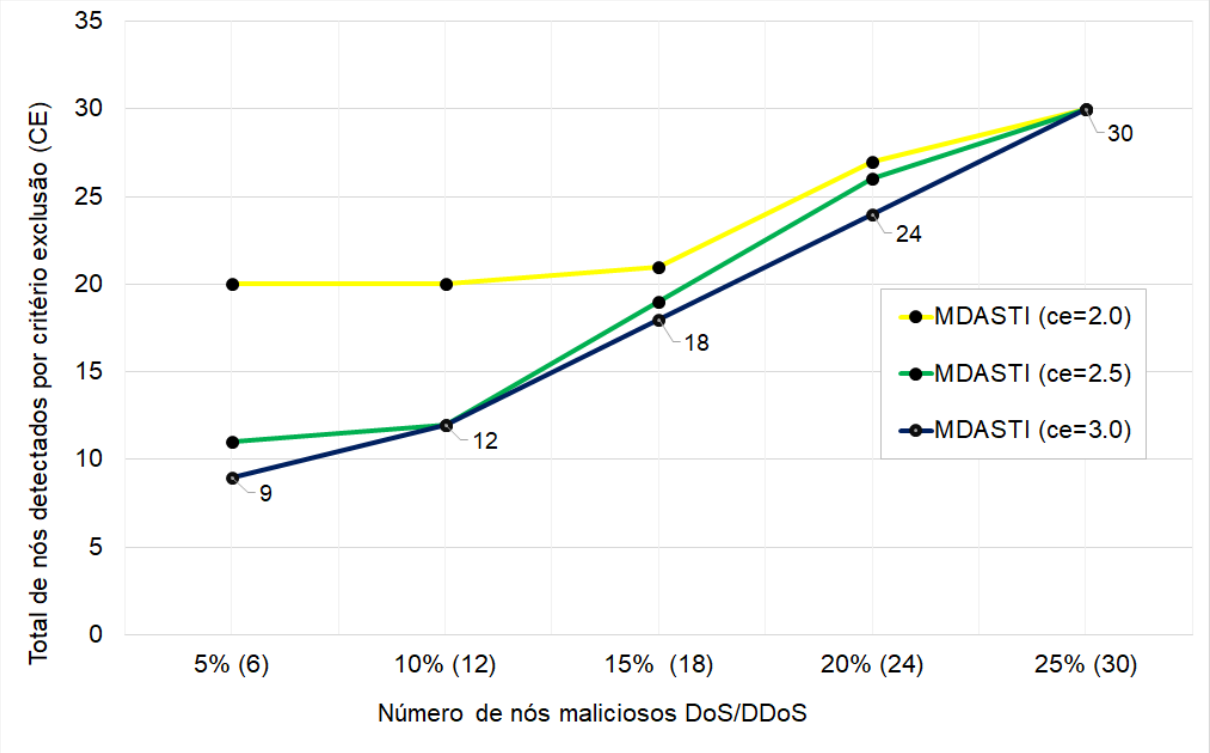
(viii) **Medida-F:** denominada de medida ou pontuação F. É a combinação das taxas de precisão e recorrência resultando em um único valor. Seu resultado deverá estar entre 0 e 1, quanto mais próximo de 1 demonstra que o mecanismo possui um equilíbrio entre estas duas taxas.

$$Medida - F = \frac{(2 * Precisão * Recorrência)}{(Precisão + Recorrência)}$$

5.4.2 Total de detecções pelo critério de exclusão

Nas primeiras etapas de simulações foram executados individualmente cada um dos critérios de exclusão de acordo com cada percentual de veículos maliciosos. No Gráfico 1 são reunidas a relação do total de veículos atacantes detectados para cada critério de exclusão aplicado (2.0, 2.5 e 3.0).

Gráfico 1 - Total de nós (DoS/DDoS) detectados pelos critérios de exclusão



Fonte: Autoria própria - MDASTI

Dentre os três critérios de exclusão simulados, para definir o limiar de rejeição de valores discrepantes, o critério que obteve melhor eficácia foi com o valor 3.0. Considerando-o mais rígido, obteve um melhor desempenho de detecção para cada percentual de veículos DoS/DDoS inseridos na rede. Ele gerou somente três falsos

positivos no primeiro percentual de atacantes, contudo, para os demais percentuais todos foram detectados corretamente.

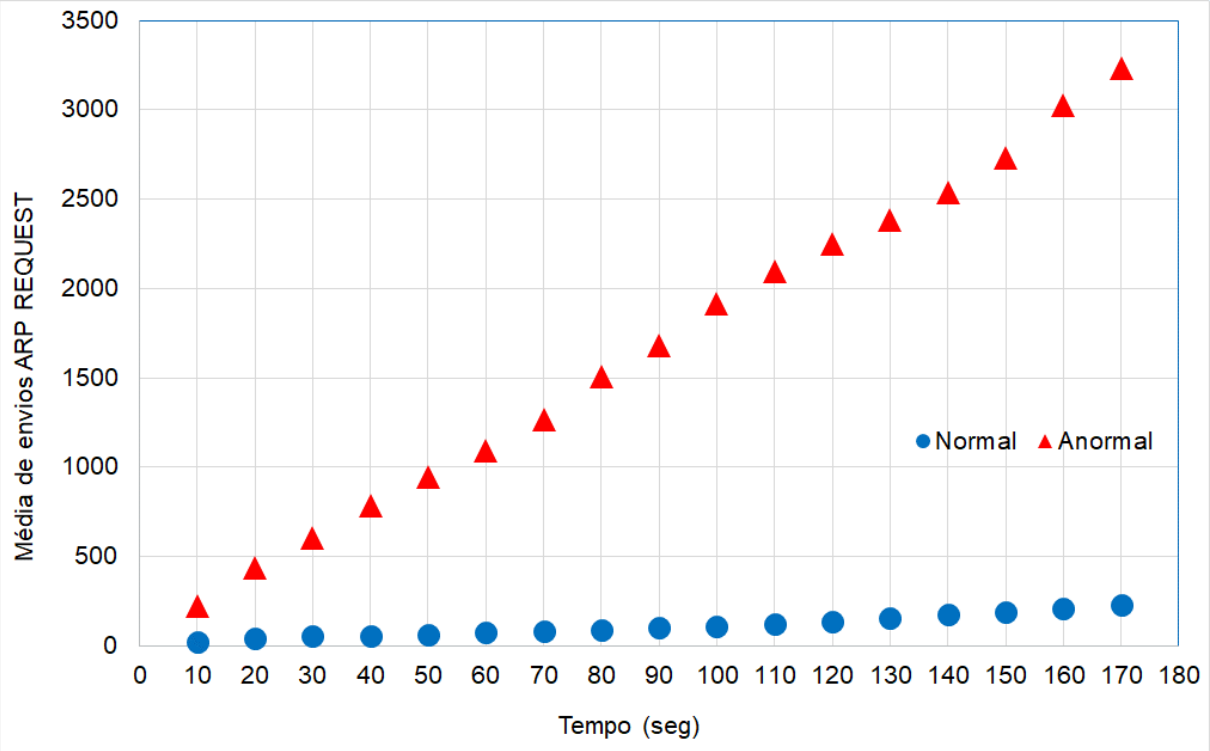
Para o critério 2.0, pouco conservador, realmente ficou provado que sua atuação, considerando este cenário de valores discrepantes, falhou pelo fato de detectar veículos corretamente normais e classificando-os como maliciosos nos percentuais de 5%, 10%, 15% e 20%.

Haja visto que o critério 2.5, considerado moderamente conservador, demonstrou oscilações e gerou falsos-positivos nos percentuais (5%, 15% e 20%). Tais resultados, demonstraram um melhor embasamento norteador entre os critérios de exclusão 2.5 e 3.0, sendo que o último critério obteve melhor eficácia.

5.4.3 Comparação entre os cenários normal e anormal (malicioso)

No Gráfico 2 é demonstrada a real diferença entre o cenário normal, com ausência de DoS/DDoS (veículos maliciosos), com o cenário anormal considerando cerca de 30% de nós maliciosos. Vale ressaltar que os valores apresentados, para ambos cenários, é o valor médio acumulativo das solicitações ARP *REQUEST* em intervalos de 10 segundos.

Gráfico 2 - Média de solicitações ARP *REQUEST* normais e anormais



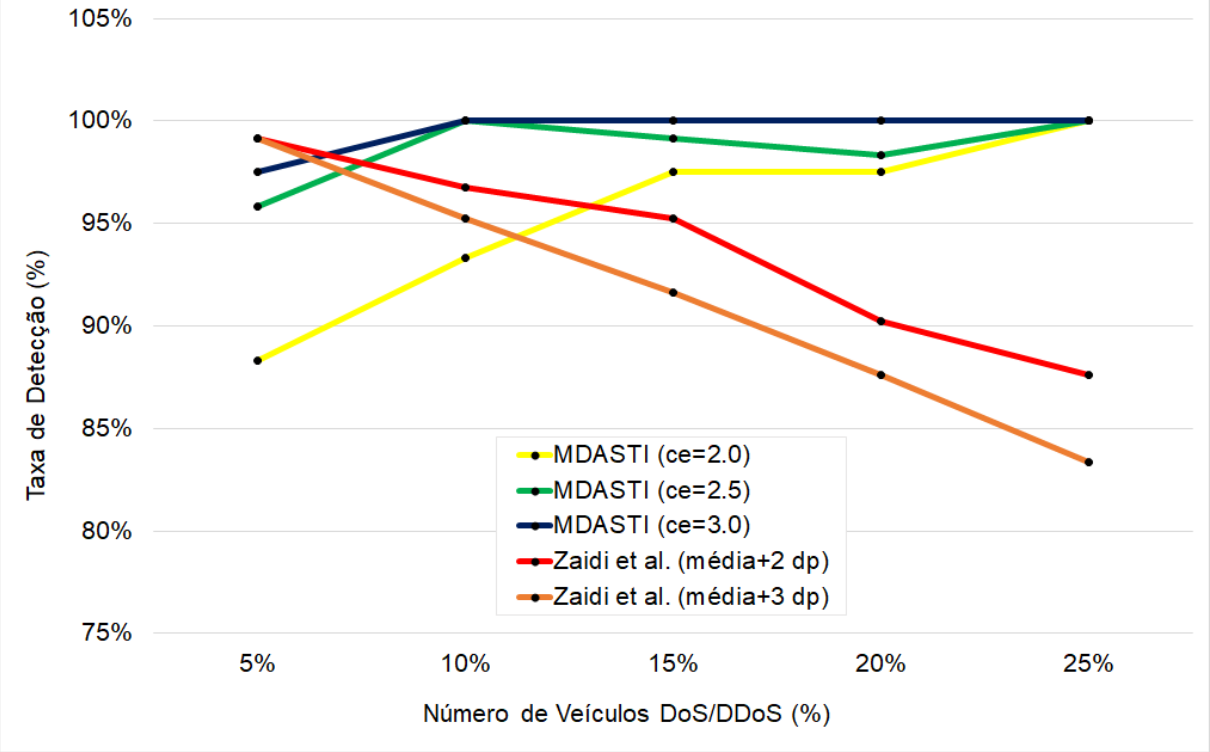
Fonte: Autoria própria - MDASTI

Pode ser visualizada uma grande desigualdade entre os cenários. Sendo que o cenário malicioso obteve o valor médio de *3.234,13* solicitações ARP *REQUEST*, comparado com o cenário normal, que obteve uma faixa média de *231,78* requisições ARP. Haja visto, que a presença de valores discrepantes é muito alta quando é efetuado o ataque de negação de serviço, considerando as características de inundação da rede, tempestade de pacotes, envios de solicitações de desassocições e negação de serviço distribuído.

5.4.4 Desempenhos da taxa de detecção

Por meio desta métrica, é possível analisar o desempenho de detecção das ocorrências que realmente são verdadeiras (positivas e negativas) do mecanismo de segurança. Os percentuais obtidos pelo MDASTI são apresentados no Gráfico 3.

Gráfico 3 - Taxa de Detecção



Fonte: Autoria própria - MDASTI

Evidentemente o MDASTI obteve um melhor desempenho para dois critérios de exclusão (2.5 e 3.0). Observando-se que o método de detecção por anomalia

pelo DAM obteve uma eficácia acima de 85% para todos os critérios e em todas as condições da presença de veículos maliciosos com o ataque de DoS/DDoS. É fato de que com o aumento do número de atacantes, são gerados mais eventos anômolos. Sendo assim, o critério de rejeição 3.0, considerado mais conservador, obteve uma melhor eficácia pela taxa de detecção apresentando entre 95% a 100%. A presença de valores discrepantes não influenciaram a mediana, base estatística aplicada pelo MDASTI. Sendo que a presença de valores extremos poderão influenciar a mediana a paritr de 50% de uma amostra infinita.

Diante de uma concepção inversa do desempenho exercido, por ambos os mecanismos, a proposta de Zaidi *et al*. (2016) utilizou a média somada a dois ou três devios-padrão. Ao aplicar a média somada com desvios padrão, são consideradas as distâncias mínimas e máximas do total de requisições ARP, encontrando uma medida de tendência central. Assim sendo, quando há presença de valores discrepantes o valor médio “estica”, ou seja, a média é influenciada acompanhando a distância exercida pelos discrepantes.

5.4.5 Comparação da taxa de Falso Positivo

Como descrito na subseção 5.4.1, a métrica falso positivo (FP) é utilizada para identificar o número de ocorrências normais classificadas como anormais.

Foram considerados os critérios de rejeição de ambas propostas, sendo estas relacionadas com a variação gradativa dos percentuais de inclusão de veículos maliciosos na VANET.

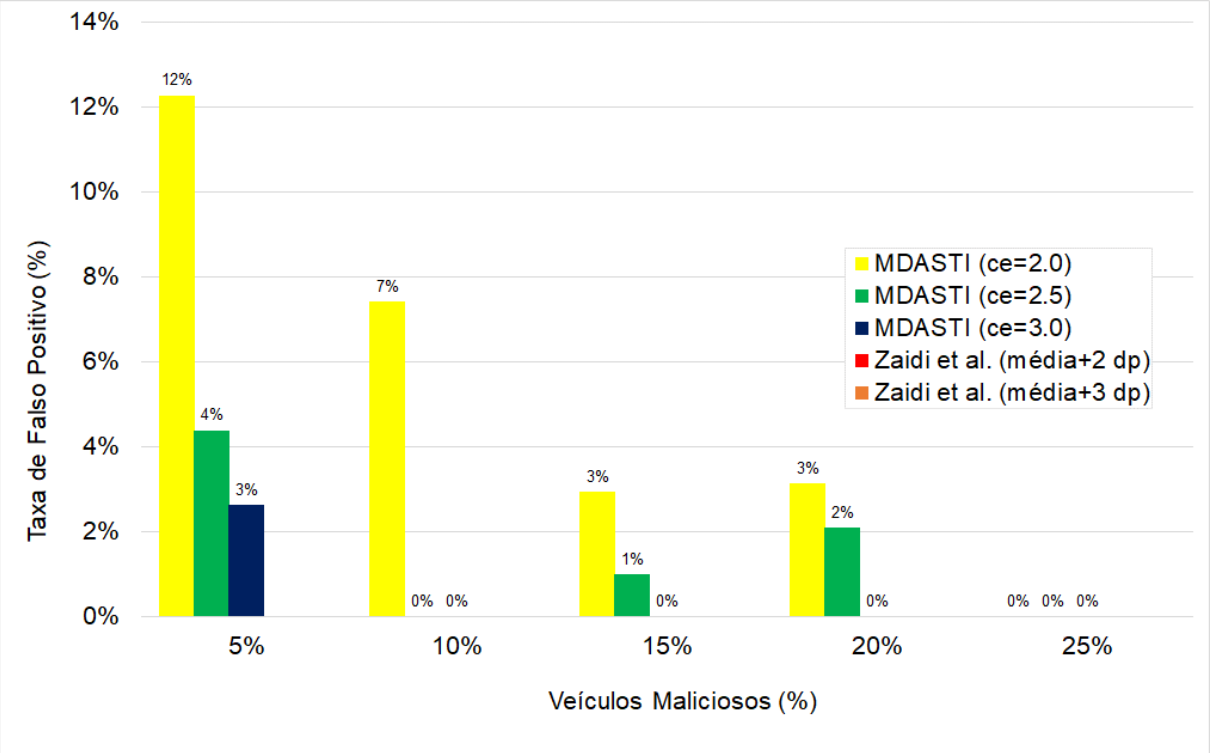
O SDI de Zaid *et al.* (2016) não apresentou nenhum falso positivo, por meio dos seus critérios de rejeição (média somada com dois ou três desvios-padrão), pois abrangeu mais o limiar de rejeição. Isso se deve aos fatores de que sua taxa de falsos-negativos, mais preocupante neste caso, foram elevadas e seu melhor desempenho de detecção foi somente no primeiro cenário com menor número de veículos malicisosos

O MDASTI apresentou possíveis taxas de falsos positivos quando o número de atacantes na rede é menor para os três critérios de exclusão, principalmente ao critério de valor 2.0. Isso se deve ao fator de que uma quantidade parcial de valores discrepantes, gerados entre 5% e 20% de atacantes, não ultrapassaram o limiar de rejeição. Uma melhor abstração é visualizar o conjunto de dados constituídos com

valores parcialmente semelhantes, ou seja, a distância entre os valores da amostra não é tão grande entre si. O melhor desempenho do MDASTI foi apresentado pelo critério 3.0, isso demonstra que o limiar de rejeição ultrapassou uma distância maior para detectar valores discrepantes.

No Gráfico 4, são apresentadas as taxas de falsos positivos obtidas entre o MDASTI e o mecanismo comparado.

Gráfico 4 - Taxas de Falsos Positivos



Fonte: Autoria própria - MDASTI

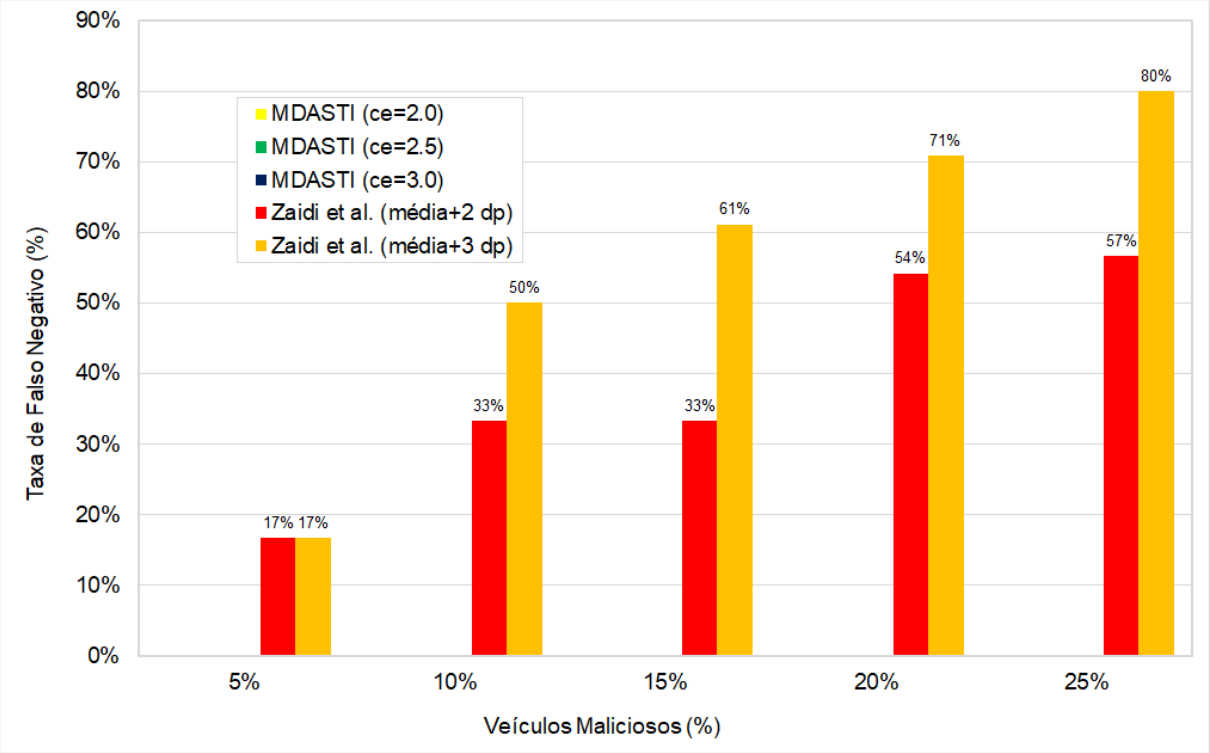
5.4.6 Comparação da taxa de Falso Negativo

A métrica de falso negativo (FN) demonstra um valor importante aos mecanismos de segurança, pois é o número de ocorrências de ataques (verdadeiras) classificadas como normais.

No Gráfico 5 demonstra que Zaidi *et al*. (2016), obteve um baixo rendimento em relação ao detectar eventos que realmente são considerados anomalias. Isso implica em um sério problema ao sistema e/ou veículo a ser protegido.

Em contrapartida o MDASTI não resultou taxas de falsos negativos, devido a sua maior abrangência entre a amostra de dados posterior ao seu limiar de rejeição em todos os critérios aplicados.

Gráfico 5 - Taxas de Falsos Negativos



Fonte: Autoria própria - MDASTI

Não muito exaustiva as devidas justificativas, para ambas comparações, são comprovadas novamente o fato de que a média é distorcida fortemente pela presença e influência de *outliers*. Contudo, o MDASTI quanto maior a presença de valores extremos exerceu um desempenho melhor, realizando a distinção entre a distância de valores normais e anormais (*outliers*). Fator originado pelo cálculo da mediana, por apresentar um ponto de ruptura de 50% de sua amostra de dados infinita.

5.4.7 Taxas de Precisão, Recorrência e Medida-F

As métricas avaliadas pelas taxas de Precisão e Recorrência, estabelecem uma análise do nível de eficácia em que o mecanismo de segurança exerce ao detectar corretamente a classe positiva, entre falso positivo e falso negativo. O

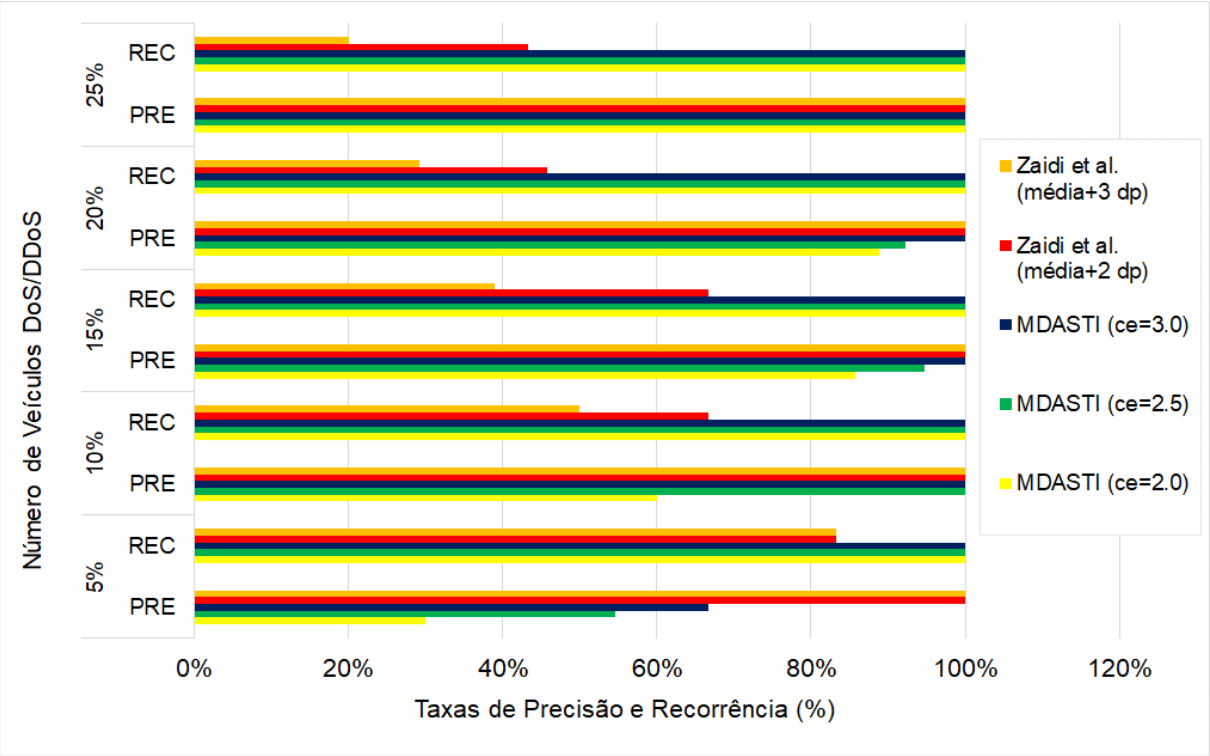
resultado obtido por estas duas taxas são parâmetros de entrada para o cálculo da Medida-F.

A taxa de Recorrência é uma métrica que auxilia na observação do desempenho do mecanismo de segurança em classificar corretamente o número de verdadeiros positivos. Quando seu valor tende a diminuir, evidentemente o algoritmo de detecção está gerando altos índices de falsos negativos. Os valores gerados para os mecanismos MADSTI e Zaidi *et al*. (2016) são dispostos no Gráfico 6.

O mecanismo proposto demontrou para os três critérios de exclusão, quando a incidência de atacantes é menor (5%) que sua precisão obteve um resultado menos eficiente. Isso porque o número de falsos positivos foi maior, conforme o Gráfico 4. Quando aumenta o índice de veículos maliciosos na rede, o critério 2.5 obteve níveis de melhoras em seu desempenho. Porém, mais uma vez o critério 3.0 obteve a melhor eficácia decorrentes das taxas de precisão e recorrência.

O outro SDI por apresentar excelente taxa de precisão, independente da quantidade de atacantes, demonstra gradativamente a sua diminuição na taxa de recorrência conforme o aumento de cenário malicisoso. Isso se deve ao fato dos seus altos números de falsos negativos.

Gráfico 6 - Taxas de Precisão e Recorrência



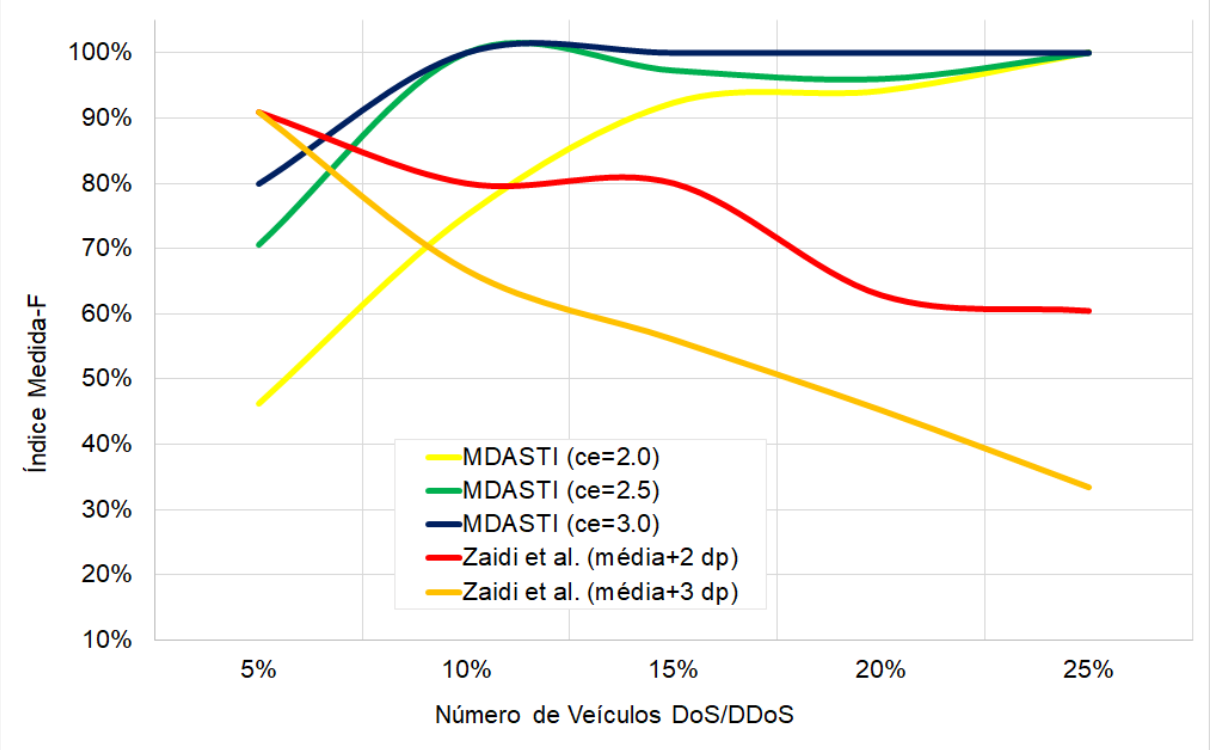
Fonte: Autoria própria – MDASTI

Uma visão abstrata destes resultantes é considerar uma métrica de eficácia total, ou seja, por meio de uma visão abrangente consegue-se visualizar se o mecanismo proposto obteve ou não níveis desejáveis de desempenho.

A Pontuação ou Medida-F é o resultado da proporação entre as taxas de precisão e recorrência, buscado demonstrar o desempenho geral do proposto avaliado. Seu valor deverá estar entre zero e um, quanto mais próximo de 1 demonstra uma ótima eficácia. No Gráfico 7 são apresentados os valores correspondentes da Medida-F.

O mecanismo de segurança comparado obteve, somente no primeiro estágio, com mínimos atacantes, valores da Medida-F satisfatórios. Mas este fator resultante é influenciado pelas suas baixas taxas de falsos positivos. Seu melhor critério de rejeição foi com a média somada com dois desvios-padrão, entre os cenários malicisosos de 5% e 15%. Porém, nos demais cenários não se manteve em condições de bons resultados. Gradativamente sua Pontuação-F demonstrou decaída em virtude de suas altas taxas de falsos negativos, impactando menor desempenho e eficácia.

Gráfico 7 - Índice de desempenho pela Medida-F



Fonte: Autoria própria – MDASTI

Evidentemente o critério 2.0 obteve valores baixos, entre os dois primeiros índices, alcançando um resultado desejável de 94% somente quando atinge o penúltimo índice de atacantes. Já o critério 2.5 novamente demonstrou algumas oscilações, entre os níveis de atacantes, tanto para mais com para menos, gerando uma instabilidade.

O MDASTI apresentou desempenho eficaz, por meio do critério 3.0, em todos os níveis de presença de veículos DoS/DDoS. Foram obtidos os resultados entre 80% e 100% desde o início dos níveis de percentuais de atacantes.

Mediante os resultados obtidos, o MDASTI demonstrou que mesmo obtendo uma Medida-F, inicialmente com 80% na etapa com menos veículos atacantes, não apresentou nenhuma taxa de falso negativo e obteve resultados eficazes e níveis de desempenho satisfatórios.

6 CONCLUSÃO

O ambiente das VANETs e o emergente campo do STI, estão cada vez mais presentes na rotina diária dos percursos urbanos e rodoviários, favorecendo inúmeros benefícios. Entretanto, a segurança de seus elementos é prioritária para que possam exercer suas operações e processos aos meios de transportes de forma segura.

Considerando que diversas ameaças e vulnerabilidades surgem com o aumento de novas tecnologias, a proposta de soluções de segurança justificam e buscam a proteção dos meios envolvidos.

Sendo assim, o mecanismo de segurança desenvolvido por este estudo buscou contribuir com melhorias na segurança dos dispositivos computacionais aplicados ao cenário veicular. Preocupando-se com a proteção da comunicação entre veículos, realizadas por meio da rede ad hoc veicular, buscando o máximo possível a proteção de vidas humanas relacionadas com o ambiente de transportes.

Foi explorado o modelo de ataque de negação de serviço, juntamente com características de inundações e tempestades de pacotes, e negação de serviço distribuída. Considerado um tipo de ataque que pode impactar de forma drástica a comunicação de serviços de socorro, gerenciamento de congestionamento e resgates dentro do âmbito urbano.

O MDASTI foi desenvolvido com base de sua execução em nós individuais e independentes de RSUs. Baseando-se nas limitações e restrições do hardware e software dos veículos, utilizou um modelo estatístico simples, com baixo processamento computacional e executado por meio da técnica de detecção de anomalias. Esta abordagem estatística utilizou o cálculo do desvio absoluto da mediana (DAM), aplicado ao processo de identificação de valores discrepantes (*outliers*), analisando grandes quantidades recebidas de solicitações ARP REQUEST.

Mediante aos processos de simulações, permitiu a validação e análise do MDASTI por meio de métricas aplicadas ao desenvolvimento de sistemas de segurança. Utilizando um cenário de mobilidade urbano realístico e incluindo gradativamente a presença de veículos maliciosos, o MDASTI obteve níveis de eficácia satisfatórios. Valores resultantes, entre 88% e 100%, na taxa de detecção

de ataques, com uma taxa de falso positivo em torno de 3% e não apresentando nenhum percentual resultante da métrica da taxa de falso negativo.

6.1 Dificuldades encontradas

O desenvolvimento e implantações de tecnologias para o ambiente das redes veiculares e STI, diferem-se de soluções propostas e direcionadas para redes de computadores tradicionais. Grande parte do desenvolvimento ainda é realizado por meio de processos e métodos de simulações. Em tempos, ainda carecem de elementos fundamentais e realísticos para procedimentos inerentes ao escopo do desenvolvimento, prototipações, *datasets* específicos e cenários de testes.

Sendo assim, uma das principais dificuldades encontradas foi na execução dos processos e métodos de simulações. Durante a revisão da literatura, também foi investigado quais os softwares e aplicações que são mais utilizados para execuções de simulações da mobilidade veicular e implementação da VANET.

Foram destacadas a aplicação de mapeamento geográfico OpenStreetMap, o simulador SUMO para mobilidade urbana e o NS-3 para todo o desenvolvimento da rede veicular. É importante ressaltar, que todas essas ferramentas são de código aberto, gratuitas e mantidades por comunidades tecnológicas responsáveis e disponibilizando constantes atualizações. Entretanto, foi exigido um período de aprendizagem (entre quatro e cinco meses) para o entendimento e aplicação destes softwares simuladores. Principalmente para o NS-3, que necessita do conhecimento da linguagem de programação C++ e de técnicas de programação orientada a objetos.

Outra complexidade encontrada, inerente ao cenário de ameaças, no simulador NS-3 não há nenhum *dataset* específico para ataques direcionados às VANETs. Os *datasets* existentes são constituídos por ataques, ameaças e vulnerabilidades antigas, e assim dificultando realizar uma análise que possa abranger mais classes atuais de ataques. Diante desta complexidade, optou-se por desenvolver o modelo de ataque de negação de serviço e suas vertentes de exploração, diretamente no NS-3.

Ao gerar ou utilizar cenários realísticos de mobilidade veicular, por meio da aplicação SUMO, considerando a quantidade de nós, operações da VANET e o tempo total de simulação, deve-se atentar ao tempo gasto pela execução de cada

cenário de simulação. Dependendo das características e funcionalidades do cenário, poderá ser exigida uma média de até doze horas para cada simulação.

Todas estas dificuldades e problemas encontrados, foram analisados e buscando solucioná-los dentro do tempo determinado do mestrado e respeitando os conceitos relacionados com a área de estudos da pesquisa.

6.2 Trabalhos futuros

Para continuação futura desta pesquisa, como melhorias, resoluções de lacunas e contribuições, mediante o próprio autor ou por pesquisadores que vierem a se identificar com esta linha de estudo, são sugeridas as etapas:

(i) Integração do MDASTI à uma plataforma distribuída, escalonada e cooperativa, sendo por meio de infraestruturas disponibilizadas por uma VANET *Cloud* ou centrais STI;

(ii) Desenvolver o método de detecção por assinaturas, tornando-se um mecanismo de segurança híbrido;

(iii) Incluir no processo da troca de dados a comunicação com RSUs, possibilitando o compartilhamento de informações, como por exemplo, a transmissão de assinaturas de ataques detectados e conhecidos;

(iv) Explorar outros modelos de ameaças, inerentes ao ambiente de comunicação sem fio veicular, como ataques *sybil*, *blackhole*, *wormhole* e outros;

(v) Aplicar novos modelos de algoritmos para detecção de ameaças, incluindo outras técnicas estatísticas e abordagens de aprendizado de máquina leve. Sendo executados tanto pelo veículo, como também na plataforma de nuvem veicular;

(vi) Aperfeiçoar a lista de reputação, baseando-se em parâmetros legais e respeitando a privacidade, incluindo procedimentos de penalidades e/ou advertências aos veículos considerados maliciosos.

REFERÊNCIAS

AGGARWAL, C. C. **Outlier Analysis**. Segunda edição. Cham: Springer, 2017. p.1, 399-416. DOI: 10.1007/978-3-319-47578-3.

ALAM, M.; FERREIRA, J.; FONSECA, J. **Intelligent transportation systems**: dependable vehicular communications for improved road safety. Cham: Springer, 2016.

ALHEETI, K. M., GRUEBLER, A.; MCDONALD-MAIER, K. **Using discriminant analysis to detect intrusions in external communication for self-driving vehicles**. Digital Communications and Networks. Elsevier: Chongqing, vol. 3, mar. 2017, p. 180-187. DOI: https://doi.org/10.1016/j.dcan.2017.03.001. Disponível em: http://www.sciencedirect.com/science/article/pii/S2352864817300913. Acesso em: 14 mar. 2019.

ALOQAILY, M.; OTOUM,S.; RIDHAWI, I. A.; JARARWEH,Y. **An intrusion detection system for connected vehicles in smart cities**. Ad Hoc Networks, Elsevier, Amsterdã, v. 90, n. 101842, ISSN: 1570-8705, jul. 2019. DOI: https://doi.org/10.1016/j.adhoc.2019.02.001. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1570870519301131. Acesso em: 01 maio 2019.

AN, S.; LEE, B.; SHIN, D. **A Survey of Intelligent Transportation System.** *In:* Third International Conference on Computational Intelligence, Communication Systems and Networks, 3, 2011, Bali. Anais […]. Bali**:** IEEE, 2011, p. 332-337. DOI: 10.1109/CICSyN.2011.76. Disponível em: https://ieeexplore.ieee.org/document/6005695. Acesso em: 19 mar. 2019.

ARSHAD, M.; ULLAH, Z.; AHMAD, N.; KHALID, M.; CRIUCKSHANK, H.; CAO, Y. **A survey of local/cooperative-based malicious information detection techniques in VANETs**. EURASIP Journal on Wireless Communications and Networking, Nova York: Springer Nature, n. 62 p. [*s. l.*], mar. 2018. DOI: https://doi.org/10.1186/s13638-018-1064-y. Disponível em: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-018-1064-y. Acesso em: 01 maio 2019.

BECHLER, M.; JAAP, S.; WOLF, L. **An optimized TCP for internet access of vehicular Ad Hoc Networks**. *In:* 4th International IFIP-TC6 Networking Conference, Waterloo, Canada, May 2-6, 2005, Proceedings. Berlin: Springer, 2005, Lecture Notes in Computer Science 3462, ISBN: 3-540-25809-4, p. 869-880. DOI: https://doi.org/10.1007/11422778_70. Disponível em: https://link.springer.com/chapter/10.1007/11422778_70. Acesso em: 20 abr. 2019.

BÍBLIBIA. Português. Livro de Filipenses. *In:* **Bíblia - Mensagem de Deus**. Tradução de LEB – Edições Loyola. nro. 4. São Paulo: Edições Loyola, 1989., Cap. 2, vr. 6-11, p. 1147.

BOUKERCHE, A.; GRANDE, R. E. D. **Vehicular cloud computing: Architectures, applications, and mobility**. **Computer Networks**, Elsevier, Amsterdã, v. 135, p. 171-189, abr. 2018. DOI: https://doi.org/10.1016/j.comnet.2018.01.004. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1389128618300057. Acesso em: 15 fev. 2019.

BRANCO, K. C.; TEIXEIRA, M. M.; GURGEL, P. H. M. **Redes de computadores: da teoria à prática com Netkit**. Rio de Janeiro: Elsevier, 2015. p. 40-41; 147-148; 163-166.

BROWNLEE, J. **Tour of Evaluation Metrics for Imbalanced Classification**. Vermont Victoria, jan. 2020. Disponível em: https://machinelearningmastery.com/tour-of-evaluation-metrics-for-imbalanced-classification/. Acesso em: 05 fev. 2020.

BRUNI, A. L. **Estatística Aplicada à Gestão Empresarial**. 4. ed. São Paulo: Atlas, 2013.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). **Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2019.** Disponível em: https://cert.br/stats/incidentes/2019-jan-dec/tipos-ataque.html. Acesso em: 05 fev. 2020.

CUNHA, F.; VILLAS, L.; BOUKERCHE , A.; MAIA, G.; VIANNA, A.; MINI, R. A. F.; LOUREIRO, A. A. F. Data communication in VANETs: protocols, applications and challenges. Ad Hoc Networks, Amesterdã, v. 44, p. 90-103, 2016. DOI: https://doi.org/10.1016/j.adhoc.2016.02.017. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1570870516300580. Acesso em: 30 jan. 2019.

DEWANJEE, R.; VYAS, R. **A Studyon IDS (IntrusionDetection System) andIntroductionof IFS (IntrusionFiltration System)**. Springer Nature, Singapore PteLtd., 2017, Computingand Network Sustainability, jul., 2017, p119-126. Lecture Notes in Networks and Systems, v. 12. DOI: https://doi.org/10.1007/978-981-10-3935-5_13. Disponível em: https://link.springer.com/chapter/10.1007/978-981-10-3935-5_13. Acesso: 30 mar. 2019.

DICIONÁRIO MICHAELIS. **AD HOC**. *In*: MICHAELIS dicionário brasileiro da Língua Portuguesa. São Paulo: Melhoramentos, 2020. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/ad%20hoc/. Acesso em: 24 abr. 2020.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE**. Automotive intelligent transport systems (ITS)**. Valbone, 2019. Disponível em: https://www.etsi.org/technologies/automotive-intelligent-transport. Acesso em: 22 abr. 2019.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **Draft ETSI EN 302 571 - V2.1.1: Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU**. Valbone, fev. 2017. Disponível em: https://www.etsi.org/deliver/etsi_en/302500_302599/302571/02.01.01_60/en_302571v020101p.pdf. Acesso em: 22 nov. 2019.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **Draft ETSI EN 302 663 – V1.3.1: Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band**. Valbone, jan. 2020. Disponível em: https://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.03.01_60/en_302663v010301p.pdf. Acesso em: 05 fev. 2020.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **Draft ETSI EN 302 637-3 – V1.3.1: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service**. Valbone, abr. 2019. Disponível em: https://www.etsi.org/deliver/etsi_en/302600_302699/30263703/01.03.01_60/en_30263703v010301p.pdf. Acesso em: 22 nov. 2019.

FERRAZ, F. S.; FERRAZ, C. A. G. **Smart city security issues**: Depicting Information Security Issues in the Role of a Urban Environment. IEEE/ACM 7th International Conference on Utility and Cloud Computing, London, p. 842-847, dez. 2014. DOI: https://doi.org/10.1109/UCC.2014.137. Disponível em: https://ieeexplore.ieee.org/document/7027604. Acesso em: 19 mar. 2019.

G1 RIO. Mulher morre após casal entrar por engano em comunidade em Niterói. **G1**. Rio de Janeiro, 04 out. 2015. Disponível em: http://g1.globo.com/rio-de-janeiro/noticia/2015/10/mulher-morre-apos-entrar-por-engano-em-comunidade-em-niteroi-rj.html. Acesso em: 04 abr. 2018.

GREENBERG, A. Hackers remotely kill a jeep on the highway - with me in it. [Entrevistados] Charlie Miller e Chris Valasek. **Wired.** Boone, IA, 21 jul. 2015. Disponível em: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Acesso em: 30 abr. 2019.

HASROUNY, H.; SAMHAT, A. E.; BASSIL, C.; LAOUITI, A. **VANet security challenges and solutions: A survey**. **Vehicular Communications**, Elsevier, Amsterdã, v. 7, p. 7-20, jan. 2017. DOI: https://doi.org/10.1016/j.vehcom.2017.01.002. Disponível em: https://www.sciencedirect.com/science/article/pii/S2214209616301231. Acesso em: 10 jan. 2019.

HE, W.; YAN, G.; XU, L. D. **Developing Vehicular Data Cloud Services in the IoT Environment.** *In:* IEEE Transactions on Industrial Informatics, Canada, vol. 10, n. 2, p. 1587-1595, maio 2014. DOI: doi: 10.1109/TII.2014.2299233. Disponível em: https://ieeexplore.ieee.org/abstract/document/6709775. Acesso em: 20 mar. 2019.

HUSSAIN, R.; REZAEIFAR, Z.; OH, H. A paradigm shift from vehicular ad hoc networks to vanet-based clouds. **Wireless Personal Communications**. **An International Journal**, Nova York, v. 83, n. 2, p. 1131-1158, jul. 2015. Disponível em: https://link.springer.com/article/10.1007/s11277-015-2442-y. Acesso em: 24 abr. 2019.

IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture. *In:* **IEEE Std 802-2014** (Revision to IEEE Std 802-2001), p.1-74, 30 jun. 2014. DOI: 10.1109/IEEESTD.2014.6847097. Disponível em: https://ieeexplore.ieee.org/document/6847097. Acesso em: 18 jan. 2020.

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. *In:* **IEEE Std 802.11-2016** (Revision of IEEE Std 802.11-2012), p. 1-3534, 14 dez. 2016. DOI: https://doi.org/10.1109/IEEESTD.2016.7786995. Disponível em: https://ieeexplore.ieee.org/document/7786995. Acesso em: 22 abr. 2019.

IEEE Guide for Wireless Access in Vehicular Environments (WAVE) – Architecture. *In:* **IEEE Std 1609.0-2019** (*Revision of IEEE Std 1609.0-2013)*, p. 1-106, 10 abr. 2019. DOI: 10.1109/IEEESTD.2019.8686445. Disponível em: https://ieeexplore.ieee.org/document/8686445. Acesso em: 25 dez. 2019.

IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages. *In:* **IEEE Std 1609.2-2016** (Revision of IEEE Std 1609.2-2013), p. 1-240, 1 mar. 2016. DOI: 10.1109/IEEESTD.2016.7426684. Disponível em: https://ieeexplore.ieee.org/document/7426684. Acesso em: 25 dez. 2019.

IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages - Amendment 1. *In:* **IEEE Std 1609.2a-2017** (Amendment to IEEE Std 1609.2-2016),p.1-123, 23 nov. 2017. DOI: 10.1109/IEEESTD.2017.8065169. Disponível em: https://ieeexplore.ieee.org/document/8065169. Acesso em: 25 dez. 2019.

IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages - Amendment 2--PDU Functional Types and Encryption Key Management. *In:* **IEEE Std 1609.2b-2019** (Amendment to IEEE Std 1609.2-2016), p.1-30, 14 jun. 2019. DOI: 10.1109/IEEESTD.2019.8734860. Disponível em: https://ieeexplore.ieee.org/document/8734860. Acesso em: 25 dez. 2019.

IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services. *In*: **IEEE Std 1609.3-2016** (Revision of IEEE Std 1609.3-2010),p.1-160, 29 abr. 2016. DOI: 10.1109/IEEESTD.2016.7458115. Disponível em: https://ieeexplore.ieee.org/document/7458115. Acesso em: 25. dez. 2019.

IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation. *In:* **IEEE Std 1609.4-2016** (Revision of IEEE Std 1609.4-2010), p.1-94, 21 mar. 2016. DOI: 10.1109/IEEESTD.2016.7435228. Disponível em: https://ieeexplore.ieee.org/document/7435228. Acesso em: 25 dez. 2019.

IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS). *In:* **IEEE Std 1609.11-2010**, p.1-62, 9 jan. 2011. DOI: 10.1109/IEEESTD.2011.5692959. Disponível em: https://ieeexplore.ieee.org/document/5692959. Acesso em: 25 dez. 2019.

IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Identifiers. *In:* **IEEE Std 1609.12-2019** (Revision of IEEE Std 1609.12-2016),p. 1-17, 22 out. 2019. DOI: 10.1109/IEEESTD.2019.8877516. Disponível em: https://ieeexplore.ieee.org/document/8877516. Acesso em: 25. dez.2019.

INTERNATIONAL ORGANIZATION OF MOTOR VEHICLE MANUFACTURES (OICA). **World vehicles in use - all vehicles**. Paris, 2015. Disponível em: http://www.oica.net/wp-content/uploads//Total_in-use-All-Vehicles.pdf. Acesso em: 04 abr. 2019.

INTERNET ENGINEERING TASK FORCE (IETF). Internet Security Glossary, Version 2. **RFC 4949: informativo**, 2007. Disponível em: https://tools.ietf.org/html/rfc4949. Acesso em: 10 fev. 2019.

ITS Canada. **Architecture for Canada. Mississauga**, 2019. Disponível em: https://www.itscanada.ca/index.html. Acesso em: 22 abr. 2019.

KDD Cup 1999 Data. Conjunto de dados KDD-99. *In:* **The UCI KDD Archive Information and Computer ScienceUniversity of California**, Irvine, out. 1999. Disponível em: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. Acesso em: 20 fev. 2019.

KENNEY, J. B. **Dedicated Short-Range communications (DSRC) standards in the United States**. *In: Proceedings of the IEEE*, v. 99, n. 7, p. 1162-1182, july 2011, Washington. DOI: 10.1109/JPROC.2011.2132790. Disponível em: https://ieeexplore.ieee.org/document/5888501. Acesso em: 22 abr. 2019.

KIM, H. K.; HAN, M. L.; KWAK, B. I. **Anomaly intrusion detection method for vehicular networks based on survival analysis**. Vehicular Communications, Elsevier, Amsterdã, v. 14, p. 52-63, out. 2018. DOI: https://doi.org/10.1016/j.vehcom.2018.09.004. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S2214209618301189. Acesso

em: 18 jan. 2019.

KUMAR, S.; DUTTA, K. **Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges**. Security and Communication Networks. Security Comm. Networks, Wiley Online Library, EUA, v. 9, p. 2484-2556, set. 2016. DOI: https://doi.org/10.1002/sec.1484. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1484. Acesso em: 15 jun. 2019.

LEE, H.; JEONG, S. H.; KIM, H. K. **OTIDS: A Novel IntrusionDetection System for In-vehicle Network byUsing Remote Frame**. *In:* 2017 15th Annual Conferenceon Privacy, Security and Trust (PST), Calgary, AB, Canada, pp. 57-5709, ago. 2017. DOI: doi: 10.1109/PST.2017.00017. Disponível em: https://ieeexplore.ieee.org/abstract/document/8476919. Acesso em: 19 fev. 2019.

LEYS, C.; LEY, C.; KLEIN, O.; BERNARD, P.; LICATA, L. **Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median**. Jornal of Experimental Social Psychology, Elsevier, EUA, v. 49, p. 764-766, jul. 2013. DOI: https://doi.org/10.1016/j.jesp.2013.03.013. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0022103113000668?via%3Dihub. Acesso em: 05 fev. 2020.

LOPEZ, P. A.; BEHRISCH, M.; BIEKER-WALZ, L.; ERDMANN, J; FLÖTTERÖD, Y.; HILBRICH, R.; LÜCKEN, L.; RUMMEL, J.; WAGNER, P.; WIEßNER, E. **Microscopic Traffic Simulation using SUMO**. IEEE Intelligent Transportation Systems Conference (ITSC), Maui, HI, p. 2575-2582, nov. 2018. DOI: 10.1109/ITSC.2018.8569938. Acesso em: 01 jul. 2019.

LOUKAS, G.; YOON, Y.; SAKELLARI, G.; VUONG, T.; HEARTFIELD, R. **Computation offloading of a vehicle's continuous intrusion detection workload for energy efficiency and performance**. Simulation Modelling Practice and Theory, Amsterdã, v. 73, p. 83-94, abr. 2017. DOI: https://doi.org/10.1016/j.simpat.2016.08.005. Disponível em: https://www.sciencedirect.com/science/article/pii/S1569190X16302234. Acessoem: 20 fev. 2019.

LOUKAS, G.; KARAPISTOLI, E.; PANAOUSIS, E.; SARIGIANNIDIS, P.; BEZEMSKIJ, A.; VUONG, T. **A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles**. Ad Hoc Networks, Elsevier, Amsterdã, v. 84, p. 124-147, mar. 2019. DOI: https://doi.org/10.1016/j.adhoc.2018.10.002. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1570870518307091. Acesso em: 10 jan. 2019.

LYAMIN, N.; VINEL, A.; JONSSON, M.; LOO, J. **Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks**. IEEE Communications Letters, Paris, vl.18, n.1, jan. 2014. DOI: 10.1109/LCOMM.2013.102213.132056. Disponível em: https://ieeexplore.ieee.org/document/6646505. Acesso em: 15 mar. 2019.

MENEGUETTE, R. I.; GRANDE, R. E. D.; LOUREIRO, A. A. F. **Intelligent transport system in smart cities**: aspects and challenges of vehicular networks and cloud. Cham: Springer, 2018.

MILLER, C.; VALASEK, C. **Remote exploitation of an unaltered passanger vehicle**. *In*: Proc. Blackhat USA, 18, ago. 2015, Las Vegas. Apresentação oral. Disponível em: https://www.blackhat.com/us-15/briefings.html#remote-exploitation-of-an-unaltered-passenger-vehicle. Acesso em: 04 abr. 2018.

MORENO, D. **Pentest em redes sem fio**. São Paulo: Novatec, 2016. p.156,178.

MORENO, D. **PYTHON para Pentest**. São Paulo: Novatec, 2018.

MURUTI, G.; RAHIM, F. A.; IBRAHIM, Z. BIN. **A Survey on Anomalies Detection Techniques and Measurement Methods.** IEEE Conference on Application, Information and Network Security (AINS), Langkawi: Malaysia, 2018, p. 81-86, DOI: 10.1109/AINS.2018.8631436. Disponível em: https://ieeexplore.ieee.org/document/8631436. Acesso em: 15 mar. 2020.

NS-3. **Network Simulator**. Versão 3.30. [*S. l.*]. NSNAM. 2019. Disponível em: https://www.nsnam.org/. Acesso em: 01 set. 2019.

NSL-KDD dataset. **Canadian Institute for Cybersecurity**. University of New Brunswick, Canada, 2009. Disponível em: https://www.unb.ca/cic/datasets/nsl.html. Acesso em: 20 fev. 2019.

Open Web Application Security Project (OWASP). **OWASP API Security Project, 2019**. Disponível em: https://owasp.org/www-project-api-security/. Acesso em: 05 fev. 2020.

ORGANIZAÇÃO MUNDIAL DE SAÚDE (OMS). **Top 10 global causes of deaths, 2016**. Disponível em: https://www.who.int/en/news-room/fact-sheets/detail/the-top-10-causes-of-death. Acesso em: 04 abr. 2019.

OSM. OpenStreetMap. 2019a. Disponível em: https://www.openstreetmap.org/copyright. Acesso em: 1 set. 2019.

OSM. OpenStreetMap. Mapa geográfico urbano cidade de São Paulo, Brasil. 2019b. Disponível em: https://www.openstreetmap.org/export#map=17/-23.61365/-46.69595&layers=N. Acesso em: 08 dez. 2019.

PILLI, E. S.; MISHRA, P.; VARADHARAJAN, V.; TUPAKULA, U. **Intrusion detection techniques in cloud environment: A survey**. Journal of Network and Computer Applications,Elsevier, Amsterdã, v. 77, p. 18-47, jan. 2017. DOI: https://doi.org/10.1016/j.jnca.2016.10.015. Disponível em: https://www.sciencedirect.com/science/article/pii/S1084804516302417. Acesso em:

14 mar. 2019.

SAKIZ, F.; SEN, S. **A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV**. Ad Hoc Networks, Elsevier, Amsterdã, v. 61, p. 33-50, jun. 2017. DOI: https://doi.org/10.1016/j.adhoc.2017.03.006. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1570870517300562. Acesso em: 10 jan. 2019.

SANDERS, C.; SMITH, J. **Applied Network Security Monitoring.** Collection, Detection, and Analysis. Massachusetts: Elsevier, 2014. p. 5

SANDERS, C. **Análise de Pacotes na Prática**. Usando Wireshark para solucionar problemas de rede do mundo real. São Paulo: Novatec, 2017.

SANTOS, L. F. S.; BARCELOS, L. B. D. Exames em detecção de intrusão. *In*: VELHO, J. A. (Org.). **Tratado de computação forense**. Campinas: Millennium, 2016. p. 375-381.

SCHMITZ, R.; LEIGGENER, A.; FESTAG, A.; EGGERT, L.; EFFELSBERG, W. **Analysis of Path Characteristics and Transport Protocol Design in Vehicular**. Ad Hoc Networks, *2006 IEEE 63rd Vehicular Technology Conference*, Melbourne, Vic., 2006, p. 528-532, maio 2006. DOI: 10.1109/VETECS.2006.1682880. Disponível em: https://ieeexplore.ieee.org/abstract/document/1682880. Acesso em: 20 abr. 2019.

SEITZ, J. **Black Hat Python**. Programação Python para hackers e pentesters. São Paulo: Novatec, 2015.

SHARMA, S.; KAUL, A. **A survey on intrusion detection systems and honeypot based proactive security mechanisms in vanets and vanet cloud**. Vehicular Communications, Elsevier, Amsterdã, v.12, abr. 2018, p. 138-164. DOI: https://doi.org/10.1016/j.vehcom.2018.04.005. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S2214209617302784?via%3Dihub. Acesso em: 10 jan. 2019.

SINDICATO NACIONAL DA INDÚSTRIA DE COMPONENTES PARA VEÍCULOS AUTOMOTORES - SINDIPEÇAS. **Relatório da Frota Circulante Nacional**. São Paulo, 2020. Disponível em: https://www.sindipecas.org.br/sindinews/Economia/2020/RelatorioFrotaCirculante_Abril_2020.pdf. Acesso em: 01 jun. 2020.

SO, S.; PETIT, J.; STAROBINSKI, D. **Physical layer plausibility checks for misbehavior detection in V2X networks**. WiSec '19, 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Miami Flórida, maio 2019, p. 84–93. DOI: https://dl.acm.org/doi/10.1145/3317549.3323406. Disponível em: https://dl.acm.org/doi/pdf/10.1145/3317549.3323406. Acesso em: 01 jun. 2019.

STALLINGS, W.; BROWN, L. Software Malicioso. *In:* STALLINGS, W.; BROWN, L. **SEGURANÇA DE COMPUTADORES**. **PRINCÍPIOS E PRÁTICAS.** 2. ed. Rio de Janeiro: Elsevier, 2014. Capítulo 6.

STALLINGS, W.; BROWN, L. Ataques de negação de serviço. *In:* STALLINGS, W.; BROWN, L. **SEGURANÇA DE COMPUTADORES**. **PRINCÍPIOS E PRÁTICAS.** 2. ed. Rio de Janeiro: Elsevier, 2014. Capítulo 7.

STALLINGS, W.; CASE, T. **Redes e sistemas de comunicação de dados**. 7. ed. Rio de Janeiro: Elsevier, 2016. p. 407-409.

STATISTA. **Connected Cars – Statistics & Facts**. Nova York: Statista Ltd., 6 abr. 2020a. Disponível em: https://www.statista.com/topics/1918/connected-cars/#dossierSummary__chapter1. Acesso em: 01 jun. 2020.

STATISTA. **Shipments of embedded OEM telematics systems worldwide between 2019 and 2023**. Nova York: Statista Ltd., 6 abr. 2020b. Disponível em: https://www.statista.com/statistics/252370/connected-car-system-shipments-worldwide/. Acesso em: 01 jun. 2020.

SUMO. **Simulation of Urban Mobility**. Versão 1.5.0. [*S. l.*]. German Aerospace Center (DLR) and others. 2020. Disponível em: https://sumo.dlr.de/docs/index.html. Acesso em: 19 fev. 2020.

UNITED STATES DEPARTMENT OF TRANSPORTATION. **Architecture reference for cooperative and intelligent transportation**: ARC-IT 8.2. Washington, 29 jan. 2019. Disponível em: https://local.iteris.com/arc-it/. Acesso em: 22 abr. 2019.

UNITED STATES DEPARTMENT OF TRANSPORTATION. **Intelligent transportation systems joint program office**. Washington, 17 jun. 2016. Disponível em: https://www.its.dot.gov/index.htm. Acesso em: 22 abr. 2019.

VEJA. **Carro é metralhado em Niterói e passageira morre**. Veja, São Paulo, 04 out. 2015. Disponível em: https://veja.abril.com.br/brasil/carro-e-metralhado-em-niteroi-e-passageira-morre/. Acesso em: 04 abr. 2018.

VICS. **Vehicle Informationand Communication System Center**. Tokyo, 2018. Disponível em: https://www.vics.or.jp/en/. Acesso em: 22 abr. 2019.

Wireshark. **Wireshark Network Protocol Analyzer.** Versão 3.2.4. [S. *l*.]: Wireshark GNU GPL. 2020. Disponível em: https://www.wireshark.org/. Acesso em: 18 jan. 2020.

ZAIDI, K.; MILOJEVIC, M. B.; RAKOCEVIC, V.; NALLANATHAN, A.; RAJARAJAN, M. Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection. **IEEE Transactions on Vehicular Technology**, Sendai, v. 65, n. 8, ago. 2016, p. 6703-6714. DOI: 10.1109/TVT.2015.2480244. Disponível em: https://ieeexplore.ieee.org/abstract/document/7272127. Acesso em: 11 nov. 2018.