UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS FLORIANÓPOLIS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE AUTOMAÇÃO E SISTEMAS

Claudio Piccolo Fernandes

UM SISTEMA DE GERENCIAMENTO DE CONFIANÇA DESCENTRALIZADO PARA VANETs BASEADO EM MECANISMO DE REPUTAÇÃO E BLOCKCHAIN

Florianópolis
2022

Claudio Piccolo Fernandes

UM SISTEMA DE GERENCIAMENTO DE CONFIANÇA DESCENTRALIZADO PARA VANETs BASEADO EM MECANISMO DE REPUTAÇÃO E BLOCKCHAIN

Tese submetida ao Programa de Pós-Graduação em Engenharia de Automação e Sistemas da Universidade Federal de Santa Catarina para a obtenção do título de Doutor em Engenharia de Automação e Sistemas.
Orientador: Prof. Carlos Barros Montez, Dr.
Coorientadora: Profa. Michelle S. Wangham, Dra.

Florianópolis
2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Fernandes, Claudio Piccolo
Um sistema de gerenciamento de confiança descentralizado para VANETs baseado em mecanismo de reputação e blockchain / Claudio Piccolo Fernandes ; orientador, Carlos Barros Montez, coorientadora, Michelle Silva Wangham, 2022.
117 p.

Tese (doutorado) - Universidade Federal de Santa Catarina, Centro Tecnológico, Programa de Pós-Graduação em Engenharia de Automação e Sistemas, Florianópolis, 2022.

Inclui referências.

1. Engenharia de Automação e Sistemas. I. Montez, Carlos Barros. II. Wangham, Michelle Silva. III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Engenharia de Automação e Sistemas. IV. Título.

Claudio Piccolo Fernandes

UM SISTEMA DE GERENCIAMENTO DE CONFIANÇA DESCENTRALIZADO PARA VANETs BASEADO EM MECANISMO DE REPUTAÇÃO E BLOCKCHAIN

O presente trabalho em nível de doutorado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Carlos Barros Montez, Dr.
Universidade Federal de Santa Catarina

Prof. Miguel Elias Mitre Campista, Dr.
Universidade Federal do Rio de Janeiro

Prof. Alysson Neves Bessani, Dr.
Universidade de Lisboa

Prof. Aldri Luiz dos Santos, Dr.
Universidade Federal de Minas Gerais

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de Doutor em Engenharia de Automação e Sistemas.

ICP-Edu
Documento assinado digitalmente
Julio Elias Normey Rico
Data: 25/11/2022 20:35:19-0300
CPF: ***.840.859-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Julio Elias Normey Rico, Dr.
Coordenador do Programa

ICP-Edu
Documento assinado digitalmente
Carlos Barros Montez
Data: 25/11/2022 18:31:18-0300
CPF: ***.035.027-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Carlos Barros Montez, Dr.
Orientador

Florianópolis, 2022.

Aos meus pais.

AGRADECIMENTOS

Em primeiro lugar agradeço ao meu grande pai (*in memoriam*), o qual dizia que a educação é a única e verdadeira herança que os pais podem deixar a seus filhos, e não mediu esforços para isso. Agradeço também pelos valores que minha mãe ensinou, que levarei comigo para o resto da vida. Ao meu brother, não só por dividirmos a mesma família, mas pela grande pessoa que é.

A Roberta pelo carinho, compreensão, força e incentivo.

Agradecimento especial ao meu amigo, Daniel Adriano, que se dispôs sempre a ajudar nos problemas das implementações quando solicitado, pois, sua preciosa ajuda foi de grande valia na conclusão desta pesquisa.

Agradeço ao meu orientador, professor Carlos Barros Montez, e minha coorientadora, professora Michelle Silva Wangham, por acreditarem no meu potencial, pela paciência, oportunidade e por confiarem neste trabalho e a ajuda durante todo o processo de desenvolvimento.

Por fim, quero agradecer a todos que de uma forma ou de outra contribuíram para a realização deste trabalho.

“Trabalhe duro e em silêncio.
Deixe que o seu sucesso faça barulho”
(Dale Carnegie)

RESUMO

As aplicações de redes veiculares tornaram-se essenciais ao fornecer aos motoristas serviços que permitam alertas e instruções de segurança para garantir uma condução com conforto e segura. Apesar de oferecer novas oportunidades, o uso dessas redes suscita várias preocupações relacionadas à segurança, incluindo a necessidade de construir confiança entre os pares. Antes que qualquer ação possa ser tomada com base nesses alertas, é fundamental verificar a veracidade dos dados e a confiabilidade dos veículos que os divulgam. Logo, torna-se necessário o desenvolvimento de soluções capazes de incentivar comportamentos cooperativos, mas que identifiquem a presença de nós maliciosos que propagam mensagens falsas na rede. Este trabalho descreve um sistema de reputação descentralizado baseado em uma blockchain de consórcio e contrato inteligente denominado BRS4VANETs. O sistema analisa a confiabilidade do veículo, detecta comportamentos maliciosos e contribui para a tomada de decisões. Veículos identificados como suspeitos ou maliciosos são armazenados em uma lista de reputação, com o objetivo ignorar suas mensagens. Os resultados são implementados, analisados e verificados através de um processo de simulação. Assim, experimentos com simuladores de rede e tráfego avaliam o risco de um ataque de mensagem falsa, a eficácia do sistema proposto e o impacto do uso do sistema em uma aplicação de segurança. Os resultados da simulação demonstram que mensagens falsas em redes veiculares têm consequências negativas e mitigadas quando utilizadas em conjunto com sistemas de reputação. Estes também mostram a viabilidade de possuir um sistema descentralizado baseado na tecnologia blockchain para armazenar e disseminar informações de reputação. Por fim, os resultados mostram que o BRS4VANETs consegue detectar com sucesso veículos considerados suspeitos e maliciosos.

Palavras-chave: Redes Veiculares. Sistemas de Reputação. Blockchain.

ABSTRACT

Vehicular network applications have become essential for providing drivers with services that are equipped with warning systems and instructions to ensure a safe and comfortable drive. Despite offering new opportunities, the use of these networks raises several security-related concerns, including the need to build trust among peers. Before any action can be taken based on these alerts, it is essential to check their data veracity and the reliability of the vehicles that disseminate them. Therefore, it becomes necessary to develop solutions capable of encouraging cooperative behavior, but that identify the presence of malicious nodes that propagate false messages on the network. This paper describes a decentralized reputation system based on a consortium blockchain and smart contracts called BRS4VANETs. This system analyzes vehicle reliability, detects malicious behavior, and contributes to decision-making. Vehicles identified as suspicious or malicious are stored in a reputation list, with the aim of ignoring your messages. Experiments with network and traffic simulators evaluated the risk of a false message attack, the effectiveness of our system, and the impact of using the system in a safety application. The results of simulations demonstrate that false messages in vehicular networks have a negative outcome unless they are used with a reputation system. They also show the feasibility of having a decentralized system to store and disseminate reputation information based on blockchain technologies. The results also demonstrate that BRS4VANETs can successfully detect the most suspicious and malicious vehicles.

Keywords: Vehicular Networks. Reputation Systems. Blockchain.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade Certificadora
ACM	Association for Computing Machinery
ACK	Acknowledge signal
AU	Application Unit
BBC	Based on biometrics blockchain
BCU	Custom Blockchain Unit
BFT	Byzantine Fault Tolerance
CSR	Certificate Signing Request
DETRAN	Departamento de Trânsito
DDoS	Distributed Denial of Service
DPoS	Delegated Proof of Stake
dPoW	Dynamic Proof-of-Work
DSRC	Dedicated Short-Range Communication
ETSI	European Telecommunications Standards Institute
GPS	Global Position System
IBFT	Istanbul Byzantine fault tolerant
ICP	Infraestrutura de Chaves Públicas
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
INM	Incremento do Número de Mensagens
IPFS	Interplanetary File System
IoT	Internet of Things
IoV	Internet of Vehicles
LDW	Local Danger Warning Application
LuST	Luxembourg SUMO Traffic
MANET	Mobile Ad hoc Network

NACK	Negative Acknowledgement
OBU	On Board Unit
OMNeT++	Objective Modular Network Testbed in C++
PBFT	Practical Byzantine Fault Tolerance
PGEAS	Pós-Graduação em Engenharia de Automação e Sistemas
PoA	Proof of Authority
PoE	Proof of Event
PoI	Proof of Importance
PoS	Proof of Stake
PoW	Proof of Work
PUF	Physical Unclonable Functions
P2P	Peer to Peer
QoS	Quality of Service
RPC	Remote Procedure Call
RSL	Revisão Sistemática da Literatura
RSU	Road Side Unit
RB	RSU-Beacon
SFW	Velocidade média do veículos
SRT	Velocidade média trânsito regular
STI	Sistemas de Transporte Inteligente
SUMO	Simulation of Urban Mobility
TA	Trust authority
TAB	Tamanho Armazenamento da Blockchain
TAV	Tempo do Aumento da Viagem
TFN	Taxa de Falso-negativo
TRV	Taxa de Redução de Velocidade

UFSC	Universidade Federal de Santa Catarina
UNIVALI	Universidade do Vale do Itajaí
VANET	Vehicular ad hoc networks
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
WAVE	Wireless Access in the Vehicular Enviroment
WM	Warning Message
WRM	Warning Revogation Message
WVM	Warning Validation Message

LISTA DE SÍMBOLOS

α	Fator de incremento da criticidade da mensagem
β	Fator de decremento da criticidade da mensagem
γ	Constante de ganho
Ω	Veículos de manutenção da rodovia
Δ	Câmeras de monitoramento da rodovia
Ack_Field	Campo da mensagem WVM
C_V	Certificado digital do veículo
$Crit\_Msg$	Criticidade da mensagem de alerta
FM_V	Número de mensagens falsas enviada pelo veículo
ID_M	Identificador da mensagem
ID_V	Identificador do veículo
ID_W	Identificador do evento de alerta
lat_V	Latitude do GPS veículo
lon_V	Longitude do GPS veículo
NC_{msg}	Nível de confiança
Rep_{New}	Nova reputação do veículo
Rep_{cur}	Reputação atual do veículo
$Sign_V$	Assinatura digital da mensagem
Th_Rep	Limiar de reputação
V_rep	Valor de reputação

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO

Devido ao acelerado processo de urbanização e ao crescimento desordenado das cidades, além do uso cada vez mais intenso de transporte motorizado individual pela população, a mobilidade passou por forte modificações. O acréscimo de carros nas ruas e rodovias resultou em congestionamentos, acidentes de trânsito, poluição e, consequentemente, baixa qualidade de vida. Contudo, alguns elementos como os avanços tecnológicos e a tendência global para a redução das emissões de gases poluentes, estão guiando para uma mudança de paradigma na mobilidade urbana (CEDER, 2021).

A indústria automobilística se prepara para estar cada vez mais integrada com a tecnologia e a conectividade. O avanço tecnológico, que engloba técnicas e instrumentos importantes para uma melhor dirigibilidade, conforto e, principalmente, segurança do motorista e dos passageiros, tem atraído muita atenção ao longo dos últimos anos. Esses avanços estão possibilitando agregar novas tecnologias aos veículos, como as voltadas para as redes veiculares, as quais viabilizam a comunicação entre veículos e o surgimento de novas aplicações que propiciam um aumento na segurança e eficiência do tráfego.

Dentre as aplicações de trânsito mais importantes, destaca-se o de Alerta de Perigo Local (LDW) pelos benefícios coletivos significativos ao divulgar mensagens de alerta que informam sobre situações de risco na rodovia (KOSCH, 2004). Nas aplicações LDW, são emitidas mensagens de alerta com informações sobre as condições das estradas quando são detectados eventos críticos, como travessia de animais, neblina, queda de pedras, buracos ou até mesmo acidentes. Os nós de rede (por exemplo, veículos) avaliam o conteúdo dos alertas recebidos. Sempre que a aplicação considerar suficiente a evidência de um evento, utilizará uma interface com o motorista para comunicar a existência do problema para que este possa reagir à situação de forma rápida e segura.

Os sistemas de transporte inteligentes (STI) desempenham um papel importante neste cenário uma vez que integram tecnologias de comunicações, controle e processamento em sistemas de transporte (GARG *et al.*, 2019). Em razão da frequente troca de dados entre os veículos, a cooperação entre eles se faz necessária. Por possuir ambientes complexos, de rápida mudança de topologia e dependente do coletivo, garantir a segurança da rede veicular é um fator crucial para o seu correto funcionamento, visto que, pelas suas características, estão sujeitos a diversos formas de ataques.

Mitigar os ataques, identificar ações de nós da rede maliciosos e as consequên-

cias de seus comportamentos torna-se relevante (KERRACHE *et al.*, 2018). Diversas aplicações podem ser úteis para prover segurança do trânsito nas rodovias. Contudo, a confiança nos nós que propagam e difundem os alertas precisa ser levada em conta, pois os veículos precisam desenvolver confiança entre si antes de coletar informações de seus pares, para que uma decisão confiável seja tomada. Além disso, nessas redes, não há garantia de que nós anteriormente honestos não serão corrompidos no futuro (ex. carros dirigidos por mais de uma pessoa).

Conforme (ZHANG, 2011), garantir a confiabilidade dos nós nas VANETs possui diversos desafios. Primeiramente, os veículos estão em constante circulação e há um dinamismo nos cenários. Em uma rodovia, a velocidade média de um veículo é de cerca de 100 quilômetros por hora. Em altas velocidades, o tempo para reagir a uma situação torna-se crítico. Portanto, é muito importante que os veículos possam verificar e confiar nas informações recebidas em tempo real. Em segundo lugar, pode ocorrer um fluxo intenso de veículos na rede em determinados horários, comprometendo a eficiência nas trocas de mensagens devido a problemas de escalabilidade.

Entre as soluções encontradas como meio de abordar esses desafios destacam-se os sistemas de reputação. Na literatura, os sistemas de confiança são frequentemente combinados com sistemas de reputação, dado que a decisão de um veículo confiar em mensagens de alerta de outro veículo deve ser baseada nas experiências anteriores. Um sistema de reputação robusto para VANETs requer capacidade de reagir a possíveis ataques, reconhecendo a reputação de veículos maliciosos e, assim, prevenir ataques ou detectá-los e reagir a eles mais rapidamente, e mitigar suas consequências.

Por conseguinte, alguns esforços já foram realizados para desenvolver um modelo de gerenciamento de confiança para VANETs (IQBAL *et al.*, 2019). No entanto, essa área ainda está aberta para pesquisas. Uma rede formada por veículos, apesar de apresentar um vasto universo de possibilidades e inovações, traz consigo uma enorme quantidade de desafios. Encontrar um equilíbrio entre segurança, eficiência e requisitos de rede continua sendo um problema em aberto. Além disso, as pesquisas podem ser aprimoradas com a integração de tecnologias atuais de ponta, como *blockchain*, *fog computing*, *big data analysis*, aprendizado de máquina, inteligência artificial, dentre outras.

Com o crescimento do escopo de aplicação da tecnologia *blockchain*, novas soluções baseadas nesta tecnologia vem sendo desenvolvidas. *Blockchain* é reconhecida como uma solução para problemas de segurança ao armazenar, monitorar, gerenciar e compartilhar dados de forma distribuída na rede (NAKAMOTO, 2009). Dessa forma, ela pode oferecer soluções práticas para muitos problemas das redes veiculares, especialmente para aqueles relacionados à confiança, pois, fornece uma plataforma eficiente para gerenciamento de reputação, protegendo os dados de forma distributiva.

1.2 PROBLEMA DE PESQUISA

Esforços contínuos vem sendo desenvolvidos para melhorar os STIs com o intuito de torná-los mais inteligentes e seguros e uma das formas é através das VANETs. Uma questão crítica em muitos STIs é a tendência em direção a uma centralização, o que pode comprometer a segurança do sistema. As tecnologias que estão se expandido rapidamente, incluindo a Internet das Coisas e a computação em nuvem, onde a maioria dos dados, análises e decisões são processadas por autoridades centralizadas ou em nuvem, afetam a segurança, uma vez que podem estar temporariamente indisponível devido a ataques maliciosos, limitações de desempenho ou simplesmente por operações incorretas (YUAN; WANG, 2016).

Muitas formas de ataques surgiram na tentativa de comprometer a segurança das VANETs em STIs. Dentre estes ataques, podem-se destacar aqueles que envolvem modificações de dados como, por exemplo, transmissão de dados fraudulentos sobre congestionamentos nas rodovias ou a localização do veículo. Tais ataques podem ser bastante prejudiciais inclusive ocasionando resultados que podem levar à perda de vidas. (WANG *et al.*, 2021).

Ambientes com grande dependência dos nós, como as VANETs, necessitam de mecanismos para lidar com a alta mobilidade dos nós e com a inerente falta de confiança entre membros. Os desafios são amplificados pelas limitações de recursos dos dispositivos do veículo, obrigando a criação de incentivos à cooperação.

No contexto das VANETs, a reputação de um veículo pode ser considerada uma coleção de opiniões mantidas por outros veículos sobre este, enquanto confiança é uma visão particular de um único veículo. Conforme (LIU, K. *et al.*, 2016), mecanismos de reputação baseiam-se no comportamento dos nós, onde cada nó possui um valor de reputação resultante do seu comportamento na rede. O valor de reputação é calculado e armazenado por outros nós que observam o seu comportamento. Esses mecanismos precisam ser capazes de calcular e atualizar os valores de reputação bem como detectar o mau comportamento e a não cooperação dos nós.

Diversos trabalhos que utilizam mecanismo de reputação para detectar ações de nós maliciosos e avaliar a confiança dos nós foram propostos (ENGOULOU *et al.*, 2019; CUI *et al.*, 2019; SAMARA, 2020; LIU, X. *et al.*, 2021; SULTAN *et al.*, 2021).

Nos últimos anos, sistemas de reputação foram desenvolvidos recorrendo à tecnologia *blockchain* (YANG, Y.-T. *et al.*, 2019; KHALID *et al.*, 2021; KUDVA *et al.*, 2021; INEDJAREN *et al.*, 2021; GAZDAR *et al.*, 2022) uma vez que substitui a centralização por um consenso confiável que, quando aplicado no contexto de gerenciamento de confiança, fornece robustez a um único ponto de falha. No entanto, o desenvolvimento de um sistema de reputação integrado com a tecnologia de *blockchain* apresenta enormes desafios. Para isso, uma *blockchain* de consórcio foi utilizada neste trabalho para

permitir que apenas entidades confiáveis gerenciem a reputação dos veículos na rede *blockchain*. Isso significa que as mudanças dos valores de reputação são armazenadas e gerenciadas de forma distribuída.

1.2.1 Pergunta de Pesquisa

O principal questionamento nesta pesquisa é:

"Um sistema de gerenciamento de confiança descentralizado pode ser capaz de identificar a presença de nós maliciosos e neutralizar suas ações mesmo diante de nós desconhecidos?"

Em busca da solução para tal questionamento, considerando o contexto apresentado, outras perguntas deverão ser respondidas no decorrer deste trabalho, como:

1. É possível projetar uma abordagem que visa analisar a confiança dos nós em redes veiculares diante de diferentes densidades?
2. Quais métricas serão utilizadas para avaliar o desempenho da abordagem proposta?
3. Qual o impacto decorrente do uso de gerenciamento de confiança descentralizado na entrega das mensagens de alerta com a utilização da tecnologia *blockchain*?

Tendo em vista os desafios dos sistemas de reputação, a **Pergunta 1** trata da complexidade em desenvolver uma abordagem, em uma rede totalmente descentralizada, de modo a realizar a avaliação da confiança dos nós em busca do benefício coletivo realizando o descarte correto das mensagens oriundas de membros maliciosos. A **Pergunta 2** trata da dificuldade de simular e avaliar abordagens do sistema proposto por meio de simulações bidirecionais entre simuladores de rede e de tráfego. Essa dificuldade é decorrente do fato que, além de simular a própria rede de comunicação e os traços de mobilidade, também deve-se controlar para ser possível avaliar o desempenho da proposta em cenários com densidades diferentes. Por fim, a **Pergunta 3** está relacionada ao impacto que a abordagem proposta e seus mecanismos podem gerar no desempenho do STI.

1.2.2 Solução Proposta

Esta tese segue a tendência atual que é combinar um sistema de confiança com um sistema de reputação. Dentre as várias categorias de comportamento malicioso (CELES; ELIZABETH, 2018), este trabalho aborda o problema de ataques falsos, onde um veículo malicioso cria uma situação de trânsito específica para poder enganar

outros motoristas espalhando informações falsas. Esses ataques podem levar a uma incompreensão do cenário real por veículos próximos, tendo consequências graves, como acidentes, engarrafamentos e mudanças de rota.

A proposta está dividida em duas partes, uma parte teórica e uma parte construída através de simulações que buscaram utilizar traços reais de mobilidade com diferentes fluxos de veículos. Na parte teórica, buscou-se definir as tecnologias escolhidas para o desenvolvimento do sistema de gerenciamento de confiança distribuído para VANETs baseado em reputação e *blockchain*. Relacionado a isso, foi definido como é realizado o mecanismo de troca de mensagens, os cálculos para avaliar a confiança dos veículos, bem como os algoritmos utilizados.

Este trabalho difere de outros estudos pelo uso de uma *blockchain* de consórcio leve, visto que a demora adicional da atualização da *blockchain* afeta o tempo da detecção de veículos maliciosos. Assim, é introduzida uma lista de reputação contendo os veículos considerados suspeitos e maliciosos, propagados aos demais veículos previamente, antes do seu registro na *blockchain*, evitando assim restrição de atrasos de tempo decorrentes do uso da *blockchain*. Além disso, o sistema proposto apresenta uma arquitetura completa em que descreve os seus componentes, algoritmos, protocolo de disseminação (comunicação, roteamento, entre outros) e utiliza traços reais de mobilidade para simulações com diferentes densidades de veículos.

Nesse sentido, esta pesquisa visa contribuir com o estado da arte relacionado à segurança em redes veiculares através da proposição de um sistema de gerenciamento de confiança descentralizado e baseado em *blockchain*, projetado para analisar e armazenar a reputação e os padrões comportamentais dos veículos.

1.2.3 Delimitação do Escopo

Nesta tese, a abordagem foi implementada em simuladores de rede e de tráfego, visto que o desenvolvimento de um protótipo real possui um custo muito elevado. Em sistemas baseados em confiança não existe remuneração pela execução de uma tarefa. Contudo, de modo a incentivar a cooperação dos veículos na troca de mensagens na rede veicular e para que os principais eventos possam ser validados na rodovia, uma abordagem baseada em retribuição e recompensas pode ser usada. Essa abordagem pode ser introduzida para recompensar os veículos com mais cooperação e incluir uma redução de valores de pedágios, descontos no IPVA e seguros. No entanto, essas abordagens estão além do escopo desta tese.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Analisar a confiança dos veículos em aplicações de segurança no trânsito, de forma a identificar a presença de nós maliciosos, neutralizar suas ações e contribuir para tomada de decisões baseada no comportamento dos veículos.

1.3.2 Objetivos Específicos

Diante do que está especificado como objetivo geral deste trabalho, os objetivos específicos são:

- Estabelecer confiança nas redes veiculares através de um sistema de gerenciamento de confiança distribuído usando *blockchain* para analisar e registrar o comportamento dos veículos. Isso envolve recompensar os veículos honestos e punir aqueles que se comportam mal;
- Estabelecer, gerenciar e armazenar uma lista de reputação, por meio de mensagens coletadas e consolidadas através das RSUs e posteriormente propagadas aos veículos, contendo informações dos nós suspeitos ou maliciosos;
- Prover uma abordagem descentralizada para excluir veículos maliciosos da rede, através da revogação do seu certificado por uma autoridade certificadora;
- Utilizar um sistema de votação para mitigar o problema de ataques de conluio por veículos maliciosos e aumentar a segurança das decisões tomadas quanto à punição destes nós na rede; e
- Avaliar a eficiência, eficácia e o impacto da abordagem proposta, por meio de um conjunto de simulações;

1.4 METODOLOGIA

Segundo (PRODANOV; FREITAS, 2013), a pesquisa científica tem por objetivo contribuir para a construção do conhecimento humano em qualquer área. Esta seção apresenta a metodologia de pesquisa adotada e os procedimentos metodológicos aplicado para realização desta pesquisa.

1.4.1 Metodologia da Pesquisa

No desenvolvimento da pesquisa descrita neste trabalho, foi aplicado o método hipotético-dedutivo. Conforme (PRODANOV; FREITAS, 2013), o método hipotético-dedutivo parte da percepção de uma lacuna no conhecimento, acerca da qual se formula hipóteses e, pelo processo de inferências dedutivas, testa a predição da ocorrência de fenômenos abrangidos pela hipótese.

Do ponto de vista de sua natureza, este trabalho pode ser classificado como pesquisa aplicada. A pesquisa aplicada visa gerar conhecimentos para a aplicação prática dirigida a solução de problemas específicos. Neste contexto, este trabalho tem como objetivo a formação de conhecimento através de um sistema de gerenciamento de confiança distribuído para redes veiculares baseado em mecanismo de reputação e *blockchain*. No desenvolvimento desta pesquisa, emprega-se o método hipotético dedutivo, em que parte da percepção de uma lacuna no conhecimento, acerca da qual se formula hipóteses e, pelo processo de inferências dedutivas, testa a predição da ocorrência de fenômenos abrangidos pela hipótese.

Do ponto de vista dos objetivos, a pesquisa pode ser classificada como exploratória, dado que exige amplo levantamento bibliográfico sobre o assunto. A pesquisa exploratória visa proporcionar maior familiaridade com o problema com vistas a torná-lo explícito ou a construir hipóteses. Do ponto de vista da abordagem do problema, essa pesquisa é majoritariamente quantitativa. No trabalho, foram coletados dados estatísticos a partir da execução de simulações que permitiram avaliar as hipóteses estabelecidas. Contudo, alguns requisitos qualitativos também são abordados nessa pesquisa com o objetivo de mensurar benefícios de segurança proporcionados aos condutores.

Por fim, pretende-se aplicar os experimentos em cenários simulados com características reais. Deve-se analisar o comportamento e características da abordagem proposta em cenários com densidades e topologias variáveis.

1.4.2 Procedimentos Metodológicos

Para o cumprimento dos objetivos, esta subseção visa descrever as etapas para realização do trabalho conforme as definições citadas anteriormente:

- **Pesquisa bibliográfica:** Tal pesquisa visou estabelecer o atual estágio do estado da arte na área de interesse desse trabalho, com o objetivo prover conhecimento e suporte teórico para o desenvolvimento da solução proposta. Foi realizado um levantamento bibliográfico, sendo que a pesquisa foi conduzida sobre os conceitos fundamentais das redes veiculares e *blockchain*. Nesta etapa foram estudados os aspectos de segurança nas redes veiculares com os conceitos de gerenciamento de confiança e sistemas de reputação visando detecção dos principais problemas, as arquiteturas, modelos, padrões e mecanismos propostos como possíveis soluções. Foram também objeto de estudo desta pesquisa, os principais mecanismos de consenso utilizados na tecnologia *blockchain* assim como as categorias de *blockchain* existentes e suas características. Neste estudo, foram utilizados materiais publicados em artigos de periódicos e de conferências científicas e congressos e também em livros.

- **Análise de trabalhos relacionados:** Na fase seguinte da pesquisa, foi realizada uma análise dos trabalhos correlatos encontrados na literatura através de uma revisão sistemática da literatura. A revisão enfocou trabalhos que empregam gerenciamento de confiança no contexto das redes veiculares com uso da tecnologia de *blockchain*.
- **Definição do sistema de gerenciamento de confiança distribuído:** Após o levantamento bibliográfico e leitura de trabalhos correlatos, foi definido um sistema de gerenciamento de confiança distribuído para redes veiculares baseado em reputação e *blockchain*. Foram definidos neste sistema como é realizado o mecanismo de troca de mensagens, os cálculos para avaliar a confiança dos veículos, bem como os algoritmos utilizados. O sistema foi modelado e implementado em um simulador.
- **Realização de simulações:** Simulações foram realizadas visando aferir alguns parâmetros e obter dados necessários para a avaliação do sistema proposto. O simulador utilizado foi o OMNeT++ (Objective Modular Network Testbed in C++) por permitir uma simulação com nível de detalhes satisfatórios. De modo a tornar as simulações mais realistas, foi utilizada uma ferramenta geradora de cenários de mobilidade, o SUMO (Simulation of Urban Mobility), a qual foi integrada e acoplada bidirecionalmente com o simulador OMNeT++.
- **Avaliação dos resultados:** Com base nos resultados obtidos nas simulações, foi possível avaliar a eficiência e eficácia do sistema de reputação desenvolvido neste trabalho para identificar nós maliciosos, bem como verificar os impactos decorrentes do seu uso.

1.5 ESTRUTURA DA TESE

O presente trabalho está enquadrado na área de concentração relacionada aos Sistemas Computacionais, estando este conforme as atividades desenvolvidas no Programa de Pós-Graduação em Engenharia de Automação e Sistemas (PGEAS) da Universidade Federal de Santa Catarina (UFSC). Mais especificamente, pretende-se abordar conteúdos no contexto de segurança em redes veiculares.

Este documento está dividido em seis capítulos, incluindo a introdução, apresentada aqui. Assim, os próximos capítulos deste documento estão organizados da seguinte forma:

- **Capítulo 2** aborda os principais conceitos envolvidos no contexto deste trabalho importantes para a compreensão dos assuntos tratados nesta tese.
- **Capítulo 3** apresenta o estado da arte em que é efetuada uma análise das soluções propostas no que diz respeito ao tema principal deste projeto de pesquisa,

ou seja, modelos de confiança ou sistemas de reputação utilizando tecnologia *blockchain*.

- **Capítulo 4** é apresentado o detalhamento da abordagem proposta que inclui as tecnologias escolhidas para o desenvolvimento da proposta.
- **Capítulo 5** inclui os resultados obtidos nas simulações e suas análises para avaliar a proposta.
- **Capítulo 6** apresenta as considerações finais sobre esta tese, destacando novamente os objetivos e motivações que nortearam o trabalho e as principais contribuições da tese. Por fim, algumas perspectivas para trabalhos futuros são apontadas.

Por fim, é apresentada a bibliografia utilizada durante a preparação deste documento. O **Apêndice A** apresenta o protocolo de busca onde os trabalhos relacionados foram selecionados e analisados por critérios definidos na revisão sistemática. O **Apêndice B** apresenta o *Smart Contract* implementado. E no **Anexo A** os valores de ganho simulados para as variáveis de incremento e decremento das mensagens.

1.5.1 Publicações

Como atividade decorrente desta tese de doutorado, o artigo intitulado **Um sistema de reputação baseado em *blockchain* contra ataques de mensagens falsas em VANETs**[1] foi publicado na trilha principal do XXI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSEG 2021). O trabalho envolveu as seguintes instituições de ensino: (i) Universidade Federal de Santa Catarina, Santa Catarina, Brasil; (ii) Universidade do Vale do Itajaí, Santa Catarina, Brasil; e (iii) Centro Universitário Estácio de Santa Catarina, Santa Catarina, Brasil.

Ainda como resultado desta tese, o artigo intitulado **Blockchain e Sistemas de Reputação em Redes Veiculares: Uma Revisão Sistemática**[2] foi publicado na trilha principal do Computer on the Beach (COTB 2021). O trabalho envolveu as seguintes instituições de ensino: (i) Universidade Federal de Santa Catarina, Santa Catarina, Brasil; (ii) Universidade do Vale do Itajaí, Santa Catarina, Brasil; e (iii) Centro Universitário Estácio de Santa Catarina, Santa Catarina, Brasil.

Outros artigos envolvendo os resultados dessa tese foram submetidos a periódicos Qualis A e estão em fase de revisão.

[1] https://sol.sbc.org.br/index.php/sbseg/article/view/17322
[2] https://periodicos.univali.br/index.php/acotb/article/view/17411

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados alguns conceitos fundamentais para a compreensão da proposta da tese. Inicialmente, são descritos os conceitos básicos de sistemas de transportes inteligentes e os fundamentos das redes veiculares e da sua segurança. Por fim, a tecnologia *blockchain* é descrita, bem como sua classificação, arquitetura, mecanismos de consenso e segurança são apresentados.

2.1 SISTEMAS DE TRANSPORTE INTELIGENTES

A mobilidade urbana é um problema atual da sociedade moderna e dos grandes centros urbanos, o qual ocasiona perdas econômicas e de tempo, maior consumo de combustível e maiores emissões de CO_2. Nesse contexto, os Sistemas de Transporte Inteligentes (STIs) se mostram o caminho para o aumento da eficiência e segurança nas vias urbanas e auto-estradas, provendo plataformas confiáveis para o transporte e soluções para cooperação.

Os STIs permitem uma integração de tecnologias de informação e comunicação direcionadas aos sistemas de transporte e gerenciamento de tráfego para melhorar a segurança, eficiência e sustentabilidade das redes de transportes, reduzir o congestionamento do tráfego e melhorar o conforto dos motoristas. Esse tipo de sistema pode abranger uma ampla diversidade de técnicas e abordagens usadas por aplicações de áreas como: controle de tráfego e semafórico, gestão de pedágios, sistemas de auxílio na condução, gerenciamento de frota, sistema de informações aos usuários entre outras.

Um STI pode ser caracterizado como uma combinação de técnicas de conectividade, coordenação, adaptabilidade e resposta automática para otimização de políticas de transporte, visando melhorar a segurança e mobilidade dos transportes, bem como auxiliar a gestão da infraestrutura (FITAH *et al.*, 2018). STIs oferecem benefícios e tomada de decisão aos usuários, de modo a melhorar a a satisfação com o sistema de transporte.

As redes veiculares constituem o pilar fundamental da nova geração dos STIs (AL-SHAREEDA *et al.*, 2021). Grandes esforços de pesquisas estão sendo dedicados tanto no sentido de aprimorar essas redes, quanto no sentido de explorar suas potencialidades, desenvolvendo novas aplicações que melhoram a segurança e o conforto para os usuários. De forma complementar, as montadoras vem, cada vez mais, investindo em pesquisas e desenvolvimentos de novas tecnologias para melhorar a dirigibilidade dos veículos e reduzir ao máximo as possibilidades de acidentes de trânsito.

2.2 REDES VEICULARES

2.2.1 Conceito

As VANETs podem ser classificadas como uma subcategoria das redes *ad hoc* móveis (*MANETs*) e se caracterizam por serem redes autoconfiguráveis e distribuídas que proveem comunicação entre veículos próximos e equipamentos fixos, denominados RSUs (*Road side units*), distribuídos ao longo das vias. Aplicações de STIs que envolvem trocas de dados entre veículos estão se tornando cada vez mais viáveis diante do crescente número de veículos equipados com tecnologias computacionais e dispositivos de comunicação sem fio, denominados OBUs (*On board units*).

Devido à mobilidade dos nós e à necessidade de segurança dos dados, é extremamente importante considerar vários aspectos ao realizar troca de dados em uma rede veicular (WANG; LIU, 2021). Essas redes têm algumas características únicas que as diferenciam (KADHIM; NASER, 2021):

- **Alta mobilidade**: o ambiente em que uma rede veicular opera é extremamente dinâmico, dado que os nós se movem o tempo todo com diferentes velocidades e direções.
- **Topologia dinâmica**: devido à alta mobilidade, os tempos de conexões são curtos, especialmente entre nós que se deslocam em direções contrárias. Portanto, a topologia da rede muda rapidamente, de forma dinâmica e imprevisível.
- **Desconexões frequentes:** a alta mobilidade dos nós, topologia dinâmica, obstáculos, interferências eletromagnéticas, e regiões com baixas densidades de nós podem provocar descontinuidades frequentes nas comunicações entre os nós.
- **Segurança e privacidade:** a segurança e privacidade são requisitos críticos em aplicações em VANETs. Se, por um lado, os receptores querem ter certeza de que podem confiar na fonte de informação, por outro lado, a disponibilidade de tal confiança pode se contrapor aos requisitos de privacidade de um remetente.

Essas características tornam desafiadoras a implementação de soluções em redes veiculares. As soluções precisam considerar o cenário descontínuo que pode existir nas vias, bem como prever requisitos para uma comunicação eficiente e segura nesse cenário. A Tabela 1 resume os principais desafios encontrados.

2.2.2 Arquitetura

As redes veiculares podem ser classificadas com base em sua arquitetura, a qual define a forma como os veículos se organizam e se comunicam. Assim, os principais elementos que compõem a arquitetura das redes veiculares são (LEE *et al.*, 2016):

Tabela 1 – Principais desafios em VANETs

Fonte: (KERRACHE, 2017)

Questões	**Descrição**
Mobilidade	Velocidades altas que causam mudanças frequentes de topologia.
	Tempo de comunicação limitado entre nós.
	Densidade da rede altamente variável.
Fator humano	Dificuldades para apresentar dados e recomendações aos motoristas sem distração e sobrecarga de informação.
	Motoristas com tempos de reação diferentes.
Interoperabilidade	Necessidade de cooperação e interoperabilidade entre fabricantes de automóveis e organizações de transporte
Conectividade	Escolha e posicionamentos de antenas.
	Escolha de frequências de comunicação e larguras de banda.
Posicionamento	Precisão dos receptores de GPS.
Tempo	Necessidade de ter acesso ao meio garantido sempre que necessário.
	Dificuldades para evitar congestionamentos na rede.
	Dificuldades para implementar e manter a Qualidade de Serviço (QoS) na rede.
Confiabilidade	Necessidade de garantir que os dados sejam recebidos corretamente pelo destinatário pretendido.
	Necessidade de balancear o conflito entre tempo e confiabilidade.
Custo	Complexidade na escolha das tecnologias de comunicação.
	Dificuldade para a escolha do número de antenas.
Ambiente rodoviário	Alta velocidade, cenários arriscados, pontos cegos, mudanças de pista, colisões.
Ambiente urbano	Problemas de conectividade devido a interferências dos prédios.
	Densidade de veículos muito alta.

- **Unidades de bordo (*OBUs*)**: embarcadas nos veículos, com capacidades de processamento, armazenamento e comunicação, que permitem a troca de informações com as *RSU* ou com outras *OBUs*.
- **Unidades de acostamento (*RSUs*)**: atuam como pontos de acesso à internet implantados às margens de rodovias, ruas e avenidas, para a comunicação entre os veículos.
- **Unidades de aplicação (*Application Units – AUs*)**: dispositivos presentes em veículos responsáveis pela execução de serviços e tarefas, como avisos de congestionamentos e colisões;

A disseminação das informações desempenha um papel crítico em VANETs pois precisa superar os desafios mencionados visando atender requisitos de desempenho, capacidade, cobertura e segurança exigidos pelas aplicações. A comunicação pode ser realizada das seguintes formas (CUNHA, F. *et al.*, 2016):

- **Veículo para veículo (*Vehicle-to-Vehicle – V2V*)**: a comunicação ocorre apenas entre veículos, atuando como roteadores e retransmitindo as mensagens através de múltiplos saltos. sem a necessidade de um elemento centralizador.
- **Veículo para infraestrutura (*Vehicle-to-Infrastructure – V2I*)**: nessa categoria de comunicação, veículos trocam informações com as infraestruturas às margens

das vias para diminuir problemas de falta de conectividade e executar aplicações para coleta de informações.

- **Arquitetura híbrida:** mescla os dois tipos de comunicação (V2V e V2I) e utiliza uma infraestrutura mínima para aumentar a conectividade. São responsáveis pela comunicação do veículo para infraestrutura em um salto (*single-hop*) ou vários saltos (*multi-hop*), para alcançar seu destino.

Outro tipo de comunicação existente, denominada V2X *(Vehicle-to-everything)*, representa a troca de informações de um veículo com qualquer dispositivo que ele possa se comunicar, tais como pedestres, ciclistas, etc. Estes serviços requerem comunicações confiáveis que permitam a propagação de informações com máxima latência mesmo com veículos em alta velocidade.

2.2.3 Aplicações

Existe um grande interesse por parte da academia e da indústria no desenvolvimento de aplicações para redes veiculares. A aplicabilidade das redes veiculares se baseia na coleta, no processamento e na disseminação das informações, que por serem diversificadas levam a diferentes categorizações das aplicações (GUERRERO-IBÁÑEZ *et al.*, 2018). Como exemplo, as aplicações para VANETs podem ser categorizadas em três grupos (JAKUBIAK; KOUCHERYAVY, 2008):

1. **Aplicações de Segurança:** visam evitar ou diminuir o número de acidentes nas rodovias. Exemplos desse tipo de aplicação, incluem alerta de mudança de faixa, alerta de perigo nas estradas, entre outros. Possuem caráter preventivo e emergencial, onde o principal desafio é divulgar rapidamente as informações para que o condutor tenha tempo para reagir.
2. **Aplicações de Conveniência:** são voltadas à assistência ao condutor com o objetivo de auxiliar na condução do veículo a partir de informações úteis como, por exemplo, navegação, alerta de pedágio, informações de disponibilidade de estacionamento, localização de postos de combustíveis, etc.
3. **Aplicações Comerciais de Infoentretenimento**: são relacionadas aos serviços baseados em localização, como propagandas e entretenimento, ou seja, transmissão de vídeos, atualização de redes sociais, etc.

A obtenção de QoS nas aplicações em VANETs pode ser fortemente influenciada por diferentes fatores que afetam, principalmente, a mobilidade dos veículos e as mudanças dinâmicas da topologia da rede. Dentre esses fatores se destacam as diferentes densidades do tráfego dependentes do horário ao longo do dia, os diferentes limites de velocidade dependentes do tipo da via (ex. autoestrada, estrada rural

ou urbana), e também as diferentes categorias de veículos (ex. caminhões, carros e motocicletas).

Devido a essa complexidade para manter a segurança e a confiabilidade nas aplicações veiculares, um dos grandes desafios enfrentados está relacionado à disseminação dos dados na rede. Um dos pilares para se enfrentar esse problema é o uso de protocolos de disseminação de mensagens confiáveis e eficientes.

2.2.4 Padrões de Comunicação

Em 2004, visando normatizar as comunicações em redes veiculares, foi definido o padrão IEEE 802.11p *WAVE*(*Wireless Access in the Vehicular Enviroment*). Este padrão suporta a troca de dados entre veículos em alta velocidade trabalhando na frequência licenciada de 5,9 GHz e com alcance de até 1000 metros (WEIL, 2009).

O padrão *WAVE* é composto por cinco documentos da família IEEE 1609: *IEEE P1609.0:* descreve a arquitetura e seus serviços necessários; *IEEE P1609.1:* descreve o gerenciamento de recursos; *IEEE P1609.2:* refere-se aos serviços de segurança para as aplicações e mensagens; *IEEE P1609.3:* descreve os serviços de rede e; o *IEEE P1609.4:* descreve as extensões para o 802.11.

O padrão *IEEE 802.11p*, extensão da família de protocolos *IEEE 802.11*, é destinado para médias distâncias, com alta mobilidade dos nós e mudanças rápidas de canal. Este padrão trabalha com sistema de prioridade usando múltiplos canais e, na arquitetura WAVE, é responsável pela definição das diferenças específicas do controle de acesso ao meio em relação ao padrão *802.11* tradicional.

2.3 SEGURANÇA

Em uma rede efêmera e dependente da cooperação entre nós, a segurança se torna um dos aspectos centrais para seu correto funcionamento. As aplicações STI dependem de informações trocadas entre veículos e informações incorretas podem comprometer a segurança dos veículos na rodovia. Além disso, as VANETs possuem características específicas diferentes das redes tradicionais e, portanto, são vulneráveis a ameaças e vulnerabilidades.

Nessas redes, os ataques de nós maliciosos podem prejudicar outros nós na rede intencionalmente. Em alguns casos, nós maliciosos podem suprimir as mensagens corretas trocadas entre os veículos, adulterá-los ou disseminar informações falsas de segurança, resultando em congestionamento, acidentes rodoviários ou indisponibilidade de recursos, o que colocará a segurança de motoristas, passageiros, e pedestres em risco (FINCK, 2018).

Diante disso, mecanismos de segurança em VANETs devem ser utilizados para

evitar esses ataques ou, caso ainda ocorram, o sistema deve agir para detectar e mitigar rapidamente seus efeitos. Uma classificação geral dos ataques e ameaças em VANETs é ilustrada na Figura 1 e descrita a seguir:

- **Ataques contra a disponibilidade:** a negação de serviço é a forma mais comum de ataque. Do ponto de vista das VANETs, o objetivo do invasor é bloquear os canais de comunicação e impedir que os veículos tenham acesso à rede.
- **Ataques contra autenticidade e identificação:** sempre que um veículo na rede precisa se comunicar com segurança, o requisito básico é a capacidade de identificar os nós envolvidos ou autenticar suas mensagens. Ações dos veículos resultantes de mensagens recebidas devem ser baseadas em mensagens autênticas enviadas por remetentes legítimos.
- **Ataques contra confidencialidade:** ataques para descobrir a localização e as rotas dos veículos podem comprometer suas privacidades. Esse tipo de ataque pode representar ameaças graves, pois permite que invasores interceptem comunicações e roubem dados críticos.
- **Ataques contra integridade:** A integridade dos dados foi projetada para garantir que esses dados não sejam alterados à medida que os usuários enviam e recebem mensagens pela rede. Os diferentes tipos de ataques incluem a capacidade do invasor de se passar por um usuário legítimo e transmitir mensagens falsas.
- **Ataques de repúdio:** Os motoristas que causam acidentes ou divulgam informações falsas na rede devem ser identificados. Os ataques de repúdio permitem que os invasores neguem serem os autores de suas ações maliciosas.

O modelo de ataque adotado nesta tese se concentra em ameaças que violam a integridade envolvendo mensagens falsificadas e alterações de mensagens, bem como a autenticidade contra ataques de repetição, mascaramento e sybil.

Como visto, muitas formas de ataques surgiram na tentativa de comprometer as aplicações veiculares (MANIVANNAN *et al.*, 2020). Ao lidar com problemas de segurança em redes veiculares é importante especificar os requisitos de segurança que precisam ser garantidos para o seu correto funcionamento e de suas aplicações.

2.3.1 Conceitos de gerenciamento de confiança e reputação

Na tentativa de reduzir as ações realizadas por nós maliciosos, surgiram alguns métodos para chamar a atenção para nós que se comportam corretamente na rede (SAMARA, 2020). Dentre esses métodos, destacam-se os que utilizam sistemas de reputação. Com base nessa abordagem, surge a ideia da criação de grupos de confiança, a qual visa a criação de grupos que confiam entre si e cooperam no intuito de combater os nós maliciosos.

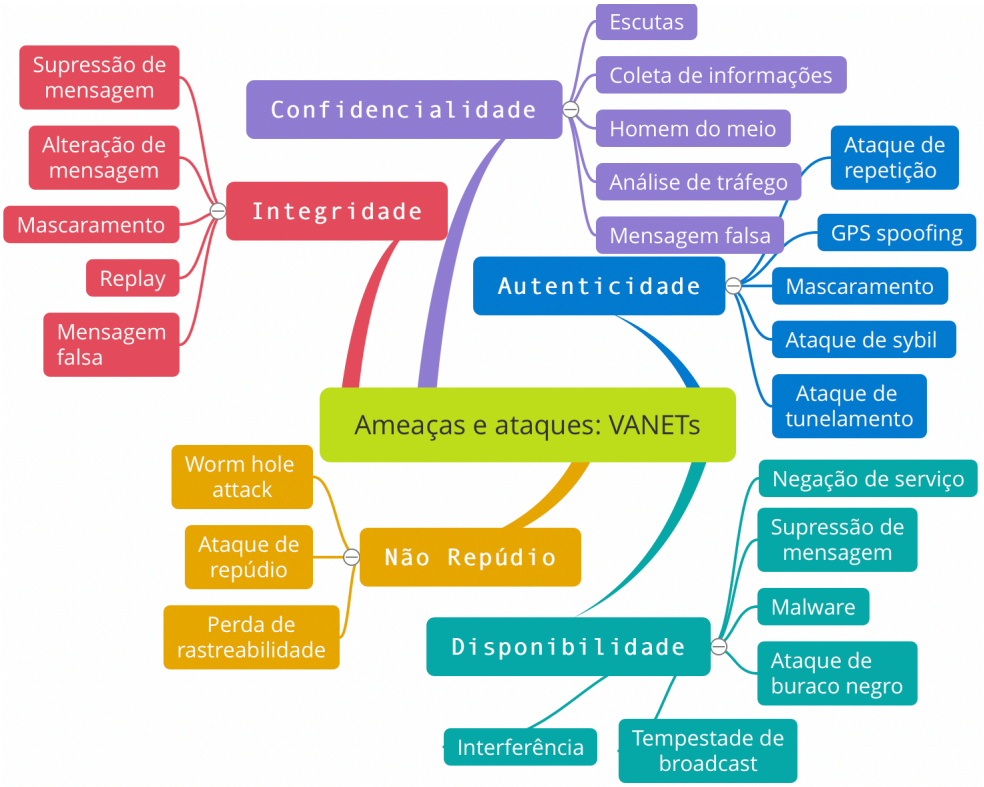


Figura 1 – Exemplos de ameaças e ataques em VANETs.

Fonte: (GAYATHRI; GOMATHY, 2021) adaptado

Os termos reputação e confiança estão fortemente ligados. Segundo (GRANDISON; SLOMAN, 2000), a confiança, em termos computacionais, pode ser definida como a crença que um nó tem na atitude favorável do outro nó em prover a qualidade de serviço esperada, em um dado contexto e período. A confiança pode ser definida também, como a firme convicção de que um nó agirá de forma confiável e segura, dentro de um contexto específico.

Assim, o nível individual de confiança em uma pessoa ou dispositivo pode ser obtido a partir de uma combinação das indicações recebidas e das experiências pessoais. Nas redes veiculares, a reputação é utilizada para criar confiança entre veículos que não possuem conhecimento prévio uns dos outros, mas que usam suas experiências passadas juntamente com o *feedback* de outros veículos para avaliar a confiabilidade dos nós na rede (IQBAL *et al.*, 2019).

Na visão de (KERRACHE *et al.*, 2016), um modelo de confiança eficaz precisa possuir as seguintes propriedades:

- **Eficiência:** precisa ser eficiente para determinar a confiabilidade e autenticidade de uma mensagem de alerta em situações esparsas ou congestionadas;
- **Privacidade:** não deve revelar informações confidenciais, como, por exemplo, a identidade real do remetente.

- **Robustez:** deve ser resistente a ataques que visam burlar a confiabilidade ou desabilitar o modelo de confiança.
- **Anonimato condicional:** as comunicações V2V e V2I devem ser anônimas para preservar a privacidade de identidade dos veículos. Por outro lado, o anonimato deve ser condicional para garantir que as autoridades possam rastrear os veículos em caso de necessidade.

Os modelos de confiança em redes veiculares podem ser divididos em três categorias principais (ZHANG *et al.*, 2019), conforme ilustrado na Figura 2. O modelo de confiança com base na entidade (nó), foca na avaliação da confiabilidade de cada veículo, considerando as opiniões dos demais veículos na rede. O modelo de confiança baseada em dados concentra-se em avaliar a confiabilidade das mensagens recebidas dos veículos próximos em vez de confiança do próprio veículo. Por fim, o modelo híbrido que combina a reputação dos veículos e das mensagens recebidas.

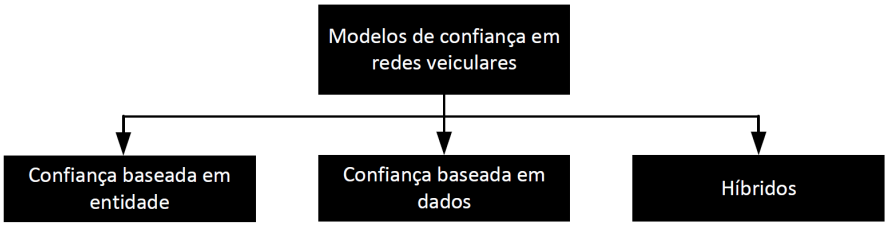


Figura 2 – Modelos de confiança em redes veiculares.

A utilização da reputação em redes veiculares requer a criação de mecanismos que formalizem o conceito de reputação como um mecanismo computacional e alguns pontos importantes destes mecanismos precisam ser observados (HU; BURMESTER, 2009; DENNIS; OWEN, 2015):

- **Confiança vs. Reputação**: confiança é uma ação concreta binária. Por outro lado, a reputação pode ser definida como um grau de medida coletiva baseada nas avaliações de diversos nós.
- **Reputação Direta vs. Indireta**: reputação direta é aquela em que um nó monitora o comportamento dos outros nós, geralmente em um salto (vizinho). Reputação indireta, as informações são obtidas consultando outros nós da rede.
- **Reputação Global vs. Local**: reputação global é aquela onde os nós utilizam informações trocadas entre os outros nós da rede para calcular a reputação de cada nó. Nos sistemas de reputação local, somente as observações locais dos nós vizinhos são consideradas.
- **Reputação Otimista vs. Pessimista**: na abordagem de reputação otimista, assume-se que um nó desconhecido é confiável até que prove o contrário. Já na abordagem pessimista, assume-se que um nó desconhecido não é confiável.

Os mecanismos de reputação constituem uma forma de promover a colaboração honesta dos nós na rede. Ao mesmo tempo, esses mecanismos reduzem a importância da participação de nós maliciosos ou com funcionamento anômalo, podendo, por fim, retirá-los completamente da rede.

2.4 BLOCKCHAIN

2.4.1 Conceito

O principal objetivo da tecnologia *blockchain* é o de garantir que informações compartilhadas publicamente possam ser armazenadas com segurança e de maneira distribuída. *Blockchain* foi originalmente desenvolvido para a operação da moeda criptográfica *bitcoin* em 2008 (NAKAMOTO, 2008), mas encontra-se em constante evolução e agora seu escopo se tornou muito mais amplo e está trazendo mudanças significativas no ambiente de tecnologias e de negócios. Além de criptomoedas, a *blockchain* pode ser um pilar para desenvolver e implantar aplicações descentralizadas de forma confiável e segura entre participantes que não necessariamente têm confiança entre si e estão dispersos em larga escala em uma rede *peer-to-peer* (P2P).

A *blockchain* foi projetada para ser um livro-razão público distribuído digitalmente que registra transações ordenadamente, servindo como um sistema de registros distribuído o qual traz transparência, segurança e integridade aos dados permitindo um registro robusto e auditável de todas as transações (GREVE *et al.*, 2018). A Figura 3 ilustra as principais características da *blockchain*:

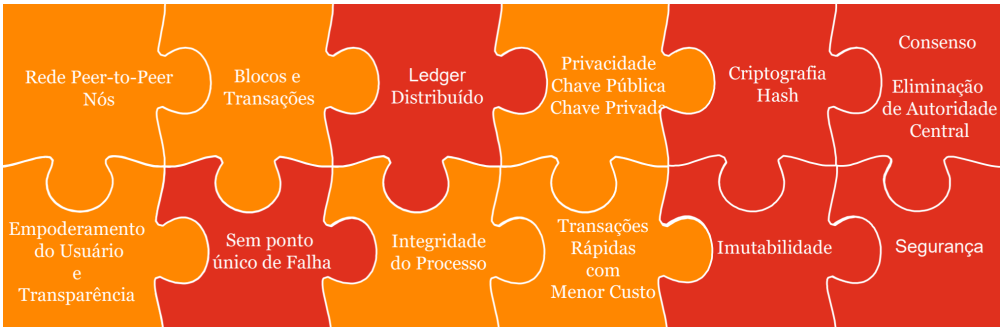


Figura 3 – Principais características da *blockchain*.

A tecnologia *blockchain* passou até o momento por quatro grandes evoluções (PANDA, 2021):

- ***Blockchain* 1.0:** a sua primeira versão está relacionada ao uso comercial da moeda, a implantação de criptomoedas em aplicações relacionadas a dinheiro, como remessa e sistemas de pagamento digital.
- ***Blockchain* 2.0:** diz respeito ao seu uso com contratos, questões econômicas, aplicações financeiras e de mercado usando a *blockchain*, mais extensas do que

transações simples de caixa: ações, empréstimos, hipotecas, títulos e contratos inteligentes.

- ***Blockchain* 3.0:** refere-se ao seu uso além da moeda, finanças e mercados, marcada pelo uso na ciência de forma geral. Traz consigo um novo paradigma para superar problemas de restrições referentes à interoperabilidade, escalabilidade e sustentabilidade das gerações anteriores.
- ***Blockchain* 4.0:** em fase de implementação e com foco na inovação, visa prover um ambiente aplicável ao mercado para criar e executar aplicações descentralizadas mais aprimoradas, tendo como foco principal, a velocidade no processo das transações e a usabilidade.

A estrutura em forma de cadeias de blocos torna a tecnologia *blockchain* resistente à violação e alteração. Neste sentido, existem propriedades que são inerentes à tecnologia de cadeia de bloco, sendo estas compostas por alguns elementos-chave (LIN; LIAO, 2017):

- **Descentralização:** os dados são gravados, armazenados e atualizados de maneira distribuída, sem a necessidade de um nó central, apenas através de estabelecimentos de confiança entre as partes.
- **Transparência:** todos os registros dos dados no sistema *blockchain* são transparentes para cada nó, estando disponíveis para todos os usuários, podendo, desta forma, serem verificados e auditados.
- **Disponibilidade e Integridade:** de maneira a manter o sistema disponível e consistente, todos os conjuntos de dados e transações são replicados, de forma segura, em diferentes nós da rede.
- **Imutabilidade e Irrefutabilidade:** uma *blockchain* consiste em uma cadeia de blocos consecutivamente conectada. Qualquer modificação no bloco anterior invalida todos os blocos consequentemente gerados, ou seja, uma vez registradas não podem ser refutadas.

2.4.2 Classificação

As *blockchains* podem ser categorizadas com base em seus modelos de permissão, os quais determinam as permissões concedidas aos participantes em sua cadeia. Basicamente, assume-se três tipos de categorias (YANG, R. *et al.*, 2020; HOY, 2017):

1. *Blockchain* pública: todas as transações são públicas, não restritivas, totalmente distribuídas, descentralizadas e sem permissão, dado que todos os nós podem realizar transações e consultar o histórico na rede. Suas regras são definidas

por consenso entre os usuários de forma descentralizada. As mais comuns atualmente são as criptomoedas, com destaque para o *Bitcoin*[1] e *Ethereum*[2].

2. *Blockchain* de consórcio: categoria formada por grupos de corporações ou instituições que dividem o investimento e estabelecem uma lista de pessoas com acesso ao sistema. Os dados dessas pessoas na *blockchain* podem ser públicos ou privados, conhecidos como parcialmente descentralizados. Um exemplo desta categoria é o projeto *Hyperledger*[3] criado pela *Linux Foundation*.
3. *Blockchain* privada: é uma categoria restrita, que descaracteriza uma das maiores qualidades da *blockchain*: o fato de não haver um proprietário único da cadeia de informações. Essas redes costumam ser mantidas e utilizadas por uma única empresa, na qual apenas membros selecionados têm permissão para participar. Na prática, são ambientes restritos corporativos tradicionais, que se utilizam da segurança que as cadeias de blocos criptografados oferecem.

Um comparativo entre as três categorias de *blockchains* pode ser observado na Tabela 2, e suas propriedades são descritas a seguir:

Tabela 2 – Comparativo entre *blockchains*
Fonte: (ZHENG *et al.*, 2017)

Propriedade	**Tipo de *blockchain***		
	Pública	**Consórcio**	**Privada**
Determinação de consenso	Todos os nós	Conjunto de nós	Uma organização
Permissão de leitura	Pública	Pública ou restrita	Pública ou restrita
Eficiência	Baixa	Alta	Alta
Centralizada	Não	Parcialmente	Sim
Processo de consenso	Não permissionado	Permissionado	Permissionado

- **Determinação de consenso:** em uma *blockchain* pública, cada nó pode participar do processo de consenso. Em uma *blockchain* de consórcio somente um conjunto selecionado de nós é responsável por validar o bloco. Já na *blockchain* privada, esta é totalmente controlada por uma organização que determina o consenso final.
- **Permissão de leitura:** transações efetuadas em uma *blockchain* pública são visíveis a todos. As *blockchains* de consórcio e privada podem ou não serem visíveis, conforme suas configurações.

[1] https://bitcoin.org/en/
[2] https://ethereum.org/en/
[3] https://www.hyperledger.org

- **Eficiência:** em uma *blockchain* pública, devido ao grande número de nós que fazem parte da rede, a latência é alta. Por outro lado, nas *blockchains* privadas ou de consórcio, por possuírem menos validadores, a eficiência é um aspecto positivo.
- **Centralização:** uma *blockchain* pública é descentralizada, uma *blockchain* de consórcio é parcialmente centralizada e uma *blockchain* privada é totalmente centralizada.
- **Processo de consenso:** em uma *blockchain* pública, todos os nós da rede podem participar do processo, visto que não requer permissão. Em *blockchain* de consórcio ou privada, por serem controlados por uma ou mais organização, há determinação de quem pode participar do processo de consenso.

2.4.3 Arquitetura

A arquitetura de uma *blockchain* é formada por uma sequência de blocos que contêm uma lista completa de registros das transações em que cada bloco aponta para o bloco imediatamente anterior através de uma referência (*hash*) do bloco anterior. A Figura 4 ilustra um exemplo deste encadeamento.

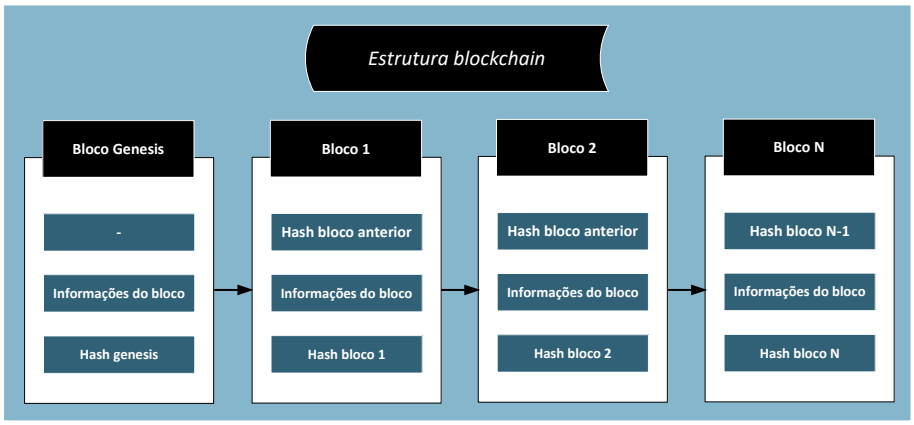


Figura 4 – Cadeia de blocos em uma rede *blockchain*.

Como cada bloco faz referência ao seu antecessor, se um bit do bloco anterior for alterado, seu *hash* irá mudar e, consequentemente, será necessário recalcular o *hash* de todos os blocos descendentes, fazendo com que o esforço de qualquer tentativa de mudança aos blocos cresça exponencialmente a cada bloco anterior que se tentar realizar a mudança. Por esse motivo, assume-se que a existência de uma cadeia longa torna o bloco imutável, garantindo a segurança das transações armazenadas (KOSBA *et al.*, 2016).

Um bloco é uma estrutura de dados que tem como dado principal uma lista de transações que será posteriormente incluído na *blockchain*. A estrutura do bloco consiste em duas partes, uma compreendendo o cabeçalho com todos os metadados

e a outra consistindo em todos os detalhes da transação, conforme ilustrado na Figura 5. Os atributos que compõem o cabeçalho do bloco são:

- **Versão do bloco:** a versão atual da estrutura do bloco.
- ***Hash* do bloco principal:** identificador único que corresponde a um valor de 256 *bits* que aponta para o bloco anterior.
- **Árvore de Merkle:** um *hash* criptográfico que resume todas as transações incluídas neste bloco.
- **Timestamp:** instante de tempo em que um bloco foi criado ou modificado.
- **nBits:** valor do *hash* atual em seu formato compactado.
- **Nonce:** número gerado de forma aleatória utilizado apenas uma vez. Inicia com o número 0 e aumenta a cada cálculo de *hash*.

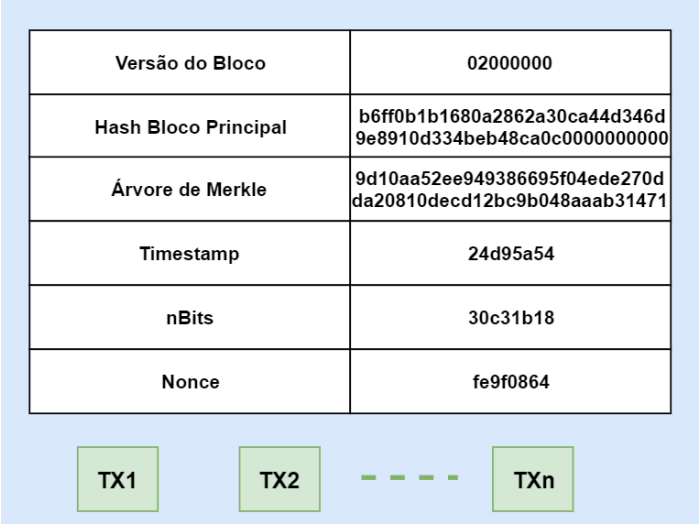


Figura 5 – Estrutura de um bloco.

Esses campos constituem o cabeçalho do bloco. O restante que compõe o bloco são as transações que serão armazenadas na *blockchain*. Os usuários criam transações e as enviam para a rede, onde ficam armazenadas em um *pool* esperando para serem incluídas posteriormente no bloco.

2.4.4 Mecanismos de Consenso

Chegar a um consenso em um ambiente distribuído, como ocorre em uma rede *blockchain*, torna-se um grande desafio, dado que, como não dependem de uma autoridade central, os elementos da rede precisam concordar na validação das transações (ZHENG *et al.*, 2017). Conforme (MINGXIAO *et al.*, 2017), mecanismos de consenso são sistemas compostos por algoritmos capazes de prover confiança a um serviço em que seus participantes não necessariamente confiam uns nos outros.

Todos os nós em uma rede *blockchain* criam e compartilham informações visando preservar esses dados com o uso de um conjunto de regras chamado protocolo de consenso. (KUDVA *et al.*, 2021) definem consenso como um mecanismo tolerante a falhas, o qual é utilizado para realizar a concordância necessária entre sistemas distribuídos de múltiplos nós.

Para atingir o consenso, pode-se usar diferentes algoritmos. Usar um algoritmo correto pode trazer um aumento significativo no desempenho da aplicação na *blockchain*. Há na literatura diversas metodologias de consenso que realizam o processo de validação. A seguir, são apresentados alguns dos principais mecanismos de consenso utilizados ou propostos em diferentes aplicações na *blockchain* (ZHENG *et al.*, 2016; CHALAEMWONGWAN; KURUTACH, 2018; KUDVA *et al.*, 2021):

2.4.4.1 Prova de Trabalho (PoW)

A PoW *(Proof of Work)* foi o primeiro protocolo de consenso distribuído utilizado para a criptomoeda *bitcoin* (NAKAMOTO, 2008), sendo ainda o mais aceito e adotado. Para se tornar um minerador da rede, um nó precisa realizar uma prova de trabalho, resolvendo um desafio criptográfico, o qual exigirá muito poder computacional.

Os nós da rede competem entre si para encontrar um *hash* com propriedades específicas e o nó que encontrar o desafio primeiro pode adicionar o novo bloco à *blockchain*. Entretanto, somente após a validação do bloco pelos mineradores que o bloco será adicionado à rede. Segundo (CACHIN, 2016), o maior problema do PoW refere-se à sua alta demanda por poder computacional para determinar a validade de uma solução para um problema. Esse mecanismo precisa ser aplicado com um alto nível de dificuldade na solução e com um baixo nível de dificuldade na verificação.

2.4.4.2 Prova de Participação (PoS)

Devido às desvantagens apresentadas pela PoW, a PoS *(Proof of Stake)* surgiu como uma abordagem alternativa, visando mitigar e resolver o problema de consumo energético, favorecendo decisões de consenso utilizando outros critérios. Nesse mecanismo, escolhe-se aleatoriamente um nó, o qual poderá criar um bloco novo. A probabilidade desse nó sair vitorioso baseia-se nos recursos que este tem na rede (TSCHORSCH; SCHEUERMANN, 2016). Os votos dos participantes para a eleição é ponderado pelo investimento já realizado na rede e o peso pode obedecer vários critérios.

Entende-se que os nós com mais participação na rede são os menos interessados em atacá-los (GAO; NOBUHARA, 2017). Sem a necessidade do alto custo computacional para o cálculo do *hash*, a PoS torna-se mais atraente quando comparada com o mecanismo PoW.

2.4.4.3 Prova de Autoridade (PoA)

Proposto em 2017 como parte do ecossistema *Ethereum*, o mecanismo de consenso PoA foi desenvolvido para redes permissionadas. Sua principal vantagem é o aumento de desempenho em comparação aos algoritmos BFT (*Byzantine Fault Tolerance*) típicos pois resulta em menos trocas de mensagens, introduzindo assim uma forma prática e eficiente para solucionar problemas com as redes *blockchain*.

Esse mecanismo é formado por um conjunto específico de nós de validação selecionados arbitrariamente como autoridades confiáveis responsáveis pela validação das transações. Os modelos baseados no PoA são altamente escaláveis, dado que estes não dependem de um grande número de validadores de bloco. Devido ao processo extremamente seletivo para a escolha dos validadores, tentar comprometer a rede torna-se uma tarefa difícil, visto que as reputações destes estão em risco (AN *et al.*, 2019).

2.4.4.4 Tolerância de Falhas Bizantinas Prática (PBFT)

Um caso particular de consenso bizantino, o conceito de PBFT (*Practical Byzantine Fault Tolerance*), originário do problema dos generais bizantinos, procura defender-se contra falhas do sistema mitigando a influência que os nós maliciosos têm sobre o funcionamento correto da rede e sobre o consenso correto alcançado pelos nós honestos no sistema. Desenvolvido para funcionar em sistemas assíncronos e otimizado para obter um alto desempenho em tempo de execução com baixo *overhead* e latência.

O modelo fornece uma replicação de máquina de estado bizantina que tolera falhas bizantinas (oriunda de nós maliciosos) pela hipótese de que existem falhas do nó e mensagens alteradas propagadas por nós específicos (CACHIN; VUKOLIĆ, 2017). Para o desempenho satisfatório do mecanismo, o número de nós maliciosos não deve ser igual ou exceder um terço de todos os nós da rede. Semelhante ao mecanismo PoW, quanto maior o número de nós em uma rede PBFT, mais segura esta rede se tornará (CASTRO; LISKOV *et al.*, 1999).

2.4.4.5 Prova de Participação Delegada (DPoS)

Considerado um mecanismo de consenso alternativo, o DPoS *(Delegated Proof of Stake)* foi implementado visando melhorar o desempenho da rede diminuindo o tempo de transação e geração dos blocos, além de ganhar flexibilidade, sem comprometer a estrutura descentralizada da rede *blockchain*. Nesse mecanismo, os nós da rede votam para eleger “delegados” e apenas os eleitos podem participar e contribuir para o processo de consenso para validação das transações e atualização da *blockchain*. A votação é um processo contínuo, pois os ”delegados” possuem incentivos

para realizar a sua função de maneira correta sob o risco de perderem sua reputação. No DPos, o fato de possuir um número reduzido de nós para validar o bloco leva a uma rápida confirmação das transações e uma baixa latência (BACH *et al.*, 2018).

2.4.4.6 Prova de Importância (PoI)

Implementado pela empresa NEM (*New Economy Movement*) (NEM, 2018), esse mecanismo associa um valor de importância a cada conta, criando assim um sistema de reputação na rede. As contas com pontuações mais altas possuem maior probabilidade de minerar o bloco.

Este mecanismo considera a importância dada a um minerador na rede com base no número de moedas que este possui, no número de transações realizadas, e na sua reputação na rede (REYNA *et al.*, 2018). Considerado uma extensão da PoS, foi desenvolvido para minimizar a desvantagem apresentado neste mecanismo, a centralização da riqueza.

Nesta seção foram citados alguns dos mais importantes mecanismos de consenso utilizados ou propostos na literatura. Como pode ser observado, nos últimos anos, a evolução das tecnologias *blockchain* veio acompanhada pelo desenvolvimento de diferentes mecanismos de consenso que ajudam a manter a consistência das informações registradas. Contudo, verifica-se que não existe um mecanismo que atue de maneira otimizada em todos os cenários nas quais a *blockchain* pode estar inserida.

2.4.5 Segurança em *Blockchain*

A tecnologia de *blockchain* oferece uma abordagem inovadora para armazenar informações, executar transações e funções e estabelecer confiança e segurança em um ambiente distribuído o qual pode facilitar um sistema de transporte inteligente, seguro, confiável e descentralizado. Embora essa tecnologia tenha recebido um interesse crescente na academia e na indústria nos últimos anos, a segurança e a privacidade continuam no centro dos estudos ao implantá-la em diferentes aplicações (ZHANG *et al.*, 2019).

Construída para garantir uma série de atributos de segurança intrínseca, como consistência, resistência à adulteração, à ataque distribuído de negação de serviço (DDoS) e a ataques de gasto duplo, o uso da tecnologia *blockchain* para um armazenamento distribuído torna necessário o uso de outros esquemas para garantir propriedades adicionais de segurança e privacidade.

Os autores (YANG, Z. *et al.*, 2017) definem a segurança na *blockchain* como a proteção de informações e dados de transações em um bloco contra ameaças internas e periféricas. A tecnologia *blockchain* utiliza-se de diversas técnicas para obter a

segurança dos dados e apoia-se fortemente na técnica de criptografia para satisfazer os requisitos de segurança do sistema e das aplicações, recorrendo a combinações de chave pública e privada para criptografar e descriptografar dados. Dentre os recursos mais utilizados, destacam-se os resumos criptográficos e as assinaturas digitais.

2.4.6 Poda na *Blockchain*

Um algoritmo de poda (*blockchain pruning*) é uma alternativa para exclusão de transações armazenadas na rede *blockchain* mantendo a sua funcionalidade e permitindo maior escalabilidade. Na remoção, as transações e blocos antigos são excluídos após um tempo predefinido, enquanto os cabeçalhos dos blocos antigos contendo a versão do *hash* são mantidos para garantir a integridade e segurança da *blockchain* (FINCK, 2018). Embora, originalmente, a remoção tenha por objetivo reduzir os requisitos de armazenamento da *blockchain*, pode-se também oferecer um maior nível de privacidade ao usuário, uma vez que transações antigas não podem ser mais localizáveis.

Embora possa haver maneiras de podar as transações, o exemplo do procedimento ilustrado pela Figura 6 substitui as transações por seus *hashes*. Em primeiro lugar, as transações que podem ser removidas da *blockchain* original são marcadas e, em seguida, as transações marcadas são substituídas por seus *hashes*. Dado que os *hashes* de transação são menores que as transações que as substituem, o tamanho da *blockchain* é reduzida.

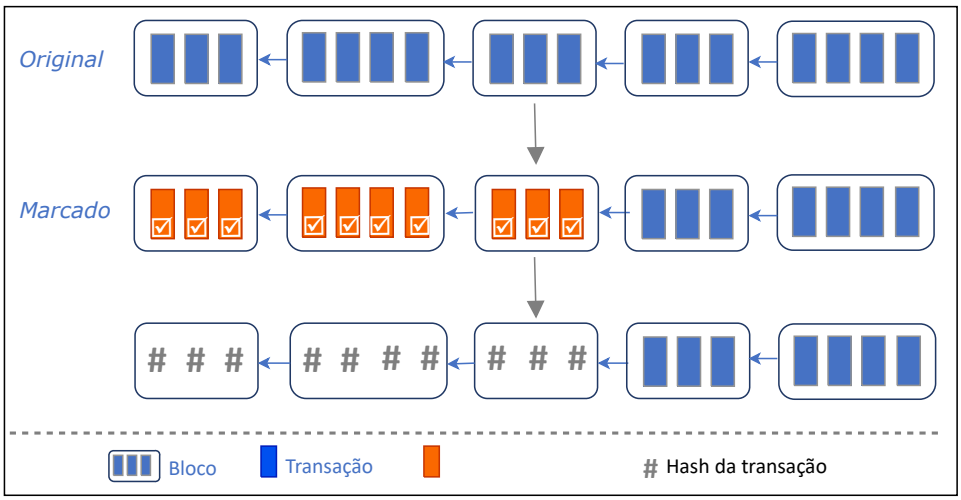


Figura 6 – Procedimento para substituir transações em bloco por seus *hashes*

Fonte: (PALM, 2017) adaptado.

A poda pode ser uma solução apropriada para estruturas de *blockchain* permissionadas onde o ambiente operacional é mais facilmente controlado e ajustado. No entanto, a ideia de poda em *blockchains* públicas permanece controversa, sendo atualmente um campo ativo de pesquisa (PALM, 2017).

2.4.7 *Blockchain* e sua integração em redes veiculares

Redes veiculares e *blockchain* são consideradas tecnologias emergentes na atualidade. Enquanto transformam conceitos e criam possibilidades novas, cada uma em seus respectivos cenários, existe a oportunidade de se criar aplicações que podem compartilhar as características intrínsecas de ambas, explorando formas de como as VANETs podem se beneficiar da natureza descentralizada das *blockchains*.

Mesclar a tecnologia de *blockchain* às redes veiculares é um desafio, sendo que essa integração desperta um crescente interesse de pesquisadores e desenvolvedores (KANG *et al.*, 2019). A *blockchain* pode oferecer soluções práticas para muitos problemas das redes veiculares (IQBAL *et al.*, 2019), especialmente aqueles relacionados à confiança para o compartilhamento e à disseminação de dados entre veículos. A ideia é de que os dados transmitidos pelos veículos conectados à *blockchain* sejam criptografados e assinados pelo verdadeiro remetente que contém uma chave pública exclusiva, garantindo a autenticidade, segurança dos dados transmitidos, bem como a sua confiança.

Os autores (HEIJDEN *et al.*, 2017) propuseram uma *blockchain* baseada em troca de mensagens e um sistema de revogação visando reduzir os requisitos de confianças dos usuários. (AWAIS HASSAN *et al.*, 2019) desenvolveram um mecanismo para criar, disseminar e proteger mensagens de alerta de emergência utilizando a tecnologia *blockchain*. Além das pesquisas citadas, os trabalhos relacionados apresentados na Seção 3 são exemplos de estudos do uso da *blockchain* com potencial para mudar significantemente a forma com que os dados são armazenados e distribuídos em aplicações dos STIs.

2.5 CONSIDERAÇÕES DO CAPÍTULO

Recentemente, a autonomia dos veículos foi aprimorada com a ajuda de várias técnicas de detecção, comunicação e análise de dados. Equipados com sensores, as informações internas e externas sobre um veículo podem ser enviadas para RSUs ou veículos próximos através de canais sem fio. Contudo, sem abordagens de segurança eficazes, os atacantes podem forjar ou manipular mensagens importantes e, eventualmente, prejudicar a segurança ou a eficiência de redes veiculares. Diante deste cenário, o uso de sistemas de gerenciamento de confiança e reputação podem auxiliar no desenvolvimento de um modelo com alta eficiência e dinâmica para as redes veiculares.

Conforme os conceitos apresentados neste capítulo, foi possível verificar que a tecnologia *blockchain* pode auxiliar na criação de sistemas e arquiteturas que garantam um gerenciamento de confiança altamente descentralizado, seguro e escalável nas redes veiculares.

O uso da tecnologia *blockchain* em redes veiculares vem ganhando muita atenção nos últimos anos. Seus principais cenários de uso estão em sistemas de gerenciamento de confiança para que trocas de mensagens ocorram de forma segura e na sua aplicabilidade para resolver problemas de anonimato e controle de acesso.

3 TRABALHOS RELACIONADOS

Este capítulo apresenta os trabalhos relacionados encontrados na literatura. São discutidas as propostas com mecanismos que utilizam modelos de confiança e também sistemas de reputação em redes veiculares que fazem uso da tecnologia *blockchain*. A Tabela 3 apresenta os trabalhos com as respectivas avaliações do veículo no qual cada um foi publicado, usando os sistemas de classificação Qualis-Periódicos[4] e do *Rank Scimago*[5].

Tabela 3 – Trabalhos selecionados

Trabalho	Ano	Journal/Conferência	Qualis	Rank Scimagojr
(ALHARTHI *et al.*)	2021	Journal	A2	Q1
(KHALID *et al.*)	2021	Journal	A1	Q1
(JAVAID *et al.*)	2020	Journal	B2	Q1
(SHRESTHA *et al.*)	2020	Journal	-	Q1
(TOMAR)	2020	Journal	-	Q3
(GAO *et al.*)	2019	Journal	A1	Q1
(YANG, Y.-T. *et al.*)	2019	Journal	A1	Q1
(KANG *et al.*)	2019	Journal	A1	Q1
(KANG *et al.*)	2018	Journal	A1	Q1
(KCHAOU *et al.*)	2018	Conferência	A2	-
(LU *et al.*)	2018	Journal	A1	Q1
(YANG, Z. *et al.*)	2017	Conferência	A2	-

Uma revisão sistemática da literatura (RSL) é uma metodologia para a realização de uma revisão bibliográfica por meio de etapas bem definidas e estruturadas que proporciona confiabilidade e base teórica (COLQUHOUN *et al.*, 2014). Desta forma, para a seleção dos trabalhos, foi realizada uma RSL e a descrição do procedimento de busca pode ser encontrada no Anexo A. Primeiramente, esse protocolo de busca foi executado no mês de julho de 2020 o qual resultou em um artigo publicado intitulado *"Blockchain e Sistemas de Reputação em Redes Veiculares: Uma Revisão Sistemática"*. Com o objetivo de identificar novos trabalhos este protocolo de busca foi novamente executado em dezembro de 2021.

Para obter a primeira lista de trabalhos possíveis, foi definida uma estratégia de busca combinando palavras-chave considerando às cinco fontes mais relevantes da área, sendo estas: *ACM Digital Library, IEEE Xplore, ScienceDirect, Scopus* e *Springer Link*. A Tabela 4 apresenta o total de publicações retornadas de cada base de dados. Critérios de inclusão e exclusão também foram pré-definidos, portanto, dos trabalhos encontrados, 57 foram removidos por publicações repetidas, *surveys*, não escritos em inglês, ou devido a uma limitação da ferramenta de busca da *Springer*

[4] https://sucupira.capes.gov.br/sucupira/public/
[5] https://www.scimagojr.com/

Link. Esta limitação resultou em um grande número de trabalhos, pois as palavras são encontradas em diversas partes do texto, que não satisfazem o contexto buscado devido ao ruído resultante.

Tabela 4 – Resultados da execução do protocolo de busca

	ACM Digital	IEEE	Science Direct	Scopus	Springer	Total
Resultado da string	5	14	4	26	30	**79**
Trabalhos repetidos	0	4	1	10	0	**15**
Trabalhos analisados	3	9	2	6	2	**22**
Trabalhos selecionados	2	8	2	0	0	**12**

Por fim, para refinar a seleção dos estudos, dos 79 artigos retornados dos resultados preliminares, 22 foram previamente analisados e todos foram lidos na íntegra para confirmar que responderam à questão de pesquisa. Portanto, 12 trabalhos foram selecionados e as informações extraídas.

3.1 REVISÃO DA LITERATURA

Os autores em (YANG, Z. *et al.*, 2017) propuseram um mecanismo de avaliação de confiança para a Internet de Veículos no qual a credibilidade das mensagens recebidas é avaliada com base na reputação de seu remetente, a partir das classificações dos veículos com base em mensagens históricas, e armazenada em uma *blockchain* pública. Como desvantagem, gerenciar uma *blockchain* em um veículo com recursos limitados incorre em custos significativos, especialmente ao usar algoritmo de consenso PoW, computacionalmente caro. Além disso, não foram realizadas simulações para demonstrar a viabilidade do *blockchain* nos veículos.

(LU *et al.*, 2018) apresentam um mecanismo de reputação que determina a confiança de um veículo por meio de suas interações. São usadas duas *blockchains* para registrar o fluxo de trabalho da AC e o histórico de todos os veículos separadamente, sendo que a primeira monitora a credibilidade da AC, e a segunda mantém a reputação dos nós do sistema e auxilia a AC na emissão de certificados. A chave pública é utilizada como pseudônimo nas comunicações, sem qualquer informação sobre a identidade real, para manter o anonimato do veículo, onde a chave é regularmente atualizada através da AC. No entanto, essa é uma abordagem difícil devido à sobrecarga da AC emitindo muitas chaves públicas.

Um sistema de gerenciamento de confiança que utiliza uma *blockchain* pública é proposto por (KCHAOU *et al.*, 2018) o qual visa estimar a credibilidade das mensagens divulgadas, com base no valor da reputação do remetente. As RSUs são responsáveis

pela formação do *cluster* em sua área geográfica e também são mineradores de dados da rede *blockchain*. Um líder é selecionado em cada *cluster* e define a credibilidade das mensagens com base nas informações de reputação do veículo. No entanto, é muito complexo manter um cluster de veículos adequado devido à comunicação de curta duração. Outro ponto é que não há implementações e simulações do sistema para avaliar seu desempenho.

(KANG *et al.*, 2018) empregam uma *blockchain* de consórcio e contratos inteligentes para construir um sistema seguro de compartilhamento de dados visando melhorar sua credibilidade. O sistema de reputação é implementado usando um modelo lógico subjetivo de três pesos. As RSUs formam a *blockchain* de consórcio e responsáveis por realizar o processo de consenso. Dois contratos inteligentes são empregados: um para armazenamento de dados e outro para compartilhamento de informações entre os veículos. No entanto, nas simulações realizadas, o processo de autenticação e segurança não obteve um bom desempenho na avaliação realizada em tempo real.

Um sistema de votação baseado em reputação de dois estágios, que visa garantir a seleção segura de mineradores na rede *blockchain* e a verificação do bloco, é apresentado em (KANG *et al.*, 2019). O sistema utiliza interações históricas e opiniões recomendadas de outros veículos para avaliar a reputação dos candidatos a mineradores (RSUs). O foco da proposta é tratar de RSUs maliciosas que podem modificar ou descartar dados durante o processo de mineração e, prevenir ataques de conluio. Porém, devido aos recursos limitados das redes veiculares, o custo de estabelecer uma blockchain pública é alto. Além disso, o sistema calcula a reputação do RSU com base em comunicações anteriores e opiniões de veículos. No entanto, a proposta não considera como verificar a confiabilidade dos dados enviados pelo veículo.

O sistema de (YANG, Y.-T. *et al.*, 2019) implementa um mecanismo projetado para garantir a confiabilidade dos eventos e confirmar a validade de suas ocorrências usando uma *blockchain* pública na qual os veículos podem validar mensagens recebidas usando um modelo de inferência bayesiana. Ao focar na confiabilidade da mensagem e confirmar a validade de suas ocorrências, os autores definiram um novo algoritmo de consenso chamado prova de evento (PoE). Entretanto, o mecanismo não considera o histórico dos veículos para reputação, apenas as notificações dos veículos adjacentes. Além disso, devido à utilização de uma *blockchain* global, que engloba uma grande área geográfica, a escalabilidade da *blockchain* pode ser comprometida.

Os autores em (GAO *et al.*, 2019) apresentam um modelo de confiança para impedir atividades maliciosas na rede veicular. Uma integração de redes definidas por software (SDN) e *blockchain* é proposta para roteamento de mensagens para garantir um gerenciamento de rede eficaz. Para reduzir os custos computacionais e atrasos,

foi implementada uma *blockchain* de consórcio para o compartilhamento de dados na rede veicular utilizando o padrão de comunicação 5G. Os veículos são agrupados em *clusters*, os quais possuem um líder, responsável pela verificação da confirmação dos alertas. Entretanto, um dos problemas de agrupamento é a utilização de um protocolo eficiente devido a restrições de mobilidade e, a escolha correta do líder e, no artigo, os autores não descrevem como é realizada a escolha do líder no *cluster*.

(TOMAR, 2020) propôs um mecanismo para tornar as informações nas redes veiculares mais confiáveis e identificar nós maliciosos. O sistema utiliza duas *blockchains*: uma no próprio veículo e outra na nuvem. Sempre que ingressarem na rede veicular ou quando mudam de região, os veículos recebem uma *blockchain* atualizada. Cada veículo é equipado com uma unidade de *blockchain* personalizada (BCU), sincronizada com a OBU onde ficam armazenadas as informações sobre eventos de alerta propagadas para os veículos vizinhos e, posteriormente, enviadas para uma RSU. A RSU consolida e analisa todas as transações recebidas sobre o mesmo evento. Assim, caso os dados enviados pelos veículos sejam iguais, a RSU assume que o evento aconteceu e incrementa as reputações dos veículos e as armazena na *blockchain* na nuvem. Nesse trabalho, o consumo de recursos computacionais ocasionados pelo armazenamento da *blockchain* nos veículos, bem como a sincronização da *blockchain* na nuvem, não foram considerados e avaliados.

(SHRESTHA *et al.*, 2020) integra um sistema de confiança onde a confiabilidade da mensagem e a dos nós são armazenadas em uma *blockchain* pública que utiliza servidores de borda para reduzir a latência na criação dos blocos.O sistema proposto também propõe manter uma *blockchain* separada com base na localização geográfica de cada país para melhorar a escalabilidade. Todos os veículos transmitem sua posição por meio de mensagens de *beacons* onde é gerado um certificado de localização disponibilizado por uma RSU, que atua como prova de localização que ajuda na identificação das mensagens de evento em uma determinada área geográfica. Entretanto, neste trabalho apenas são discutidas a escalabilidade e a sobrecarga de armazenamento da *blockchain*, mas não foi realizada nenhuma avaliação experimental.

Em (JAVAID *et al.*, 2020) é proposto um sistema de gerenciamento de confiança escalável baseado em uma *blockchain* pública para a Internet dos Veículos. Emprega contratos inteligentes com dispositivo PUF (*physical unclonable functions*) em substituição as chaves privadas para gerar os certificados (emitidos pelas RSUs). O sistema aplica um contrato inteligente que visa garantir o estabelecimento da confiança. Esse contrato interage diretamente com as RSUs para certificar que os dados gerados pelos veículos sejam provenientes de fonte confiável. O sistema adota um algoritmo de consenso dinâmico denominado dPoW (*dynamic Proof-of-Work*) executado pelas RSUs, o qual permite que o protocolo seja estendido conforme o fluxo de veículos na via. Em-

bora a integração entre PUFs e *blockchain* sejam promissores, resolver os problemas existentes em protocolos de autenticação é um desafio.

(KHALID *et al.*, 2021) apresentam um sistema de incentivos financeiros para veículos que cooperam fornecendo informações sobre incidentes e recorrendo à *blockchain* de consórcio e contratos inteligentes para validar esses eventos e calcular a reputação com base em eventos anteriores. O sistema adota um protocolo para armazenamento de arquivos distribuídos (IPFS) projetado para armazenar dados relacionados a incidentes na rodovia. Após a verificação de um evento, as RSUs armazenam as informações relacionadas a este em um *IPFS*, via contrato inteligente, e o valor da reputação do veículo na *blockchain*. Além disso, todos os incentivos e transações da autoridade certificadora também são armazenados na *blockchain*.

Os autores (ALHARTHI *et al.*, 2021) propuseram uma *blockchain* biométrica (BBC) na qual os recursos de biometria são combinados com a tecnologia *blockchain* para fornecer transmissão confiável de dados, rastreamento das mensagens trocadas, e identificação do veículo que propaga mensagens falsas na rede. No sistema, as informações biométricas servem para manter um registro da verdadeira identidade do emissor da mensagem, preservando a sua privacidade, além de garantir a credibilidade da mensagem. Para o registro do veículo na rede, uma AC coleta os dados biométricos do condutor e informações do veículo. O trabalho utiliza *blockchain* pública sendo um fator delimitador devido a sua complexidade e eficiência, principalmente quando implementadas em redes veiculares.

3.2 ANÁLISE DOS TRABALHO RELACIONADOS

Segundo o estudo realizado nesta seção, a Tabela 5 apresenta um resumo comparativo dos trabalhos selecionados na RSL, e inclui as seguintes características: (i) contribuição da solução proposta, (ii) a categoria *blockchain*, (iii) a localização da instalação de armazenamento da *blockchain*, e (iv) o processo de consenso.

Muitas das abordagens propostas implementam *blockchains* públicas (YANG, Z. *et al.*, 2017; LU *et al.*, 2018; KCHAOU *et al.*, 2018; KANG *et al.*, 2019; YANG, Y.-T. *et al.*, 2019; TOMAR, 2020; SHRESTHA *et al.*, 2020; JAVAID *et al.*, 2020; ALHARTHI *et al.*, 2021), sem restrições de acesso, descentralizadas e com a participação igualitária entre todos os membros. Contudo, devido aos recursos limitados da rede veicular e à instabilidade de comunicação entre os nós da rede, o custo de construção de uma *blockchain* pública é muito alto, dado que, os participantes da rede veicular precisam inicialmente baixar uma grande quantidade de dados da *blockchain*. Além disso, a questão de escalabilidade é também um grande desafio das *blockchains* públicas, exacerbando os problemas de custos de infraestrutura e atrasos nas transações.

Tabela 5 – Análise dos trabalhos relacionados (em ordem cronológica)

Autores	Contribuição	Categoria da Blockchain	Local da Blockchain	Processo de consenso
Yang et al. 2017	Evitar a geração de eventos falsos e garantir a credibilidade das mensagens.	Pública	Veículo	PoW/PoS
Lu et al. 2018	Garantir a privacidade dos veículos na rede com o uso de pseudônimos.	Pública	RSU	PoW
kchaou et al. 2018	Avaliar o comportamento dos veículos através de um gerenciamento de confiança distribuído.	Pública	RSU	PoW
kang et al. 2018	**Avaliar o comportamento dos veículos através de um gerenciamento de confiança distribuído.**	**Consórcio**	**RSU**	**PoS**
kang et al. 2019	Evitar conluio entre candidatos a mineradores por meio de um sistema de reputação.	Pública	RSU	PoS
Yang et al. 2019	Garantir a confiança e aumentar a segurança nas redes veiculares.	Pública	RSU	PoE
Gao et al. 2019	**Detectar e isolar nós maliciosos na rede veicular.**	**Consórcio**	**RSU**	**PBFT**
Tomar 2020	Aumentar a confiança dos usuários finais na rede veicular.	Pública	Veículo Nuvem	PoW
Shrestha et al. 2020	Avaliar a credibilidade da mensagem e veículos utilizando sistema de confiança.	Pública	Veículo RSU	PoW
Javaid et al. 2020	Garantir um gerenciamento de confiança escalável em um ambiente IoV.	Pública	RSU	dPoW
Alharthi, NI, Jiang 2021	Proteger o compartilhamento de dados entre veículos com o uso de blockchain biométrica.	Pública	Veículo RSU	PoW
Khalid et al. 2021	**Garantir a segurança contra ataques maliciosos através de incentivos.**	**Consórcio**	**RSU**	**PoW**
BRS4VANETs 2022	**Garantir a segurança contra ataques de mensagens falsas em redes veiculares.**	**Consórcio**	**RSU**	**PoA**

Nos trabalhos de (YANG, Z. *et al.*, 2017; TOMAR, 2020; SHRESTHA *et al.*, 2020; ALHARTHI *et al.*, 2021) os veículos armazenam todos os blocos como um nó completo, para poderem acessar diretamente a reputação do veículo e as mensagens de tráfego na rede *blockchain*. No entanto, quanto maior o número de transações, maior a demanda por recursos computacionais e maior o tempo de execução. Assim, os veículos são dispositivos com recursos limitados em termos de poder computacional e de armazenamento para manter uma *blockchain* e, não foram realizadas simulações nos trabalhos para demonstrar a viabilidade da *blockchain* nos veículos.

O mecanismo de consenso PoW foi utilizado nos trabalhos (YANG, Z. *et al.*, 2017; LU *et al.*, 2018; TOMAR, 2020; SHRESTHA *et al.*, 2020; ALHARTHI *et al.*, 2021; KHALID *et al.*, 2021), porém este protocolo é excessivo em recursos, em que cada minerador precisa investir grandes recursos computacionais. Além disso, à medida que mais veículos aderirem a *blockchain*, torna-se difícil chegar a um consenso para adicionar novos blocos. Outros trabalhos utilizam implementações alternativas, assim como implementações híbridas de consenso e alguns com estratégias totalmente novas que estão sendo constantemente desenvolvidas.

Todos os trabalhos analisados, envolvem avaliar o comportamento dos veículos ou RSUs, mas com foco em diferentes aspectos. Algumas soluções mitigam o problema do conluio (KANG *et al.*, 2018; JAVAID *et al.*, 2020). Em outras, a verificação de eventos por nós vizinhos não considera o histórico de reputação (YANG, Y.-T. *et al.*, 2019). Os autores (KCHAOU *et al.*, 2018; GAO *et al.*, 2019) não analisam o processo de formação de *cluster* entre veículos. Além disso, os trabalhos (KCHAOU *et al.*, 2018; SHRESTHA *et al.*, 2020; TOMAR, 2020) não possuem análise de simulação ou avaliação experimental.

Em alguns trabalhos, algumas questões ficaram em aberto e não foram bem discutidas. O problema voltado à preservação da privacidade não é tratado nos trabalhos de (YANG, Z. *et al.*, 2017; KCHAOU *et al.*, 2018). Além disso, a questão da latência e os custos computacionais do processo de consenso na *blockchain*, não são discutidos ou analisados de forma satisfatória em (YANG, Z. *et al.*, 2017; YANG, Y.-T. *et al.*, 2019; JAVAID *et al.*, 2020; KHALID *et al.*, 2021). Em (SHRESTHA *et al.*, 2020; TOMAR, 2020) não foram realizadas simulações para comprovar a eficácia do mecanismo da confiabilidade das mensagens e a latência pelo armazenamento dessas na *blockchain*.

Na Tabela 5 as abordagens que possuem características semelhantes e que mais se identificam com esse trabalho são destacadas em negrito: (KANG *et al.*, 2018), (GAO *et al.*, 2019) e (KHALID *et al.*, 2021). Uma análise comparativa frente ao BRS4VANETs é descrita a seguir.

No trabalho do (KANG *et al.*, 2018), os veículos fazem o papel de provedores de

dados cujo objetivo é selecionar fontes de dados mais confiáveis. Para isso, eles usam o mecanismo de consenso *PoS* baseado na riqueza ou participação do nó. Dessa forma, a seleção de mineradores com base nos nós mais ricos pode tornar um único nó responsável pela criação de todos os blocos, resultando em distribuição injusta ou eventual centralização. Em vez disso, o BRS4VANETs se concentra na detecção de veículos maliciosos e usa o mecanismo PoA, um protocolo simples que não requer nenhum poder computacional extenso, onde os participantes (RSUs) são conhecidos e há um grau de confiança entre esses.

No trabalho de (GAO *et al.*, 2019) diferente do BRS4VANETS, o objetivo do sistema de reputação está focado no uso de protocolos de roteamento para gerenciar e controlar a rede de forma eficaz e eficiente. Além disso, os veículos são agrupados em *clusters*. No entanto, a abordagem de *cluster* pode ser usada no gerenciamento de confiança em cenários limitados devido aos canais de comunicação de curta duração. Portanto, devido ao número limitado de veículos adjacentes, esse esquema não é adequado para cenários altamente móveis e esparsos.

Em (KHALID *et al.*, 2021) além do poder computacional significativo requerido pela adoção do mecanismo PoW, o próprio veículo emissor do alerta também é responsável por receber as validações/verificações dos veículos testemunhas e então enviar a RSU para ser armazenada na *blockchain*. A diferença é que no BRS4VANETs, o veículo que valida as mensagens as envia diretamente para a RSU mais próxima para evitar a modificação das informações durante a transmissão.

Por fim, todos os trabalhos não consideram em suas análises um cenário com fluxo veicular denso, conforme utilizado no BRS4VANETs, apenas com um número reduzido de veículos ((KANG *et al.*, 2018) — 100 veículos, (GAO *et al.*, 2019) — 40 veículos e (KHALID *et al.*, 2021) — 50 veículos).

Após a análise dos trabalhos previamente selecionados, fica claro que integrar novos mecanismos para tornar as redes veiculares mais seguras e confiáveis sem comprometer seu desempenho ou recursos computacionais continua sendo uma tarefa desafiadora.

Diferente dos demais trabalhos apresentados, um dos objetivos do BRS4VANETs é a divulgação de Alertas de Perigos Locais (LDW), cujo foco é distribuir informações sobre os eventos com precisão e com a menor atraso possível. Isso porque as mensagens de alerta são utilizadas para comunicar situações de risco na rodovia. É inevitável que haja atrasos na avaliação da confiança do nó usando *blockchain*. Primeiro, é necessário coletar evidências de outros veículos da rede por meio de mensagens de validação (WVM), depois agregar essas evidências e realizar cálculos com o auxílio de RSUs e, por fim, registrar a reputação na *blockchain*. Assim, foi introduzida uma lista de reputação contendo veículos considerados suspeitos

e maliciosos, propagados aos demais veículos previamente, antes do seu registro na *blockchain*. Essas decisões de projeto influenciaram a arquitetura do sistema BRS4VANETs, tornando-o escalável e com respostas rápidas à divulgação de alertas.

3.3 CONSIDERAÇÕES DO CAPÍTULO

Ao analisar as abordagens estudadas neste capítulo, percebe-se que a reputação e confiança podem ser utilizadas na concepção de mecanismos que possam fornecer serviços de forma segura. Em redes veiculares, devido à sua natureza dinâmica, podem existir veículos que nunca interagiram previamente. A utilização destes mecanismos pode fornecer uma avaliação preliminar de ações que podem ser executadas de modo seguro e confiável. Sendo assim, compreender os sistemas de reputação existentes, bem como avaliá-los e compará-los é um passo importante para a construção de novos modelos.

Este capítulo apresentou os trabalhos encontrados a partir de uma revisão sistemática da literatura e referenciados por diversos autores que procuram desenvolver mecanismos de reputação e confiança nas questões relacionadas a disseminação de dados seguros em redes veiculares com o emprego da tecnologia *blockchain*. Os trabalhos aqui pesquisados e descritos serviram de base e permitiram demonstrar que algumas limitações e questões ainda precisam ser abordadas para se alcançar um modelo de gerenciamento de confiança/reputação com alta eficiência e dinâmico para as redes veiculares.

4 BRS4VANETS: SISTEMA DE GERENCIAMENTO DE CONFIANÇA DESCENTRALIZADO PARA VANETS

Este capítulo apresenta o sistema proposto nesta tese, denominado BRS4VANEts, que visa analisar a confiança dos veículos em aplicações de segurança no trânsito de forma a identificar a presença de nós maliciosos, neutralizar suas ações e contribuir para tomada de decisões baseada no comportamento dos veículos. A Seção 4.1 apresenta uma visão geral do sistema e as suas premissas são apresentadas. Na Seção 4.2, o modelo da rede veicular é descrito, com os tipos de mensagens disseminadas na rede veicular. Na Seção 4.3, o Sistema de Gerenciamento proposto neste trabalho é detalhado. Por fim, são tecidas as considerações finais do capítulo.

4.1 VISÃO GERAL E PREMISSAS

Os elementos fundamentais de uma rede veicular são seus nós e o BRS4VANETs baseia-se em uma arquitetura híbrida de redes veiculares. Os nós são formados por RSUs e OBUs, os quais trocam mensagens entre si, conforme ilustrado na Figura 7. O padrão IEEE 802.11p WAVE é empregado como tecnologia de comunicação onde as RSUs, localizadas ao longo da rodovia, fornecem maior cobertura de comunicação e servem como nós de retransmissão para a disseminação de mensagens. Além disso, algumas informações são mantidas em um banco de dados distribuído baseado na tecnologia *blockchain* que estão nas RSUs.

O BRS4VANETs utiliza uma **estratégia investigativa** na qual a reputação do nó é avaliada consultando outros nós participantes da rede e adota uma **estratégia otimista** na qual os nós são confiáveis até que se prove em contrário.

Considera-se no BRS4VANETs, as seguintes premissas:

1. Cada veículo tem sua identidade definida de forma única na rede, cujo identificador é baseado na sua chave pública;
2. Os veículos participantes da rede possuem componentes que possibilitam a comunicação e a execução das aplicações, tais como, sensores, unidades de armazenamento, unidade de comunicação sem fio, sistema de posicionamento GPS e uma interface com o usuário para mostrar ao condutor as mensagens de alerta e a localização dos eventos reportados;
3. O GPS possui precisão suficiente para detectar a localização e o tempo exato do veículo na estrada.
4. Considera-se que os eventos são sempre detectados, de forma correta, pelos sensores dos veículos e também pelas RSUs. O funcionamento dos sensores e a tecnologia empregada estão fora do escopo deste trabalho;

5. A rede veicular recorre a uma infraestrutura de chave pública (ICP) e considera-se que cada veículo recebe previamente da Autoridade Certificadora (AC) seu certificado correspondente; e
6. As mensagens de alerta podem ser revogadas por unidades confiáveis, como, por exemplo, veículos da empresa concessionária da rodovia, câmeras instaladas, etc.

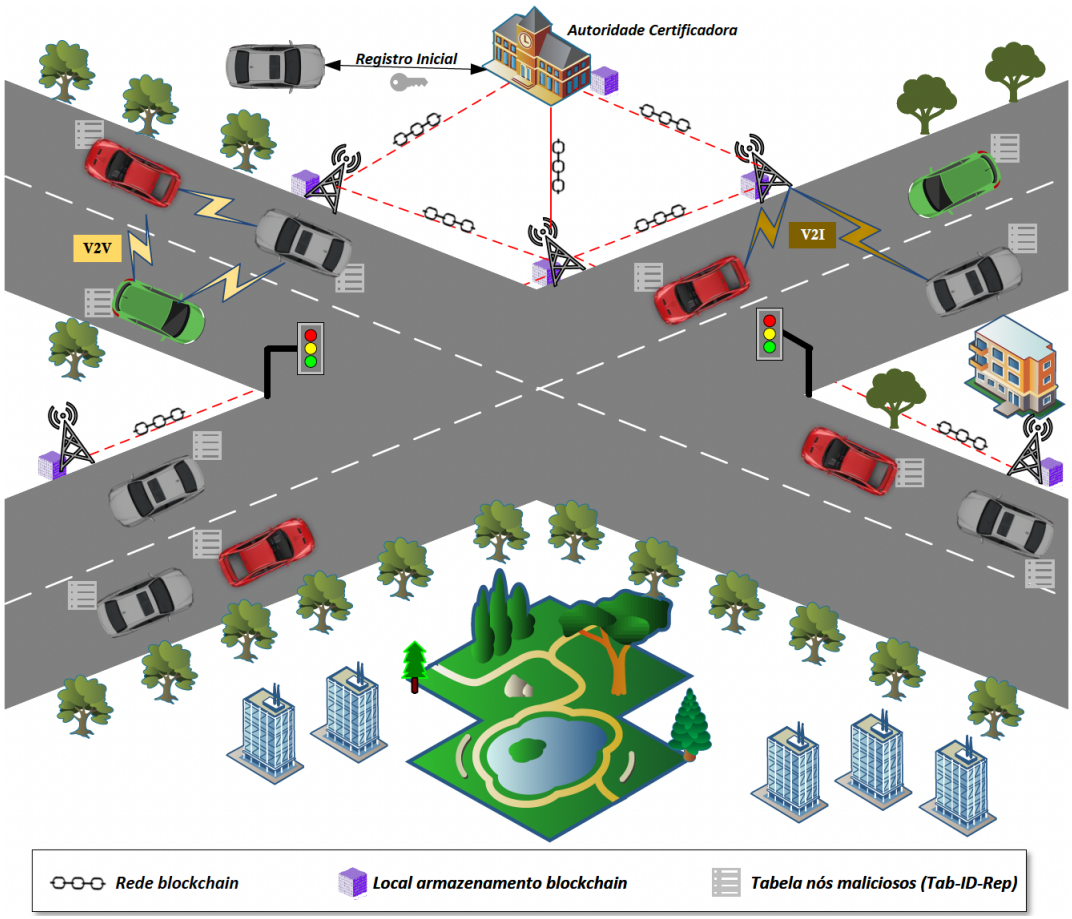


Figura 7 – Visão geral do BRS4VANETs.

O mecanismo BRS4VANETs é executado nas RSUs e veículos e tem como objetivo analisar a credibilidade dos nós e a confiabilidade da mensagem com base em um sistema de reputação para auxiliar na tomada de decisões, o qual será detalhado na Seção 4.3. Cada veículo recebe da RSU mais próxima, uma lista de reputação chamada *Tab-ID-Rep* contendo a relação dos veículos considerados maliciosos. Esses valores de reputação são posteriormente armazenados em uma *blockchain* de consórcio nas quais as transações são mais rápidas, possuem maior escalabilidade e armazenadas com integridade, transparência e segurança. Isso permite a construção de um sistema de gerenciamento de confiança distribuído e confiável baseado no uso de qualificações emitidas por terceiros, comprovando a confiabilidade de seus portadores.

4.2 MODELO DA REDE VEICULAR

No modelo da rede veicular proposto, os veículos e RSUs possuem uma identidade única na rede. Devido a restrições de tempo e de confiabilidade inerentes a aplicações STI, torna-se necessário um protocolo de roteamento eficiente para a disseminação das mensagens. Conforme (ETSI, 2011), o protocolo de roteamento *GeoNetworking* é adequado para redes cujos nós são altamente dinâmicos, como nas redes veiculares.

No protocolo *GeoNetworking*, cada nó deve informar aos vizinhos sobre sua presença, transmitindo periodicamente mensagens de *beacons* denominadas *geoNetworking beacons*. Com base nessas mensagens, o nó cria uma tabela de localização, contendo os nós a um salto de distância e pode ser consultada a qualquer momento para coletar informações como, por exemplo, velocidade e direção dos nós.

O BRS4VANETs adota o padrão IEEE 802.11p para a comunicação V2V e V2I. As RSUs, distribuídas ao longo da rodovia, estão interligadas entre si através de enlace de fibra óptica. Desta forma, as RSUs estendem o alcance de comunicação da rede veicular oferecendo um maior raio de cobertura para disseminação de mensagens. Estas são responsáveis também, pela criação e manutenção da *blockchain* na rede veicular e pelo cálculo da reputação dos veículos conforme descrito na Seção 4.3.3.

Os veículos são responsáveis pela disseminação das mensagens na rede e pela validação dos eventos ocorridos e propagados por outros veículos, contribuindo desta forma para o processo da composição da reputação. Entre as mensagens, destacam-se as mensagens de alerta (*Warning Message* – WM), transmitidas quando eventos críticos ocorrem na estrada. Outra mensagem disseminada é a mensagem de validação de alerta (*Warning Validation Message* – WVM), utilizada para validar a ocorrência dos eventos críticos relatados e para, posteriormente, identificar mensagens de alerta falsas propagadas por nós maliciosos.

As RSUs também propagam periodicamente mensagens de *beacons* aos veículos que estão no seu raio de cobertura. Essa troca de *beacons* permite que uma RSU notifique os veículos de sua presença e envie a *Tab-ID-Rep*. De forma similar, os veículos também propagam mensagens de *beacons* aos veículos vizinhos e RSUs.

Conforme ilustrado na Figura 8, além das RSUs e OBUs, o modelo de rede incorpora uma cadeia de ACs, organizadas de forma hierárquica para tratar eficientemente a emissão de certificados digitais utilizados pelos veículos. Esta hierarquia no BRS4VANETs é baseada em áreas, as quais são divididas em regiões. Cada região tem sua AC local e está ligada às demais regiões por meio da AC de área (raiz), com base em uma relação de confiança para realizar o processo de emissão e verificação dos certificados.

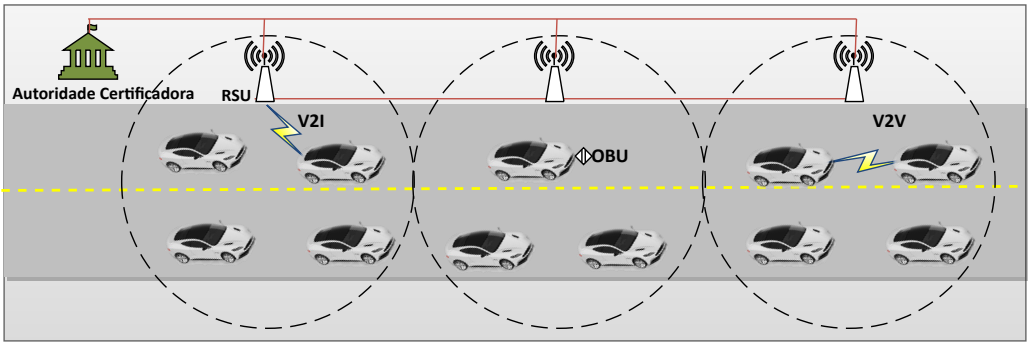


Figura 8 – Modelo da rede veicular.

Como descrito anteriormente, o padrão WAVE, além de ser um modo de operação do *IEEE 802.11p*, é composto por um conjunto de normas. Dentre elas, destaca-se a *IEEE 1609.2* que especifica um conjunto de serviços para prover segurança às mensagens WAVE contra análise de tráfego (*eavesdroping*), forjamento (*spoofing*) e outros tipos de ataques em ambientes de redes veiculares. O BRS4VANETs segue esta norma e adota o serviço de assinatura digital, que usa o padrão ECDSA (*Elliptic Curve Digital Signature Standard*), e os certificados digitais compactos especiais para comunicações veiculares.

A norma *IEEE 1609.2* trata dos serviços de segurança para as aplicações e gerenciamento das mensagens o qual define os métodos de processamento e o formato das mensagens de segurança utilizados pelos sistemas *WAVE* e *DSRC* mas não define como deve ser a identificação do veículo. Portanto, torna-se importante construir um sistema de gerenciamento de identidades para os veículos baseado na Entidade de Gerenciamento de Certificados definida na *IEEE 1609.2*. Para isso, o registro do veículo deverá ser feito junto a uma AC, por exemplo, um departamento de trânsito (DETRAN), para que o certificado digital seja emitido tendo como base o par de chaves gerado internamente na OBU do veículo. A revogação dos certificados decorrente da identificação de veículos com comportamentos maliciosos será realizada descentralizadamente e está descrita na Seção 4.3.4.

4.3 SISTEMA DE REPUTAÇÃO PROPOSTO — BRS4VANETS

O sistema de gerenciamento de confiança proposto é classificado como híbrido, visto que combina a avaliação da reputação de um nó e a confiabilidade das mensagens propagadas pelos veículos. Nesta proposta, para o cálculo da reputação de um veículo, são considerados como comportamentos maliciosos: (i) a propagação de mensagens falsas na rede (que podem ser comprovadas pelos nós vizinhos) e (ii) a modificação de mensagens propagadas na rede.

Cada veículo possui um valor de reputação que reflete o seu comportamento

na rede. As opiniões sobre o comportamento dos veículos são sinalizadas por veículos vizinhos que verificam a confiabilidade no nó e a credibilidade das mensagens de alerta geradas. A reputação de um veículo aumenta à medida que este se comporta de maneira correta, e diminui com suas ações maliciosas.

Como observado, a reputação do veículo varia ao longo do tempo e as RSUs são responsáveis por calcular e armazenar esses valores na *blockchain*. Como diferentes concessionárias podem gerenciar as RSUs ao longo do mesmo caminho, a *blockchain* desempenha um papel importante na manutenção da integridade das informações sobre reputação. Os veículos são responsáveis por validar os eventos publicados por outros veículos e aprimorar o processo de construção da reputação.

Além da reputação, a *blockchain* armazena e gerencia o histórico das mensagens enviadas pelos veículos que atestaram, confirmando ou não, o evento. Essa abordagem permite uma análise mais aprofundada do comportamento dos nós dentro de um determinado período. Sistemas de recompensa podem ser introduzidos para incentivar a cooperação entre os veículos para que os principais eventos possam ser validados na rodovia. Essas recompensas, as quais estão além do escopo desta tese, podem permitir, por exemplo, a redução de valores de pedágios ou impostos.

De modo a avaliar o nível de confiança do veículo, o limiar de reputação (*Th_Rep)* é uma variável parametrizável do sistema que reflete o menor valor de reputação de um veículo para que este ainda possa ser considerado confiável. Neste trabalho, assume-se que o valor de *Th_Rep* é 0.5. O BRS4VANETs segue uma abordagem otimista, ou seja, todo o veículo ao ingressar na rede pela primeira vez, terá seu valor de reputação inicial definido com o valor de *Th_Rep*.

O BRS4VANETs mantém uma lista de reputação denominada *Tab-ID-Rep*, distribuída pelas RSUs e armazenada no próprio veículo, para fins de consulta e verificação da reputação. A *Tab-ID-Rep* contém apenas os veículos considerados suspeitos ou maliciosos, ou seja, veículos com reputação abaixo de *Th_Rep*.

A arquitetura do BRS4VANETs consiste em três módulos. A Figura 9 ilustra a arquitetura do sistema de gerenciamento de confiança, com seus módulos e componentes, sendo descritos nas próximas subseções.

4.3.1 Módulo Registro do Veículo

Antes de ingressar na rede, cada veículo precisa ser registrado em uma AC. O processo de registro começa com o veículo, através de um canal de comunicação seguro, realizando uma solicitação de assinatura de certificado (*CSR - Certificate Signing Request*) para a AC contendo as credenciais do veículo, como sua identificação e o número do chassi, utilizadas para criar o certificado. Além disso, a solicitação contém a chave pública que será incluída em seu certificado digital, assinada com

Figura 9 – Módulos e componentes do BRS4VANETs.

a chave privada correspondente. A Figura 10 ilustra o processo de registro na rede veicular.

Durante o registro, a OBU do veículo gera o par de chaves pública e privada. A AC registrará o veículo e emitirá o certificado apenas se a informação for válida. Importante destacar que este procedimento deve ser efetuado de forma segura e por uma autoridade de trânsito que possa atestar o procedimento.

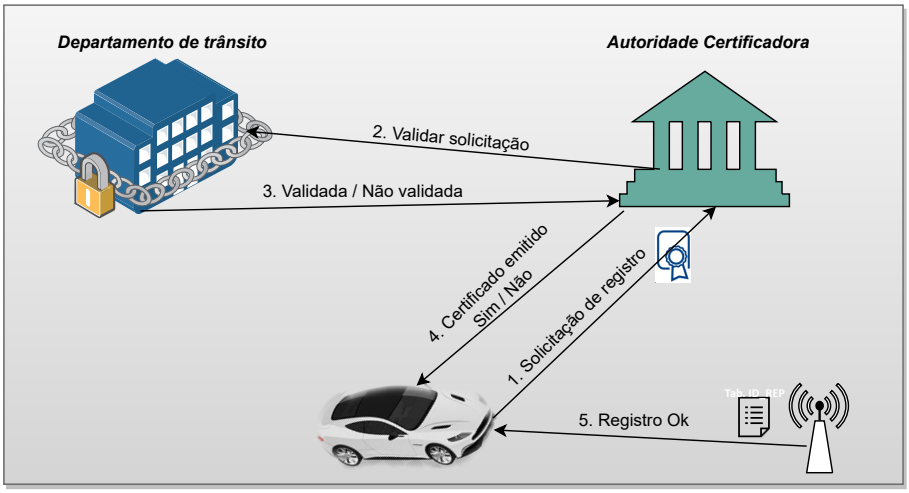


Figura 10 – Processo de registro na rede.

A privacidade dos condutores é garantida pelo uso da chave pública como pseudônimo para quebrar a correspondência com a identidade real do veículo. A chave fica armazenada na AC que atribui uma pseudo-identidade ao veículo e assim, durante o processo de geração do certificado apenas a pseudo-identidade é utilizada. Cada pseudo-identidade consiste em um número exclusivo para cada nó, e somente a CA conhece a identidade real associada à chave pública. Desta forma, o veículo pode ser identificado e seu certificado pode ser revogado pela AC caso se comporte de maneira maliciosa.

A identificação do veículo na rede também está associada a um contador de renovação (CR), responsável por contabilizar o número de vezes que o veículo foi registrado na rede. Portanto, uma vez excluído do processo de participação na rede veicular, por ações maliciosas, e ter o seu certificado revogado, o veículo pode tentar se registrar novamente na rede. Para isso, a sua identidade será verificada e se o seu CR for igual ou inferior a 3, será emitido um novo certificado. Isso permite ao veículo malicioso ingressar novamente na rede e ter possibilidade de corrigir o seu mau comportamento pregresso, por duas vezes.

Após o seu registro, a primeira vez que o veículo ingressar na rede veicular e estiver no raio de alcance de uma RSU, este recebe a lista de reputação dos veículos considerados suspeitos ou maliciosos (*Tab-ID-Rep*) da RSU mais próxima.

4.3.2 Módulo Gerenciamento das Mensagens

Toda vez que um sensor de um veículo detecta um evento em uma rodovia (Figura 11), o veículo verifica se é um evento já reportado ou trata-se de um novo evento. Caso o evento detectado não tenha sido relatado anteriormente, uma mensagem WM (*Warning Message*) é criada e propagada para informar o evento ocorrido. Caso o evento já tenha sido relatado, outros veículos validarão o alerta, por meio de uma mensagem WVM (*Warning Validation Message*) ao se aproximarem do local do incidente.

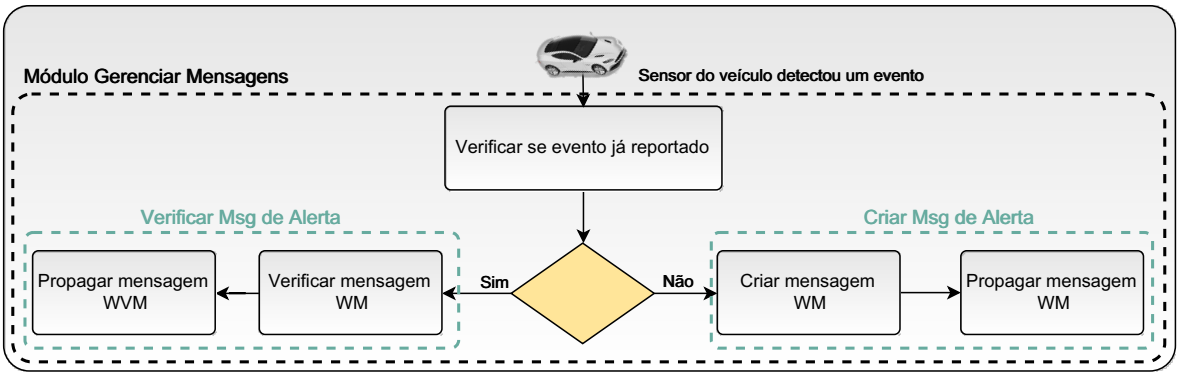


Figura 11 – Detecção do evento.

O módulo gerenciamento das mensagens é composto por três componentes: (i) criação de uma mensagem de alerta, (ii) verificação/validação desta mensagem e (iii) revogação da mensagem de alerta. Esses componentes são descritos a seguir.

4.3.2.1 Criar mensagem de alerta – WM

Sempre que um veículo detecta pela primeira vez um evento crítico na rodovia através de seus sensores, uma mensagem de alerta (WM) é propagada pela rede,

informando sobre o perigo. O Algoritmo 1 descreve o processo de criação desta mensagem de alerta e um exemplo do processo de disseminação da mensagem criada é ilustrado na Figura 12.

Algoritmo 1: Criação da Mensagem de Alerta – WM

início

se *veículo V com identificador* ID_V *e certificado digital* C_V *detectar evento novo* **então**

$ID_W \leftarrow$ Gera um identificador novo para o evento

$Crit_W \leftarrow$ Define a criticidade do evento cm base no sensor que capturou o evento

lat_V,$lon_V \leftarrow$ Obtém informações do GPS do veículo de latitude e longitude

TimeStamp $\leftarrow$ Obtém data e hora do evento

$ID_M \leftarrow$ Calcula hash (ID_W, $Crit_W$, ID_V,C_V, lat_V, lon_V, TimeStamp)

$Sign_M \leftarrow$ Assina(ID_M)

WM $\leftarrow$ CriaMsg(ID_M, Sig_M, ID_W, $Crit_W$, ID_V, C_V, lat_V, lon_V, TimeStamp)

Disseminar WM

fim

fim

Como pode ser observado no Algoritmo 1, cada evento possui um identificador próprio e criticidade associada. Se o sensor do veículo detecta um evento novo na estrada, ele obtém a localização e o momento exato do evento através do GPS. Após, calcula-se o *hash* do identificador único da mensagem o qual é assinada digitalmente. Por fim, com essas informações, é criada a mensagem de alerta a ser propagada na rede. Os campos que compõem a mensagem WM são indicados na Tabela 6.

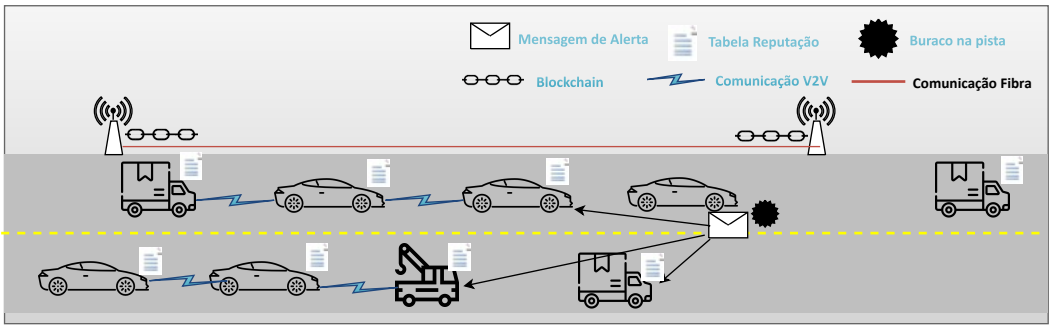


Figura 12 – Exemplo disseminação da WM.

Veículos próximos ao local do incidente relatado, após receberem a mensagem WM, consultam a reputação do veículo que emitiu o alerta via Tab-ID-Rep. Esse valor de reputação será utilizado para decidir se o alerta será exibido ao motorista. Mais detalhes sobre este processo são descritos na Seção 4.3.3.

Tabela 6 – Estrutura da Mensagem WM

Campos	**Descrições**
ID_M	Identificador único da mensagem gerado por uma função *hash*
Sign	Assinatura digital da mensagem de evento
ID_W	Identificador do evento de alerta
ID_V	Identificador do veículo emissor
T_A	Tipo do alerta
lat_V, lon_V	Coordenadas do GPS que indicam o local do evento ocorrido
TimeStamp	Data e hora em que o sensor detectou o evento
$Cert_V$	Certificado digital do veículo

4.3.2.2 Verificar Mensagem de Alerta – WVM

No BRS4VANETs, os veículos são responsáveis por monitorar e avaliar a confiabilidade dos eventos relatados em mensagens de alerta tendo como base um sistema votação que será detalhado na Seção 4.3.3. Para isso, torna-se necessário realizar uma análise prévia das mensagens de alerta (WM) propagadas.

O diagrama de atividades ilustrado na Figura 13 descreve os passos que devem ser executados para que os veículos avaliem o nível de confiança de quem gerou a mensagem de alerta, a partir do valor da reputação, e defina as ações a serem tomadas. As atividades executadas após o recebimento de uma mensagem de alerta WM são:

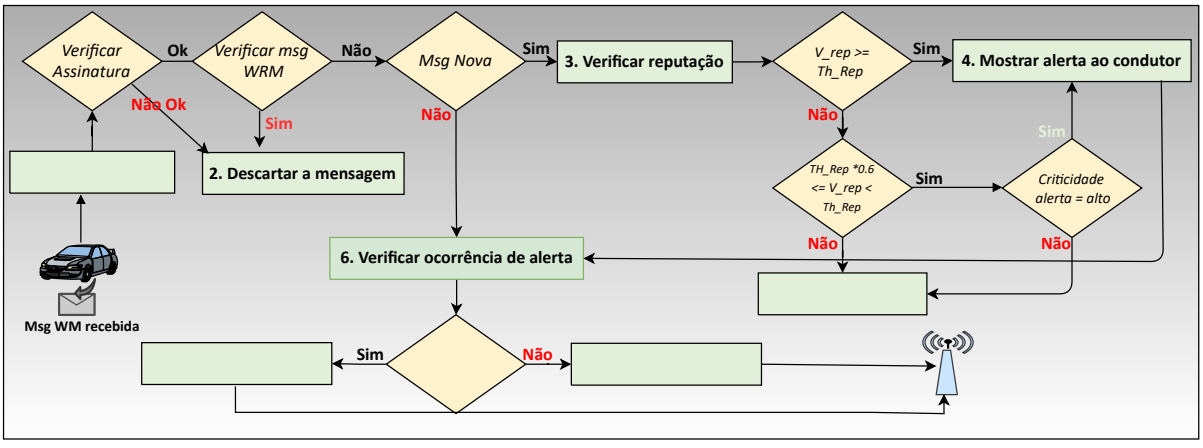


Figura 13 – Diagrama de tratamento da mensagem WM recebida.

1. **Analisar WM:** um veículo próximo ao local do evento, ao receber uma WM irá primeiramente obter o ID_m da mensagem de alerta e o ID_v do veículo que a gerou. Antes de propagar a mensagem na rede, ele verifica, através da assinatura

digital, a sua integridade, se possui uma mensagem de revogação (WRM) e também se trata de uma mensagem nova. Caso o veículo já tenha recebido esta mensagem, verificará a ocorrência do alerta.

2. **Descartar mensagem:** caso ocorra uma detecção de alteração da mensagem, o veículo que a recebeu a descarta devido à violação da integridade desta. Caso exista uma mensagem *WRM* a mensagem será também descartada.
3. **Verificar reputação:** ao receber a WM, o veículo consulta a reputação do nó emissor *V_rep* através da *Tab-ID-Rep* para avaliar a sua confiança e tomar decisões.
4. **Mostrar alerta ao condutor:** se a reputação do veículo for maior ou igual ao limiar de reputação *Th_rep*, este é considerado confiável e seu alerta é mostrado ao condutor. É importante notar que essa verificação é realizada de forma implícita, pois um veículo é confiável se não estiver incluído na *Tab-ID-Rep*, dado que somente veículos considerados suspeitos ou maliciosos são adicionados à tabela. Na situação em que a criticidade do alerta recebido for alta e a reputação do veículo for maior ou igual à 60% do valor de *Th_Rep* e menor que *Th_Rep*, a mensagem também será mostrada ao condutor, mesmo tratando-se de um veículo suspeito.
5. **Ignorar alerta:** os alertas serão ignorados quando os veículos forem categorizados como maliciosos na *Tab-ID-Rep*.
6. **Verificar ocorrência de alerta:** utilizado para que o veículo, ao aproximar-se do local do evento relatado na mensagem WM, verifique, por meio de seus sensores, a ocorrência (avalie a confiabilidade da mensagem de alerta).
7. **Enviar WVM (Ack):** caso o sensor do veículo detecte o evento ao passar pelo local do evento, o veículo envia uma WVM que confirma (Ack) a ocorrência do evento (campo denominado *Ack_Field*) para a RSU mais próxima, conforme pode ser observado no Algoritmo 2 e Figura 14.
8. **Enviar WVM (Nack):** caso o sensor do veículo não detecte o evento, o veículo envia uma WVM que indica a não ocorrência (Nack) do evento (campo denominado *Ack_Field*) para a RSU mais próxima, conforme pode ser observado no Algoritmo 2 e Figura 14.

Conforme descrito anteriormente, de modo a validar a ocorrência do evento recebida pelo veículo, é gerada uma mensagem WVM assinada digitalmente pelo receptor e os campos que a compõem a são mostrados na Tabela 7.

Algoritmo 2: Verificar Evento – WVM

```
início
    para cada WM recebida faça
        evento ← WM
        se ( evento=true ) então
            Ack_Field ← 1;   /* Usa campo da WVM para confirmar o evento */
        fim
        senão
            Ack_Field ← 0;   /* Usa campo da WVM para não confirmar o evento */
        fim
        Disseminar WVM;    /* Envia WVM à RSU mais próxima */
    fim
fim
```

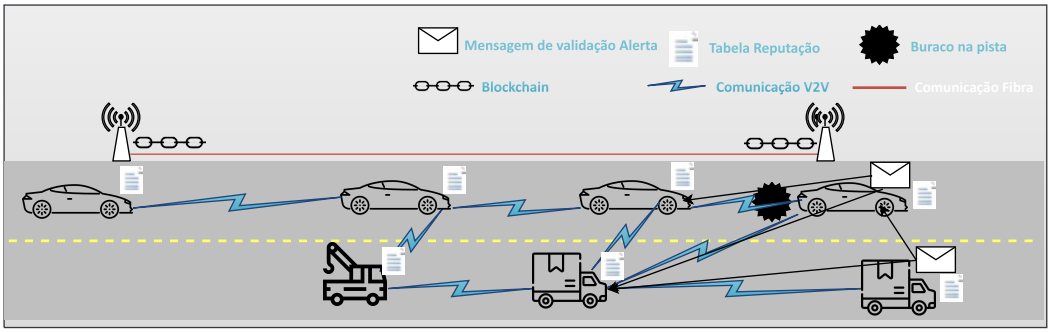


Figura 14 – Exemplo de disseminação da WVM.

Tabela 7 – Estrutura da Mensagem WVM

Campos	Descrições
ID_M	Identificador único da mensagem gerado por uma função *hash*
Sign	Assinatura digital da mensagem de validação
ID_W	Identificador do alerta
T_A	Tipo do alerta
Ack	Confirmação do evento ocorrido
Nack	Confirmação do evento não ocorrido
TimeStamp	Data e hora na qual o sensor atestou o evento

4.3.2.3 Criar mensagem de revogação de alerta – WRM

O BRS4VANETs também faz uso de mensagens de revogação de alerta (WRM), disseminadas por veículos de manutenção da concessionária ou por câmeras de vigilância. O objetivo dessa mensagem é informar aos veículos que receberam uma WM que o evento já foi revogado. Ou seja, o evento deixa de existir. Exemplos vão desde uma colisão entre veículos que já foram removidos por um guincho da concessionária da rodovia, até um animal que cruzou a rodovia, mas já foi retirado.

Quando um veículo recebe uma mensagem WRM, ele deve ignorar a respectiva

mensagem WM. O Algoritmo 3 descreve as atividades necessárias para criar uma WRM, assim como os campos que compõem a mensagem são apresentados na Tabela 8.

Algoritmo 3: Criação da Mensagem de Revogação de Alerta – *WRM*

```
início
    Ω: Veículos de manutenção da rodovia e Δ: câmeras de monitoramento da rodovia
    para cada WM recebida por Ω ou Δ faça
        /* Verifica localmente ou através das câmeras se o evento ainda é válido */
        Status.event ← Verifica WM
        se Status.event ≠ valido então
            TimeStamp ← Recebe data e hora atual
            ID_M ← Calcula hash (ID_W, TimeStamp)
            Sig ← Assina ID_M
            WRM ← CriaMsg(ID_M, Sig, ID_W, TimeStamp)
            Dissemina WRM
        fim
        senão
            /* Evento ainda válido. Não envia mensagem WRM */
        fim
    fim
fim
```

Tabela 8 – Estrutura da Mensagem WRM

Campos	Descrições
ID_M	Identificador único da mensagem gerado por uma função *hash*
Sign	Assinatura digital da mensagem de revogação
ID_W	Identificador do alerta
T_A	Tipo do alerta
TimeStamp	Data e hora em que a mensagem WRM foi gerada

4.3.3 Módulo Gerenciamento da Reputação

O módulo *gerenciamento da reputação* é executado nas RSUs para avaliar a mensagem de alerta WM e certificar de sua veracidade. Esse módulo utiliza um sistema de votação que leva em consideração as verificações de outros veículos para avaliar a confiabilidade do alerta. O sistema de votação visa aumentar a segurança das decisões tomadas dentro de um agrupamento de nós.

A RSU mais próxima consolida as informações recebidas nas mensagens WVMs. A agregação das WVMs recebidas é calculada pela Equação 1 e esse valor, chamado de NC_{msg} (Nível de confiança na mensagem), será armazenado posteriormente na *blockchain*.

$$NC_{msg} = \sum_{i=1}^{n} \frac{Ack}{Ack + Nack} \tag{1}$$

onde:

$$\begin{cases} se\ WVM\ for\ verdadeira,\ então\ \ Ack = Ack + 1 \\ se\ WVM\ for\ falsa, \qquad então\ Nack = Nack + 1 \end{cases}$$

As ações executadas pelas RSUs são mostradas no Algoritmo 4. Cada veículo tem um valor de reputação que reflete seu comportamento na rede. A reputação de um veículo aumenta se ele se comportar corretamente e diminui se realizar atividades maliciosas. As RSUs operam mesclando as "opiniões" recebidas dos veículos sobre a credibilidade da mensagem (através da Equação 1). Os resultados consolidados alteram a reputação do veículo que emitiu o alerta.

Algoritmo 4: Votação e atualização da reputação

```
início
    cont ← 0, Quorum ← 15, Ack ← 0, Nack ← 0
    para cada WVM recebida pela RSU faça
        cont ← cont+1
        se Ack_Field é 1 então
            Ack ← Ack +1      /* confirma o evento */
        fim
        senão
            Nack ← Nack +1    /* não confirma o evento */
        fim
        se cont ≥ Quorum então
            Calcula a Rep_New usando a Equação 1
            se (NC_msg ≥ 0.55) então
                /* A nova reputação do emissor do alerta é incrementada */
                status_evento ← Verdadeiro
                Calcula Rep_New usando a Equação 2
            fim
            se (NC_msg ≤ 0.45) então
                /* A nova reputação do emissor do alerta é decrementada */
                status_evento ← Falso
                Calcula Rep_New usando a Equação 3
            fim
            se (NC_msg > 0.45) e (NC_msg < 0.55) então
                /* Não há evidências conclusivas sobre o evento */
                /* Não calcula a nova reputação */
                status_evento ← Indefinido
            fim
        fim
    fim
fim
```

Com o objetivo de aumentar a segurança das decisões tomadas, o BRS4VANETs possui um mecanismo de votação que mitiga os efeitos de ataques de conluio por veículos maliciosos. Após receber um determinado número de

votos (O quorum foi definido como 15 no algoritmo, mas parametrizável no sistema), a RSU, dentro do seu raio de cobertura, consolida o resultado da votação e algumas ações são tomadas. Se uma porcentagem razoável de veículos (0,55 ou mais no algoritmo) validar o evento de mensagem de alerta, este é considerado **Verdadeiro** e a pontuação da reputação do veículo emissor do alerta é aumentada. Se uma pequena parte dos veículos (0,45 ou menos) validar o alerta, este é considerado **Falso** (*bogus*) e a pontuação da reputação do veículo é reduzida. No entanto, se o número total de veículos que validaram o evento como Verdadeiro for próximo daqueles que o validaram como Falso, este é considerado como **Indefinido**, pois não há evidências suficientes para validá-lo. Assim, a RSU não altera a reputação. Caso a pontuação de reputação do veículo tenha sido alterada, ela será posteriormente registrada na *blockchain*.

Após o procedimento do sistema de votação, se o evento for confirmado, o valor da reputação do veículo que emite a mensagem de alerta será incrementado, conforme indicado na Equação 2 e armazenado na *blockchain* para disseminação aos veículos na rede veicular.

$$Rep_{New} = Min(1, Rep_{cur} + ((Rep_{cur} * NC_{msg}) * \alpha)) \tag{2}$$

onde Rep_{cur} representa a reputação atual do veículo que emite o alerta, α é um valor no intervalo entre (0,1] que denota um fator de incremento dependendo da criticidade da mensagem propagada e Rep_{New} representa a nova reputação do veículo.

Por outro lado, se uma pequena parte dos veículos confirmar o evento, o valor da reputação do veículo que emite a mensagem de alerta será reduzido, conforme representado pela Equação 3.

$$Rep_{New} = Max(0, Rep_{cur} - ((1 - NC_{msg}) * \beta * FM_V)) \tag{3}$$

onde β é um valor no intervalo (0,1] que denota um fator de decremento dependendo da criticidade da mensagem propagada, e FM_V representa o número de vezes que o veículo enviou mensagens falsas de alerta em uma determinada janela de tempo, o que pode ser parametrizado no sistema (por exemplo, 1 a 3 anos).

Caso não haja evidências suficientes para validar o evento relatado, ou seja, o total do número de *Ack* e *NAck* são próximos, não há alteração na reputação do veículo.

Os veículos são incentivados a enviar mensagens de validação de eventos. Os veículos que atestam corretamente as mensagens de alerta às RSUs, por meio das WVM, ganham benefícios e têm seus valores de reputação aumentados, conforme

expresso na Equação 4.

$$Rep_{New} = Min(1, Rep_{cur} + (T_{WVM} * \gamma)) \quad (4)$$

onde na Equação 4, T_{WVM} corresponde ao número total de mensagens validadas corretamente pelo veículo e γ, um valor no intervalo (0,1], que representa uma constante de ganho o qual possui um valor parametrizável, independente da criticidade da mensagem atestada.

A Tabela 9 apresenta os valores de ganho utilizados neste trabalho e aplicados nas equações 2, 3 e 4 para incremento e decremento dos valores de reputação. Esses valores são associados conforme a criticidade do evento.

Tabela 9 – Incremento e decremento dos valores de ganho – *WM* e *WVM*

Criticidade mensagem	**Baixa**	**Média**	**Alta**
Ganho α	0,020	0,040	0,060
Ganho β	0,010	0,030	0,050
Ganho γ	0,001	0,001	0,001

Segundo (CUNHA, A. L. *et al.*, 2009), a calibração de um modelo matemático se refere ao processo de ajuste de parâmetros deste modelo para que esse consiga representar a área em estudo de uma forma adequada, coerente com a realidade observada. Assim, calibração dos valores de ganho para o incremento de decremento das mensagens WM e WVM, foi realizada através da simulação com diferentes valores de ganho, o qual encontra-se no Anexo A e fazendo os ajustes necessários para sua calibração.

O BRS4VANETs diminui a reputação de um veículo que divulga mensagens falsas e aumenta gradativamente sua reputação quando divulga mensagens verdadeiras. Adota uma abordagem otimista, em que sempre que um veículo se junta à rede pela primeira vez, sua reputação inicial é definida para o valor limite de reputação (*Th_Rep*).

O veículo que recebe uma WM, a mostrará ao motorista ou a ignorará, dependendo da sua importância e da reputação do veículo que emitiu o alerta. O Algoritmo 5 descreve as principais etapas seguidas nesta tomada de decisão.

Algoritmo 5: Tomada de decisão para uma WM recebida

```
início
    Tab-ID-Rep: Tabela de reputação recebida das RSUs pelos veículos
    para cada WM recebida faça
        Crit_Msg ← Criticidade da WM
        V_rep ← Tab-ID-Rep
        se ( V_rep ≥ Th_Rep ) então
            Mostra alerta ao motorista    /* Veículo considerado confiável */
        fim
        se ( (Crit_Msg=high) and ((Th_Rep * 0.6) < V_rep < Th_Rep) ) então
            Mostra alerta ao motorista   /* Veículo considerado suspeito e criticidade alta */
        fim
        /* Caso contrário, alerta é ignorado e não mostrado ao motorista */
    fim
fim
```

Veículos com reputação maior ou igual a *Th_Rep* são considerados confiáveis. Os demais veículos podem ser categorizados em dois tipos: suspeitos ou maliciosos. Um veículo é considerado suspeito quando sua reputação está na faixa de 60% a 100% do limite da reputação. Veículos com reputação inferior a esta faixa são considerados maliciosos.

4.3.4 Neutralizar Veículo Malicioso

Em muitos trabalhos encontrados na literatura, a revogação de certificados é uma forma de exclusão do veículo na rede, de modo que suas mensagens sejam ignoradas, sendo as AC responsáveis por propagar na rede a revogação de certificados inválidos. Entretanto, soluções baseadas em AC centralizadas necessitam alto poder computacional no processo de verificação diante a uma grande cadeia de regiões, além da dificuldade, visto que a distribuição dessas listas deve cobrir todas as regiões, pois os veículos se movem de uma região para outra.

Devido a esse problema, o BRS4VANETs, adota uma abordagem descentralizada para a revogação dos certificados, nas quais as RSUs são responsáveis pela tomada de decisão da exclusão do nó por mau comportamento (veículo malicioso). A AC é utilizada para realizar a revogação, contudo, a decisão e a execução do processo de eliminação são efetuadas pelas RSUs. Este processo é conhecido como exclusão de nós (*node eviction*), e possui diversas fases, como detectar o veículo com mau comportamento, relatar o mau comportamento, revogar o certificado (função das ACs) e disseminar a informação na rede.

4.3.5 Sistema de *Blockchain*

Os sistemas que utilizam a tecnologia *blockchain* apresentam problemas de escalabilidade que dificultam seu uso em diversas aplicações. Dentre essas questões, destacam-se: baixo *throughput*, alto custo da transação e armazenamento necessário para a cópia da *blockchain*. O tempo de transação também é um problema, relacionado à frequência com que novos blocos de transações são criados.

Assim, o BRS4VANETs recorre a uma *blockchain* de consórcio, denominada *Reputation-BC*, e emprega contratos inteligentes, como pode ser observado na Figura 15, pois oferece alto grau de segurança em ambientes de compartilhamento de dados e incorre em menores custos nos processos de mineração. Em uma *blockchain* de consórcio, um conjunto selecionado de nós é responsável por validar e manter os dados compartilhados e distribuídos. Na *Reputation-BC*, os nós pré-selecionados são as RSUs, as quais têm o direito de controlar o processo de consenso e escrever na *blockchain* veicular, além de serem responsáveis por compartilhar o valor da reputação dos veículos sem depender de terceiros confiáveis.

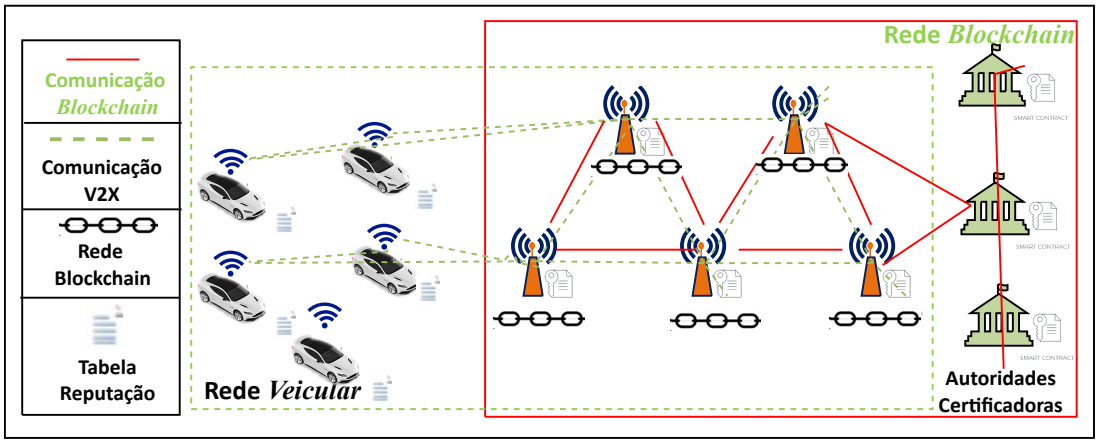


Figura 15 – Arquitetura geral da Reputation-BC.

Informações sobre um incidente, como congestionamentos ou acidentes rodoviários, são relevantes para uma determinada localização geográfica, não sendo de interesse para outras regiões. Desta forma, o BRS4VANETs adota uma *blockchain* local que registra apenas as reputações e histórico dos veículos em uma determinada rodovia e assim mitiga os problemas de escalabilidade da rede.

Uma das razões de implementar a *blockchain* apenas em RSUs é que os veículos geralmente possuem recursos limitados em termos de capacidade de armazenamento e processamento. Os veículos da rede veicular cumprem apenas o papel de mensageiros externos e retransmissores de mensagens ao relatar ou atestar eventos na estrada.

Como redes *blockchain* formam um grande ambiente distribuído, é um grande

desafio chegar a um consenso. Os diferentes membros da rede precisam concordar na validação das transações. Como as RSUs são semi confiáveis, pois são controladas por várias concessionárias da rodovia, assumimos um protocolo de consenso mais simples. Por esta razão, o BRS4VANETs adota um algoritmo PoA no consenso devido ao seu desempenho, quando usado em redes permissionadas, visto que há um número reduzido de troca de mensagens e menor *overhead*.

Os protocolos de consenso PoA funcionam quando os participantes se conhecem e há um certo nível de confiança entre eles. O IBFT foi criado para fornecer um protocolo de consenso alternativo para o protocolo *blockchain Ethereum* de uso instantâneo que é mais adequado para blockchains privadas e de consórcio, onde o esforço computacional para alcançar o consenso não é necessário. O IBFT faz parte de uma família de protocolos de consenso do PoA na qual apenas um conjunto especial de nós chamados validadores está autorizado a propor novos blocos. No IBFT, nenhum cliente envia uma requisição para a rede, ao invés disso, todos os validadores podem, propor um bloco.

A *Reputation-BC* é responsável por registrar e armazenar os valores de reputação dos veículos que fazem parte da rede veicular. Todas as informações contidas na *blockchain* são armazenadas e compartilhadas através da RSU. A *Reputation-BC* também armazena e gerencia o histórico das mensagens referente ao comportamento do veículo no tratamento das mensagens de alerta. Para garantir evidências permanentes, as mensagens referentes a comportamentos maliciosos são registradas na *blockchain*. A Tabela 10 mostra a estrutura dos campos de cada bloco.

Tabela 10 – Estrutura de um bloco do Reputation-BC

Campos	**Descrições**	**Tamanho**
Index	Índice sequencial único para cada bloco	24 bits
TimeStamp	Data e hora da criação do bloco	32 bits
Hash	*Hash* gerado para o bloco	256 bits
Pre-Hash	*Hash* do bloco anterior	256 bits
ID_v	Identificação do veículo	64 bits
ID_M	Identificação da mensagem	16 bits
Alert type	Identificação do tipo de alerta	16 bits
Reputation	Reputação do veículo	8 bits
Ack	Total de eventos *ACKs*	40 bits
Nack	Total de eventos *NACKs*	40 bits

4.4 CONSIDERAÇÕES DO CAPÍTULO

Um dos desafios encontrados nas redes veiculares é a inserção de novos mecanismos para prover segurança aos condutores dos veículos, como a disseminação de mensagens de alerta. Entretanto, uma das ações necessárias é a de analisar a confiança dos veículos propagadores de alertas. Sistemas de gerenciamento de confiança baseados em reputação surgem como mecanismo relevante por fornecer serviços que buscam tornar mais segura a disseminação das mensagens.

Este capítulo descreveu o sistema de gerenciamento proposto que utiliza a tecnologia de *blockchain* de consórcio e visa avaliar o nível de confiança de maneira distribuída entre os membros da rede veicular. As premissas a serem adotadas, o detalhamento do modelo de rede e funcionamento do sistema foram definidos e especificados. Os métodos para o cálculo da reputação e avaliação do nível de confiança também foram descritos.

5 EXPERIMENTOS E RESULTADOS

Este capítulo descreve o projeto experimental empregado para avaliar a solução e realiza uma análise dos resultados da simulação. A avaliação teve como objetivo detectar ataques falsos, tendo em vista tanto a sua eficiência na utilização dos recursos como a sua eficácia na detecção de veículos maliciosos. A Seção 5.1 apresenta as condições onde as simulações foram realizadas, a Seção 5.2 as métricas de desempenho adotadas e, por fim, a Seção 5.3 descreve os resultados da simulação.

5.1 AMBIENTE DE SIMULAÇÃO

Para a implementação de tecnologias em redes veiculares, há um conjunto de abordagens avaliativas que podem ser empregadas que vão desde coletas e análises de dados, passando por simulações até experimentos no mundo real (KILLAT *et al.*, 2007). Segundo (CHENG *et al.*, 2015), para se avaliar o funcionamento de simulações em redes veiculares, é necessário integrar um conjunto de *softwares* que incorporem o aspecto de arquitetura de redes de comunicações juntamente com *softwares* que produzam a mobilidade e a aleatoriedade existente em ambientes veiculares.

A utilização de ferramentas de simulação foi a abordagem experimental escolhida por este trabalho para o experimento do sistema de gerenciamento de confiança proposto. Além disso, a utilização de simuladores permite um controle melhor sobre o ambiente, como a repetição dos experimentos considerando diferentes cenários (por exemplo, o fluxo de veículos em uma rodovia).

5.1.1 Simulador de Rede

O simulador de rede baseado em eventos OMNeT++ foi usado para os experimentos. Trata-se de um simulador de eventos discretos, extensível, modular e baseado em componentes C++, para modelagem de redes de comunicação e há adaptabilidade às diversas plataformas de sistemas operacionais. Entretanto, protocolos e padrões de comunicação não são implementados pelo OMNeT++ e sim por módulos adicionais acoplados ao simulador.

A escolha por este simulador é devido à possibilidade do uso de *frameworks* específicos para redes veiculares e sua ampla utilização no meio acadêmico. Outro fator importante para a escolha, é a capacidade de poder trabalhar bidirecionalmente acoplado com geradores de tráfegos, facilitando as simulações mais detalhadas sobre os efeitos de determinados parâmetros sobre o tráfego na rede.

5.1.2 Simulador de Tráfego

Os *softwares* de simulação de tráfego são utilizados em sistemas de transportes essenciais para a mobilidade e ajudam a descrever o desenho do trânsito rodoviário ou urbano da forma eficiente. Assim, para garantir que as simulações fossem conduzidas de maneira mais realista, foi utilizado o framework SUMO (*Simulation of Urban Mobility*) acoplado bidirecionalmente ao OMNeT++. O SUMO destaca-se ainda por permitir a realização de ultrapassagens, sempre que a via da esquerda esteja livre, retornando a sua faixa logo após a ultrapassagem.

Os principais fatores que justificam a escolha da ferramenta se deve a possibilidade de utilização de traços reais de mobilidade, propiciando simulações mais detalhadas sobre os efeitos de determinados parâmetros sobre o tráfego na rede, além de ser amplamente utilizado em pesquisas acadêmicas na área de redes veiculares. A Figura 16 ilustra o cenário utilizado no framework SUMO para as rotas simuladas.

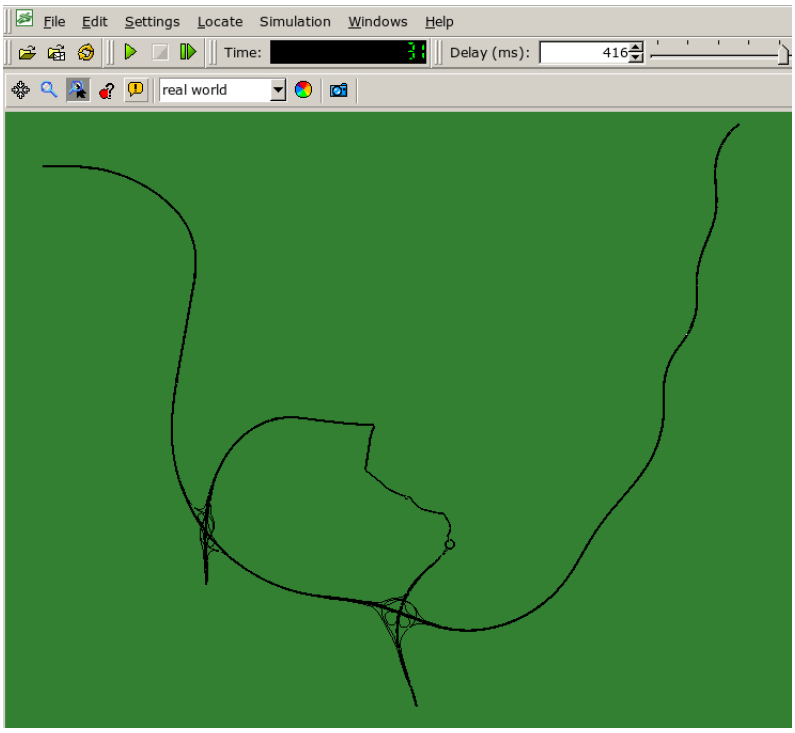


Figura 16 – Trajeto das rotas simuladas convertidos para o SUMO.

5.1.3 *Framework* para o acoplamento bidirecional

Um dos módulos adicionais do simulador OMNeT++ é o Artery, um *framework open source* que contém bibliotecas para execução de simulações de redes veiculares. As interfaces do OMNeT++ e do SUMO podem ser utilizadas em conjunto com o Artery, permitindo a configuração do modelo de maneira mais rápida e a execução de simulações interativas.

O *framework* possui o módulo de mobilidade (*Mobility*) ligado ao SUMO (*Road Traffic Simulation*) através de uma interface de controle de tráfego (*TraCI*) que utiliza uma porta TCP para comunicação. Isto faz com que cada simulação de rede veicular no Artery execute os dois simuladores em paralelo: OMNeT++ e SUMO.

O Artery também utiliza uma relevante coleção de módulos aplicados em suas simulações de redes veiculares. Estes módulos servem como base para a construção de uma simulação específica, utilizando apenas aqueles relevantes para o cenário concebido. O modelo de propagação *Two-Ray Interference* foi também usado, pois consegue capturar tanto a atenuação do sinal quanto os efeitos da reflexão do solo.

5.1.4 Parâmetros do Ambiente Computacional

Todas as simulações realizadas durante o desenvolvimento deste trabalho foram executadas em uma máquina equipada com um processador Intel Core I5 de terceira geração com dois núcleos, cada um com *clock* de 3,2 GHz, 16GB de memória RAM e sistema operacional Ubuntu 18.04.6 LTS de 64 bits.

5.1.5 Parâmetros de Simulação e Mobilidade

O Artery implementa o padrão *IEEE 802.11p* e os modelos de camada superior da pilha *IEEE 1609.4 DSRC/WAVE*. No SUMO, a única categoria de veículo definida foi ”carros”; suas principais características são baseadas em cenários reais de estradas (por exemplo, velocidade máxima, comprimento do veículo e aceleração). A Tabela 11 mostra os principais parâmetros de rede utilizados na simulação.

Tabela 11 – Parâmetros da simulação

Parâmetro	**Valor**	**Parâmetro**	**Valor**
MAC	IEEE 802.11p	Frequência do rádio	5.9 GHz
Tempo de simulação	900 s	Potência do rádio	25 mW
Tempo de Warmup	200 s	Tamanho do beacon	32 bytes
Repetições	30	Intervalo envio beacons	3 s
Modelo de propagação	Two-ray interference	Força do sinal	2 mW

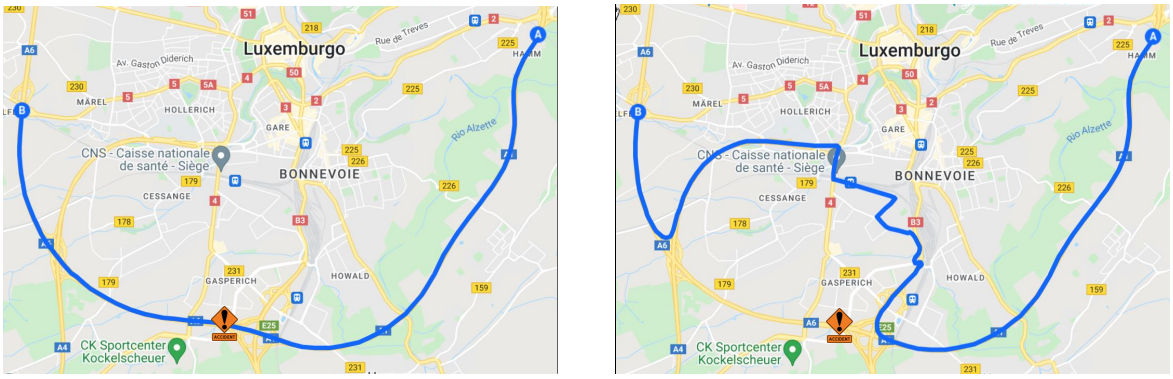
O cenário de mobilidade utilizado foi dividido em três fases: (i) inicialmente, selecionou-se a via de circulação dos veículos, utilizando-se o gerador de tráfego SUMO com o LuST (*Luxembourg SUMO Traffic*); (ii) em seguida, foram testados diferentes horários do dia para extração do fluxo de veículos; e (iii) finalmente, foram definidos os cenários de mobilidade necessários para as simulações. Na Tabela 12 são apresentados os três fluxos de tráfego definidos em nossos experimentos: esparso, normal e denso.

Tabela 12 – Características dos cenários simulados

Cenário	Horário	Nós/900s	Nós/hora	Nós/minuto
Esparso	5 h	250	1.000	16,6
Normal	14 h	625	2.500	41,6
Denso	8 h	1.000	4.000	66,6

No que diz respeito à implementação do ambiente de testes na *blockchain*, o *smart contract* (Apêndice B) foi desenvolvido na plataforma *Hyperledger Besu*[1] no qual foi utilizada a linguagem de programação *Solidity*[2] com o *framework Truffle*[3]. De modo a compilar e implementar chamadas de funções, foi utilizada a *IDE Remix*[4]. No entanto, devido a algumas limitações e dificuldades na interface de conexão do protocolo RPC (*Remote Procedure Call*) nos módulos, a plataforma *Hyperledger Besu* não foi integrada ao simulador de rede OMNeT++, as simulações foram implementadas separadamente.

Para reproduzir padrões de mobilidade que refletem uma demanda real de tráfego, foi usado o gerador de tráfego projetado especificamente para a cidade de Luxemburgo: LuST (CODECA *et al.*, 2017). Este gerador de tráfego inclui dados de tráfego de 24 horas em uma área de 155,95 km^2. No entanto, o estudo ficou restrito a um ambiente mais controlado, pois a divulgação da mensagem de alerta é importante apenas para veículos próximos ao local do incidente, e uma determinada região desse cenário foi escolhida.



(a) normal (11.58 km) (b) com desvio (15 km)

Figura 17 – Rotas simuladas | Fonte: Google Maps.

Neste recorte da região escolhida, a estrada possui 11,58 km de extensão, conforme ilustrado na Figura 17(a), e consiste em uma pista dupla com três faixas em cada sentido, perfazendo um total de seis faixas, com limite de velocidade máxima

[1] https://www.hyperledger.org/use/besu
[2] https://soliditylang.org/
[3] https://trufflesuite.com/
[4] https://remix.ethereum.org/

de 130 km/h. Nesta mesma região, uma rota alternativa foi definida quando a estrada for bloqueada parcialmente, com 15 km de extensão (Figura 17(b)). Nota-se que o aumento da extensão total do itinerário é de 3,42 km, mas a extensão do percurso alternativo por estradas secundárias é maior (cerca de 7,3 km), e também que a velocidade média dos veículos deste percurso alternativo é muito inferior que a velocidade da rota normal.

Ao longo da rodovia existem sete RSUs localizadas em intervalos de 2 km (com exceção da última que fica no final da rota simulada), interligadas por fibra ótica. Estas são responsáveis por calcular a reputação, transmitir mensagens de alerta aos veículos e pelo armazenamento da *blockchain*. Foi definido um evento falso de bloqueio parcial de duas faixas da rodovia, disseminado por um veículo malicioso, localizada na posição 7,5 km. Antes deste local, na posição 6,3 km, é possível sair da rodovia por desvio (Figura 17(b)). A Tabela 13 apresenta os parâmetros de simulação da rodovia utilizados.

Tabela 13 – Parâmetros de simulação da rodovia

Parâmetros	**Valor**	**Parâmetros**	**Valor**
Comprimento da rota simulada	11,58 km	RSU_4 posição	6 km
Comprimento da rota com desvio	15 km	Posição do desvio	6,3 km
Números de RSUs	7	Posição do evento falso	7,5 km
RSU_1 posição	0 km	RSU_5 posição	8 km
RSU_2 posição	2 km	RSU_6 posição	10 km
RSU_3 posição	4 km	RSU_7 posição	11,5 km

5.2 MÉTRICAS DE DESEMPENHO

Os sistemas, incluindo as redes veiculares, precisam ser avaliados com base em métricas de desempenho. As seguintes métricas foram utilizadas para determinar o comportamento da rede, avaliar os impactos dos ataques e verificar a eficácia do BRS4VANETs na detecção de nós maliciosos:

- **Tempo do Aumento da Viagem (TAV**): corresponde ao aumento do tempo de viagem do veículo causado pela emissão de um alerta falso.

$$TAV = \mid T_{rotaAlternativa} - T_{rotaNormal} \mid \tag{5}$$

  onde $T_{rotaAlternativa}$ corresponde ao tempo médio gasto de viagem pela rota alternativa (Figura 17(b)) e $T_{rotaNomral}$ o tempo médio gasto de viagem pelos veículos seguindo a rota normal (Figura 17(a)).

- **Taxa de Redução de Velocidade (TRV)**: refere-se à redução da velocidade média dos veículos, desde o recebimento da mensagem de alerta até o final do

trecho simulado.

$$TRV = (1 - (SFW/SRT)) * 100 \quad (6)$$

onde *SFW* é a velocidade média dos veículos após a divulgação de uma mensagem falsa e *SRT* é a velocidade média dos veículos em trânsito regular.

- **Mudança de rota do veículo (MRV)**: corresponde à taxa de veículos que mudaram sua rota após receber uma mensagem de alerta falso.

$$MRV = ((RM - PL)/RM) * 100 \quad (7)$$

onde *RM* é o número total de veículos que receberam uma mensagem de alerta e *PL* o número de veículos que passaram pelo local do evento relatado.

- **Incremento do Número de Mensagens (INM)**: corresponde à taxa do aumento do número de mensagens enviadas como o uso do sistema de reputação.

$$INM = ((NMR - NM)/NM) * 100 \quad (8)$$

onde *NMR* é o número de mensagens sem o mecanismo de reputação e *NM* é o aumento de mensagens causadas pelo sistema de reputação.

- **Tamanho do Armazenamento da *Blockchain* (TAB)**: permite fazer uma análise dos custos decorrentes do crescimento da *blockchain* causado pelos blocos gravados para armazenar reputações e seu histórico de mensagens.

$$TAB = NB * (EB + (TWM * 9) + (TWVM * 10)) \quad (9)$$

onde *NB* é o número de blocos criados, *EB* é o tamanho de um bloco vazio (sem *payload*), *TWM* o número total de mensagens de alerta e *TWVM* o número total de mensagens atestadas. Os valores 9 e 10 da fórmula referem-se aos tamanhos do *payload* das mensagens *WM* e WVM, respectivamente.

- **Taxa de Falso-negativos (TFN):** corresponde à taxa do número de veículos que identificaram erroneamente um nó malicioso como confiável.

$$TFN = MT/RM * 100 \quad (10)$$

onde MT é o número de nós que confiaram na mensagem recebida e RM é o número de nós na rede veicular que receberam a mensagem.

- **Taxa de Falso-positivos (TFP):** representa a taxa do número de nós que identificaram como sendo malicioso um nó não malicioso em relação ao número total de nós da rede veicular. No BRS4VANETs, esses valores tendem a zero. Isso ocorre porque o sistema adota uma abordagem otimista, assumindo que os nós desconhecidos são sempre confiáveis.

5.3 ANÁLISE DOS RESULTADOS

Nesta seção, os resultados da simulação são analisados em diferentes cenários de tráfego, onde há a propagação de uma mensagem de alerta falso sobre um bloqueio parcial da via. Para obtenção destes resultados, foram realizadas 30 simulações para cada cenário e uma média aritmética simples dos resultados de cada cenário foi calculada. Todos os resultados apresentados dos experimentos possuem 95% de intervalo de confiança. Conforme já descrito anteriormente, foi considerado um tempo de simulação de 15 minutos (900 segundos).

Dois cenários de rede foram implementados em nossos experimentos e explicados com mais detalhes na próxima subseção:

- **Cenário para análise do mecanismo de reputação:** nesse cenário, o objetivo foi determinar os impactos causados pela disseminação de informações falsas sem a utilização de um sistema de reputação, e também tentar estimar os *overheads* quando do uso do sistema na rede veicular.
- **Cenário para análise de falso-negativos:** Nesse outro cenário, o objetivo foi analisar a mudança de comportamento de um veículo que vinha agindo maliciosamente por um certo período e verificar sua correta identificação e o descarte das mensagens enviadas por este veículo.

5.3.1 Cenário para análise do mecanismo de reputação

Inicialmente, os experimentos foram realizados em um caminho livre com tráfego regular; em seguida, os experimentos foram repetidos com a propagação de uma mensagem falsa, com e sem o uso do sistema de reputação, para avaliar seu impacto no sistema. Neste caso, o veículo que emite a mensagem tem o valor de reputação definido como *Th_Rep* no sistema de reputação. Nas tabelas 14 e 15, os resultados são exibidos para uma distância de 11,58 km no trecho normal da via, ou 15 km quando do desvio de alguns veículos pela rota alternativa.

Tabela 14 – Redução da velocidade e o atraso causado por uma mensagem falsa

	Tráfego Regular		**Impacto da mensagem falsa sem sistema de reputação**			**Impacto da mensagem falsa com sistema de reputação**		
Fluxo	**Velocidade**	**Tempo**	**Velocidade**	**Tempo**	**TAV**	**Velocidade**	**Tempo**	**TAV**
Esparso	120,1 km/h	347,1 s	91,3 km/h	577,4 s	230,3 s	117,5 km/h	355,2 s	8,1 s
Normal	117,2 km/h	355,8 s	89,4 km/h	597,7 s	241,9 s	112,7 km/h	370,1 s	14,3 s
Denso	108,9 km/h	382,8 s	77,0 km/h	682,1 s	299,3 s	103,2 km/h	404,9 s	22,1 s

Note-se nas tabelas 14 e 15 que o impacto causado pela velocidade média dos veículos e os desvios com o sistema de reputação são menores que sem o sistema

de reputação. É possível verificar também que em todos os fluxos simulados houve redução na velocidade média, com maior impacto em cenários com maior fluxo de veículos. Com isso, há um aumento no tempo de viagem do trecho simulado. No caso dos veículos que alteraram a rota, o número é menor à medida que o fluxo de tráfego aumenta. A razão para isso é que, com o fluxo maior de veículos, após o recebimento da mensagem, há um número significativo de veículos que já passaram pelo local do desvio e estão em velocidade reduzida.

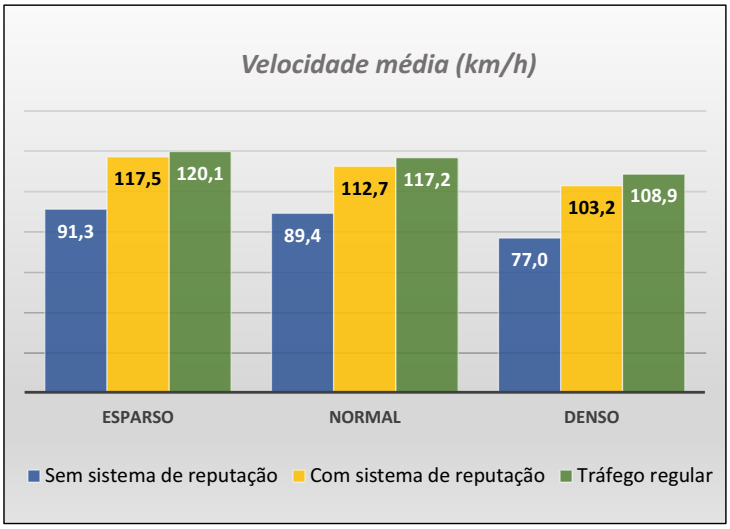
Tabela 15 – Redução da velocidade e o atraso causado por uma mensagem falsa

	Impacto da mensagem falsa sem sistema de reputação		**Impacto da mensagem falsa com sistema de reputação**	
Fluxo	**TRV**	**MRV**	**TRV**	**MRV**
Esparso	24,0%	92,7%	2,2%	4,4%
Normal	27,6%	80,9%	3,8%	3,2%
Denso	29,3%	50,1%	5,2%	2,2%

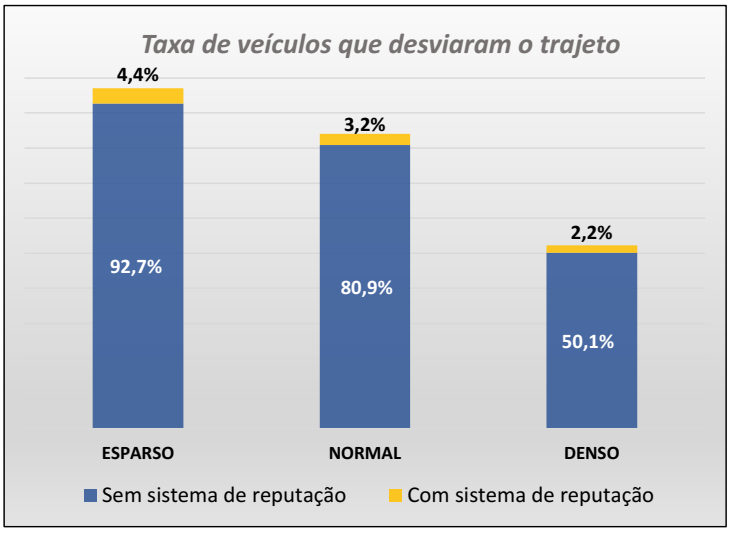
Como pode ser observado na Figura 18(a), o impacto de uma mensagem falsa é mais significativo em um sistema sem mecanismo de reputação. As maiores reduções de velocidade ocorrem no tráfego denso quando a redução de velocidade em cenários sem sistema de reputação é superior a 29% (redução de 108,9 para 77 km/h). Ao contrário, com o sistema de reputação, a redução foi de apenas 5,2% (redução para 103,2 km/h). A Figura 18(b) mostra que o sistema de reputação reduz bastante o número de veículos que são forçados a desviar a rota devido à mensagem falsa.

Entre os veículos que confiaram na mensagem falsa, aqueles que tomaram o trajeto alternativo, tiveram um aumento significativo no tempo decorrido. Enquanto o aumento de um caminho desviado é de cerca de 29,5%, o acréscimo do tempo de viagem é maior devido ao aumento da distância percorrida em vias urbanas e em velocidades mais baixas. Por exemplo, em um tráfego regular sem desvio, o tempo médio é de 361,9 s; porém, quando há desvio, esse tempo sobe para 619,1 s, ou seja, um aumento de mais de 70%.

A Figura 19 ilustra o intervalo de tempo necessário para se detectar um veículo malicioso em três fluxos diferentes. Como pode ser observado, 300 segundos após o início da simulação, um veículo malicioso com reputação igual a *Th_Rep* propaga uma mensagem falsa (*WM*) sobre um engarrafamento na rodovia. Os veículos que recebem esta mensagem reduzem a velocidade e, após passarem pela área do evento, enviam uma *WVM*, notificando de que não houve tal incidente. Após a RSU ter recebido a *WVM* de no mínimo quinze veículos, ela calcula a nova reputação do veículo que enviou a mensagem falsa, a armazena na *blockchain* e transmite a nova lista de reputação aos veículos. Com base nesta informação, os demais veículos, conseguem desconsiderar a mensagem falsa após recebê-la, podendo retornar à velocidade normal na rodovia.



(a) Velocidade média em diferentes fluxos de tráfego que incluem: uma mensagem falsa em um cenário sem sistema de reputação, uma mensagem falsa em um cenário com sistema de reputação, e tráfego regular (sem mensagem falsa).

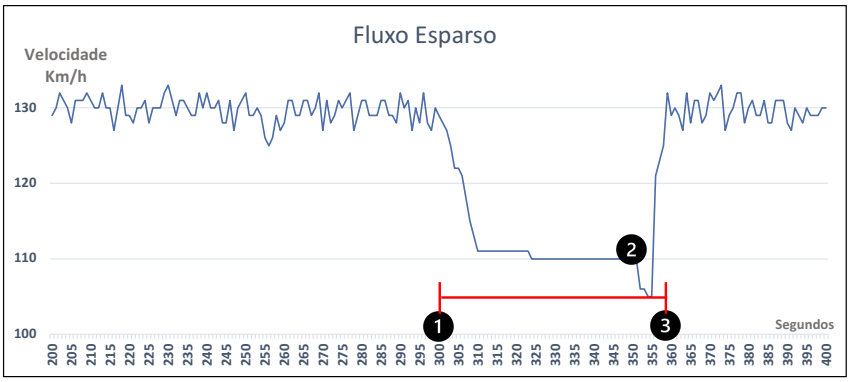


(b) Comparação da taxa de veículos desviados em diferentes fluxos de tráfego com e sem sistema de reputação.

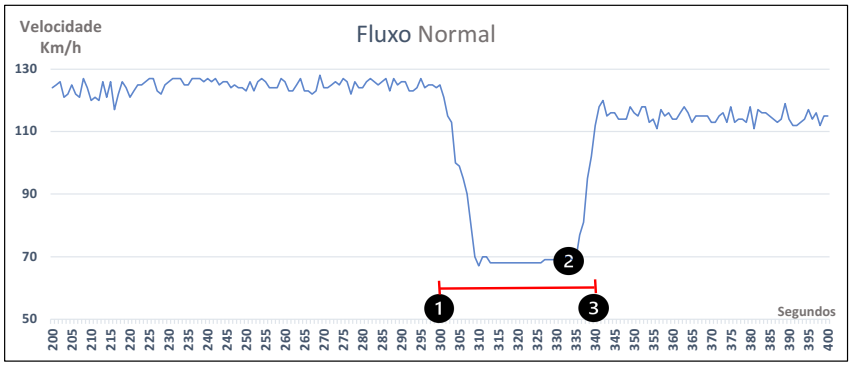
Figura 18 – Avaliação do sistema de reputação.

Ao observar-se como veículos maliciosos podem ser detectados em diferentes fluxos de tráfego, pode-se perceber que, após o envio de uma mensagem falsa, quanto maior o fluxo de tráfego, maior a redução na velocidade média; no entanto, o intervalo de tempo para detectar o veículo malicioso é menor.

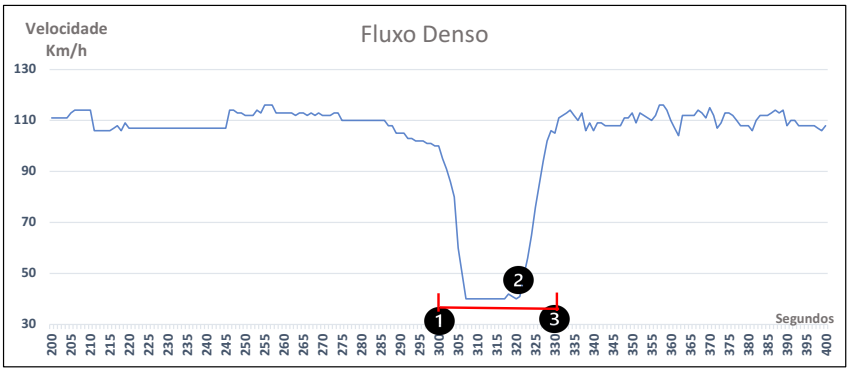
Uma segunda avaliação analisou o aumento do número de mensagens vinculadas com a utilização do mecanismo de reputação. A Tabela 16 e a Figura 20 mostram o número de mensagens propagadas na rede veicular com e sem o mecanismo de reputação.



(a) Intervalo de tempo para detectar veículos maliciosos - Fluxo esparso



(b) Intervalo de tempo para detectar veículos maliciosos - Fluxo normal



(c) Intervalo de tempo para detectar veículos maliciosos - Fluxo denso

Figura 19 – Avaliação do sistema de reputação - ① Um veículo malicioso propaga uma mensagem de alerta falso (WM); ② RSU recebe WVM, calcula a nova reputação e propaga o Tab-ID-Rep que contém a reputação do suspeito; ③ fim do intervalo de tempo para detectar o veículo malicioso.

Devido à adição de mensagens *WVM* ao sistema de reputação, há um aumento no número de mensagens transmitidas na rede. No entanto, mesmo com o acréscimo de mensagens, não há perda significativa da eficiência do sistema. Quando em um fluxo denso, o impacto é menor, pois o problema do congestionamento impede que a maioria dos veículos chegue ao local do incidente em tempo hábil e enviem as mensagens *WVM*

Tabela 16 – Aumento do número de mensagens (sem mensagens de *beacons*)

Fluxo	Número de mensagens sem sistema de reputação	Número de mensagens com sistema de reputação	INM
Esparso	1.308	1.432	9,5%
Normal	11.535	12,390	7,4%
Denso	31.558	32,696	3,6%

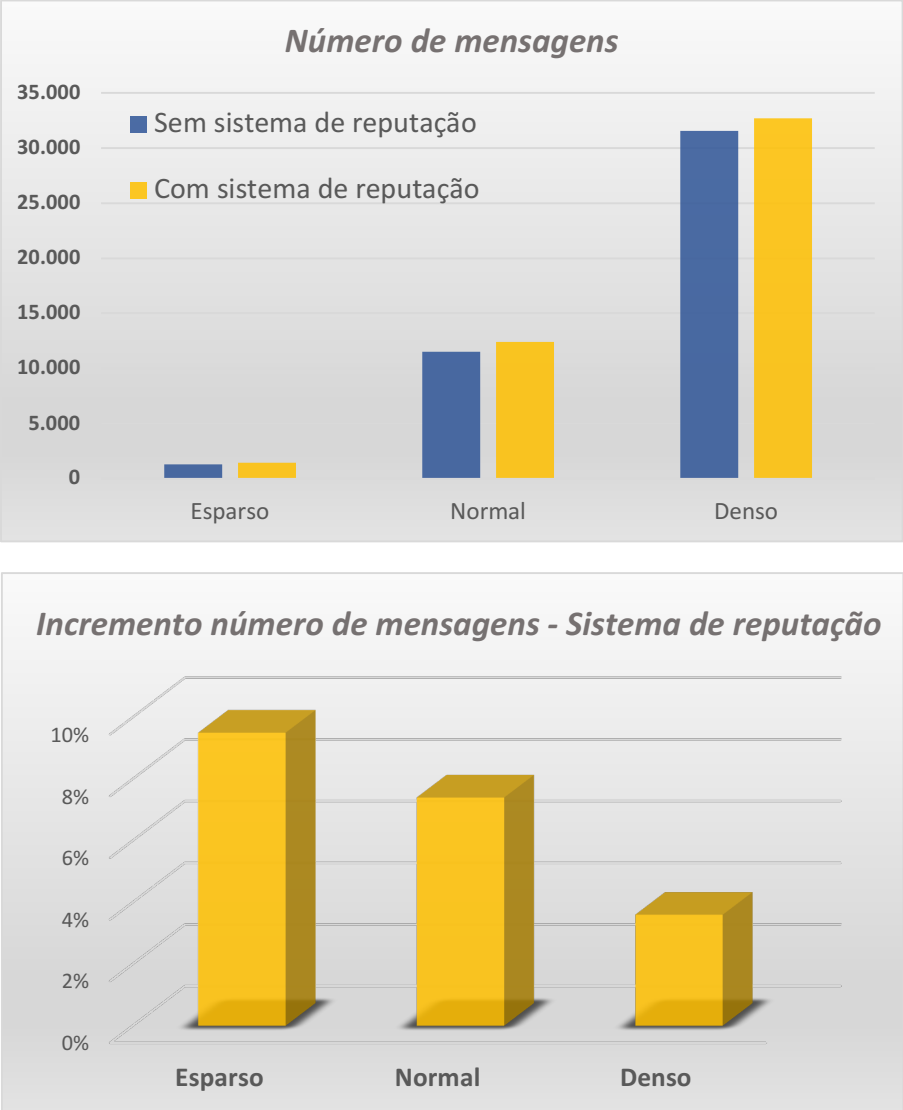


Figura 20 – Incremento do número de mensagens (sem contabilizar os *beacons*).

Outra análise foi realizada para avaliar o desempenho do sistema no que diz respeito ao aumento do armazenamento na *blockchain*, conforme o número de blocos criados (Tabela 17). Um bloco vazio (somente cabeçalho), no sistema proposto, possui cerca de 80 bytes; o tamanho da mensagem de reputação de cada veículo gravada na *blockchain* possui 9 *bytes*; e o histórico de cada mensagem validado e atestado pelos veículos através das mensagens *WVM* possui 10 *bytes*.

A Tabela 17 mostra o crescimento da *blockchain* em termos do número de blocos registrados como resultado i) do número de veículos com suas reputações armazenadas e ii) do histórico das mensagens validadas por outros veículos através de *acks* e *nacks*. A gravação da *blockchain* é realizada a cada dez minutos, tempo este parametrizado no sistema. Este tempo corresponde à passagem de 416 veículos em média em um cenário de fluxo normal e 666 veículos com fluxo de tráfego no cenário denso (ver Tabela 12). O valor máximo definido na simulação é de 420.480 blocos, perfazendo um total de oito anos de reputações armazenadas.

Tabela 17 – Análise de escalabilidade da *blockchain*

Tempo armazen.	**Tamanho armazenamento blockchain em bytes**			
	Nº blocos	**Mensagens alerta**	**Mensagens atestadas**	**TAB**
10 minutos	1	1	100	1.089 B
1 ano	52.560	1	100	57.237.840 B
2 anos	105.120	1	100	114.475.680 B
4 anos	210.240	1	100	228.951.360 B
8 anos	420.480	1	100	457.902.720 B
8 anos	420.480	10	500	2.173.881.600 B

Assumindo um cenário de fluxo normal em que cerca de 24% dos veículos (100 veículos) transmitem mensagens *WM* e *WVM*, será necessário um espaço de armazenamento na *blockchain* de 1.089 *bytes* para cada bloco e 0,46 GB após 8 anos. Mesmo no caso de um fluxo de tráfego denso onde cerca de 75% dos veículos (500 veículos) tenham seu valor de reputação atualizado, o tamanho máximo de armazenamento será de 2,17 GB.

Desse modo, pode-se concluir que o sistema *blockchain* que executa em RSUs é viável mesmo por um longo período. Aliado a isso, se o processo de poda for aplicado a *blockchain*, permitirá uma redução ainda mais significativa no espaço necessário para armazenar dados ou reduzir o intervalo de armazenamento (por exemplo, intervalo menor que 10 minutos).

5.3.2 Cenário para análise de falso-negativos

A métrica de falso-negativos, em que veículos maliciosos são considerados como não maliciosos, foi adotada para avaliar a capacidade de o BRS4VANETs detectar corretamente nós maliciosos na rede veicular. As simulações foram realizadas com diferentes fluxos, conforme ilustrado na Tabela 12, com diferentes criticidades de alerta e definidos quatro valores iniciais de reputação:

1. **Nó malicioso considerado confiável (V_rep = 0,7):** nesta situação, o veículo com histórico confiável na *blockchain*, começa a agir maliciosamente, através

da propagação de alerta falsos na rede. No momento da propagação da primeira mensagem, o nó emissor possui seu valor de reputação armazenado na *blockchain* de 0,7 que é maior que o valor assumido para Th_Rep que é 0,5.

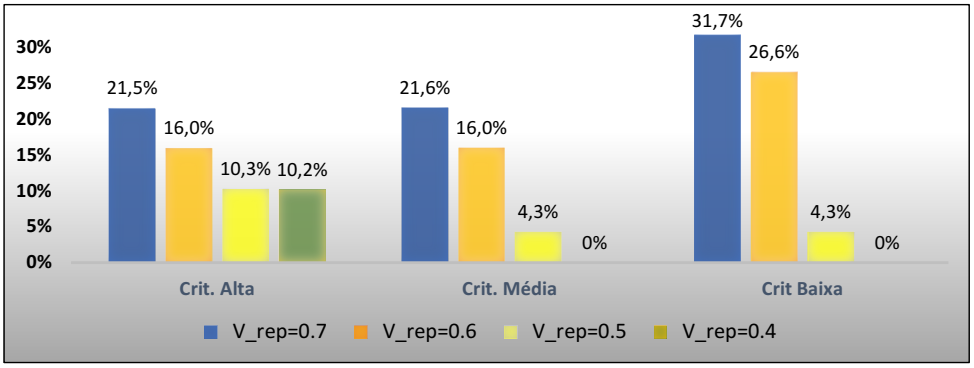
2. **Nó malicioso considerado confiável (V_rep = 0,6):** semelhante à situação anterior, o veículo também com histórico confiável na *blockchain*. Entretanto, o nó emissor possui seu valor inicial de reputação definido em 0,6, maior que o valor assumido para Th_Rep.

3. **Nó malicioso sem histórico na *blockchain* (V_rep = 0,5):** nesta situação, o veículo ingressou na rede e não possui ainda interação, ou seja, não enviou ou validou mensagens de alerta. Assim, devido à abordagem otimista do sistema, seu valor inicial de reputação na rede é o valor de Th_Rep.

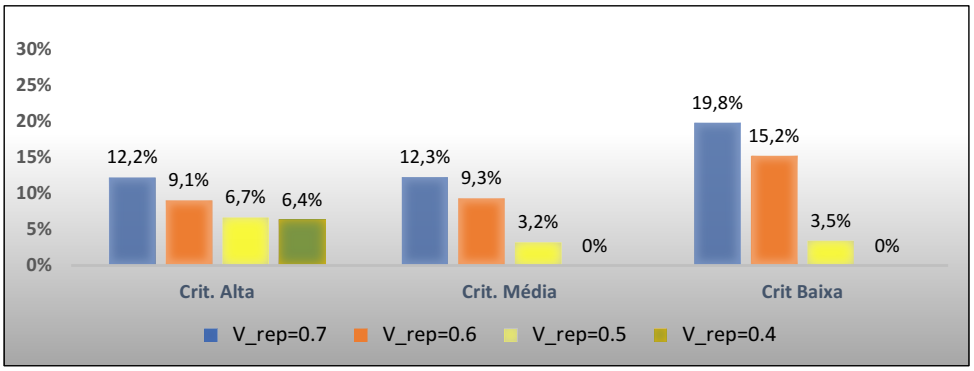
4. **Nó malicioso considerado não confiável (V_rep = 0,4)** o veículo considerado suspeito ou malicioso, dependendo da criticidade da mensagem, propaga um alerta falso na rede, porém, este veículo já se encontra na tabela de reputação dos demais veículos (*Tab-ID-Rep*) enviadas pelas RSUs.

A Figura 21 apresenta os resultados agrupados em termos de criticidade da mensagem, em diferentes fluxos e com os quatro valores iniciais de reputação definidos. Como pode ser constatado, o cenário de veículos em que havia um fluxo de tráfego esparso, foi o que apresentou maior índice de falso-negativos. Isso decorre devido ao fato dos veículos estarem distantes entre si e, porque o tempo necessário para receber as mensagens *WVM* e calcular a nova reputação do veículo malicioso foi maior que nos demais cenários simulados. Nos três cenários simulados, a maior taxa de falso-negativos foi encontrada quando o veículo teve seu valor de reputação definido em 0,7. Isso pode ser explicado pelo fato de que o veículo malicioso possui uma boa reputação na rede (ou seja, o nó é considerado confiável no sistema de reputação), portanto, precisa de um tempo maior para que sua reputação decaia até que os outros veículos o considerem malicioso.

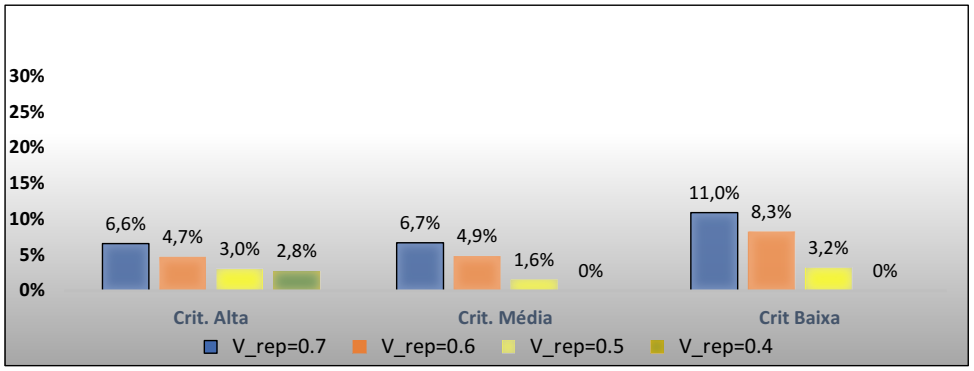
Quando o valor de reputação foi igual a 0,4 na simulação (ou seja, quando o nó possui V_rep menor que Th_Rep e é considerado suspeito no sistema de reputação), a taxa de falso-negativos foi zero em quase todos os cenários. A exceção ocorre quando a criticidade da mensagem de alerta propagada é alta, pois, nesta situação, as mensagens *WM* enviadas pelo nó malicioso são entregues aos motoristas, pois, o veículo é categorizado primeiramente como suspeito para só posteriormente ser assumido como malicioso, como pode ser constatado no Algoritmo 5.



(a) Fluxo esparso



(b) Fluxo normal



(c) Fluxo denso

Figura 21 – Taxas de falso-negativos em diferentes fluxos de veículos.

A reputação dos veículos varia temporalmente conforme seu comportamento na rede. As figuras 22 e 23 apresentam, em diferentes criticidades, uma análise comparativa do decremento do valor de reputação de um veículo que propaga recorrentes mensagens *WMs* falsas na rede e, com limiares iniciais de reputação definidos em 0,7 e 0,5 respectivamente.

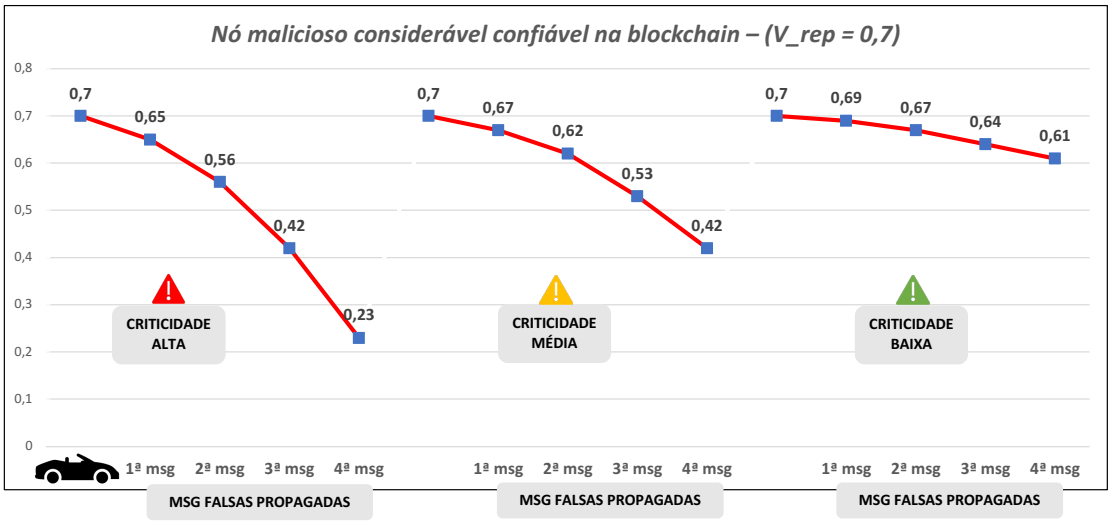


Figura 22 – Decremento da reputação de um veículo inicialmente confiável na *blockchain*.

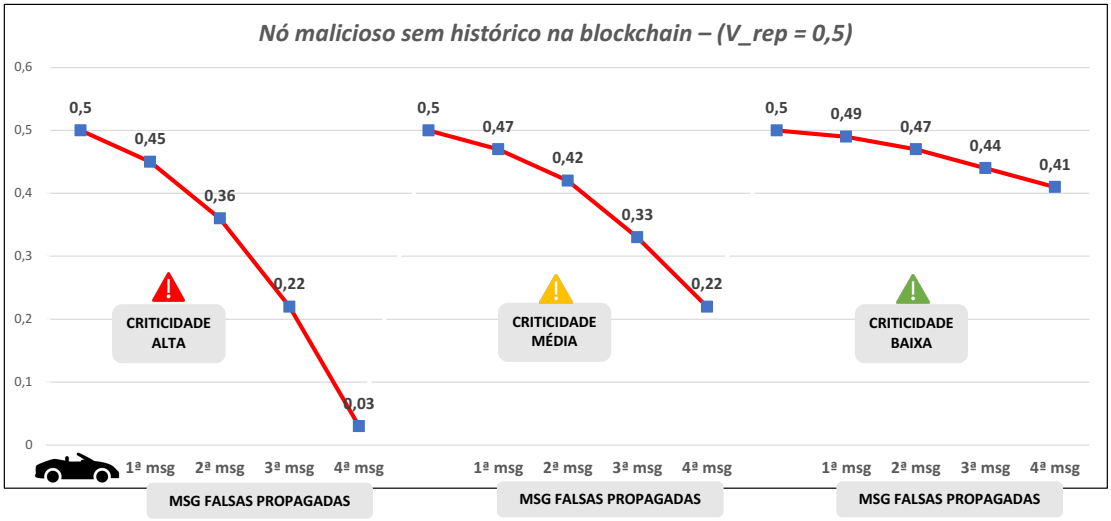


Figura 23 – Decremento da reputação de um veículo inicialmente sem histórico na *blockchain*.

Nota-se que, quanto maior o número de mensagens falsas propagadas, a proporção de redução da reputação também é maior. Na Figura 22, na primeira mensagem falsa com grau de criticidade alta, há um decremento de cerca de 7,1%. No entanto, o veículo ao continuar com ações maliciosas e propagar uma quarta mensagem falsa, a sua reputação reduz cerca de 45,2%. Diante disso, devido ao seu histórico armazenado

na *blockchain*, suas ações são ponderadas por um coeficiente de peso, FM_V (Equação 3) o qual é dimensionado conforme o número de mensagens falsas disseminadas.

Evidencia-se também nas análises comparativas que, embora com uma taxa de redução menor, há também um impacto no decremento da reputação de acordo com o grau de criticidade das mensagens. Este resultado é decorrente das variáveis de valores de ganho utilizados para essas criticidades, conforme descrito anteriormente na Seção 4.3.3 e ilustrado na Tabela 9.

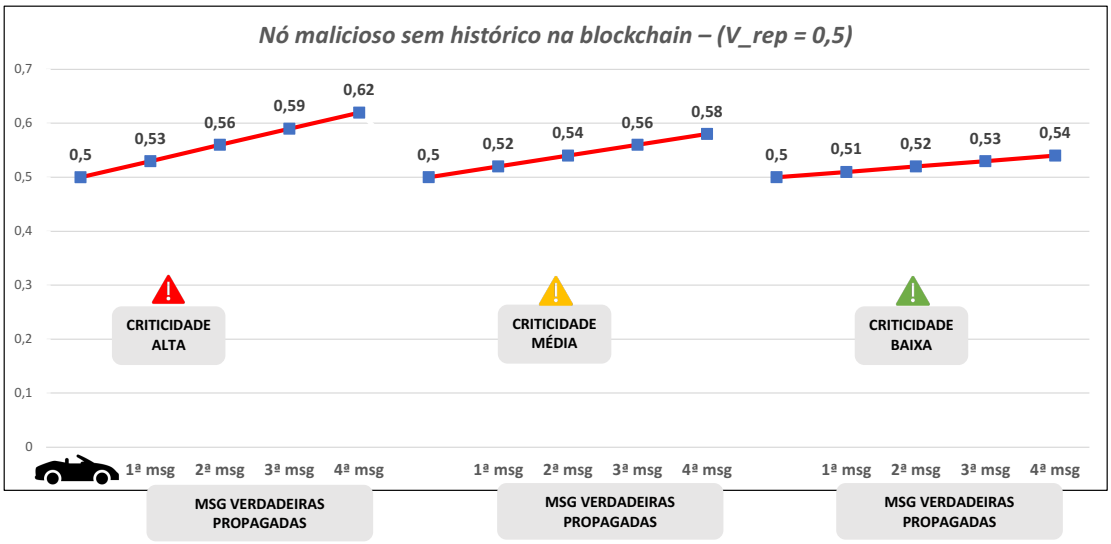


Figura 24 – Incremento da reputação por mensagens verdadeiras propagadas.

Em outro experimento, ilustrado na Figura 24, é apresentando o valor de incremento dos veículos que, ao ingressarem na rede, ainda sem histórico na *blockchain*, comportam-se de maneira honesta disseminando mensagens de alerta verdadeiras. Verifica-se que o valor da reputação modifica conforme o nível de criticidade da mensagem de alerta, sendo que, quanto maior a sua criticidade maior o incremento da reputação. Em mensagens com criticidade alta, o percentual de aumento é de 5,65% a cada mensagem propagada. Enquanto em criticidades baixa, essa aumento é de cerca de 1,88%.

Os veículos que atestam mensagens de alerta recebidas também têm o seu valor de reputação aumentado, porém, gradualmente. A Figura 25 exemplifica este incremento em que um veículo após passar por diversos locais dos eventos relatados em mensagens de alerta WMs, valida estas ocorrências e, após consolidadas pelas RSUs, e confirmadas como evento verdadeiro pela maioria dos veículos, tem seu valor de reputação incrementado e armazenado na *blockchain.* Constata-se que nas mensagens de WVM, este aumento gradativo é mais moderado quando comparado ao aumento da reputação por mensagens WM. Isto justifica-se de modo que um veículo com intenções maliciosas, não se comporte primeiramente como confiável, incremen-

tando a sua reputação apenas propagando WVM verdadeiras para posteriormente se tornar um nó malicioso. Desta forma, no sistema BRS4VANETs, após uma única ação maliciosa do veículo, para que este recupere novamente a sua reputação através de mensagens WVM, serão necessárias 150 mensagens de ações verdadeiras.

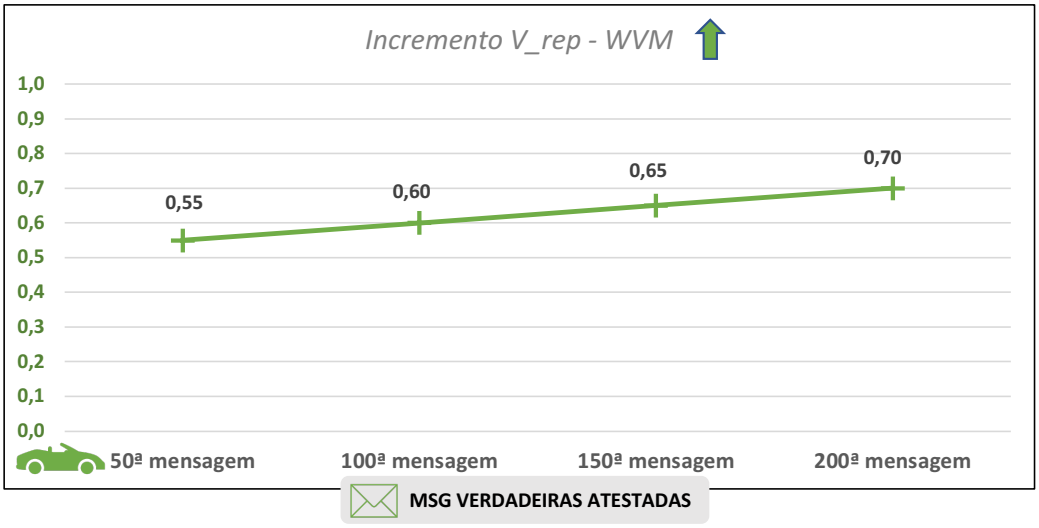
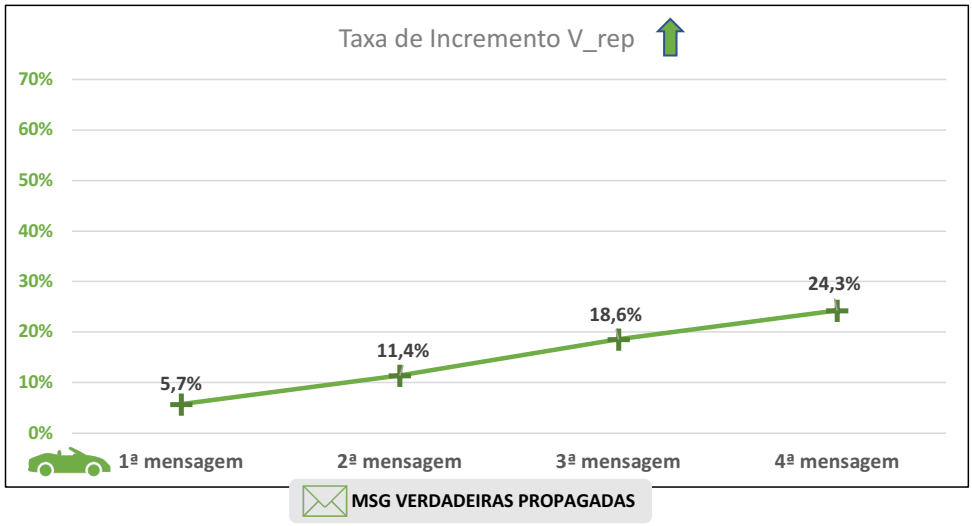
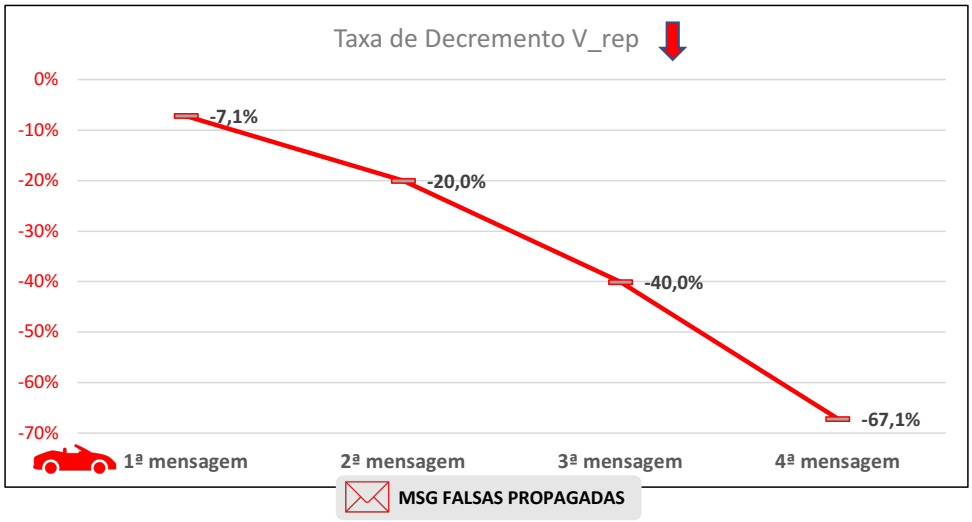


Figura 25 – Incremento da reputação por mensagens verdadeiras atestadas.

Na Figura 26 é possível observar as taxas de aumento e redução da reputação do veículo que propaga mensagens (*WMs*) na rede, comprovadas por outros veículos (WVMs). Pode-se observar que há um impacto mais significativo a cada mensagem propagada quando o veículo comporta-se maliciosamente (Figura 26b) quando comparada com o seu bom comportamento (Figura 26a). Portanto, o BRS4VANETs visa reduzir a reputação mais rapidamente punindo os veículos que se comportam mal, tornando mais fácil perder reputação do que ganhá-la. Por outro lado, veículos honestos são recompensados por suas ações, porém aumentando a sua reputação de maneira mais gradativa.



(a) Taxa de incremento.



(b) Taxa de decremento.

Figura 26 – Mudança de valores de reputação conforme o comportamento do veículo na rede.

5.4 CONSIDERAÇÕES DO CAPÍTULO

Este capítulo apresentou os resultados obtidos nos experimentos, os quais serviram para avaliar o desempenho da abordagem proposta. Diante dos resultados, pode se concluir que o BRS4VANETs é eficiente quando são considerados cenários rodoviários com diferentes fluxos de densidades, sendo uma solução adequada para as aplicações de segurança que requerem troca confiável de dados, como nas redes veiculares.

Os impactos do uso do sistema proposto na rede veicular foram avaliados medindo diferentes métricas como, por exemplo, a redução da velocidade e o atraso causado por mensagens falsas propagadas. Neste contexto, foi verificado que, inde-

pendente do fluxo simulado, as mensagens falsas ocasionaram redução na velocidade dos veículos, chegando a uma redução de 29%, no pior cenário, sem o uso do sistema de reputação. Porém, com o uso do sistema de reputação o decremento foi de apenas 5,2%.

Os resultados dos experimentos também demonstram que o tempo necessário para detectar um veículo malicioso modifica em relação ao fluxo de veículos na rodovia. Isso decorre pelos seguintes aspectos: (i) tempo necessário para os veículos atestarem o evento, (ii) cálculo da nova reputação executada pelas RSUs, (iii) armazenamento na *blockchain* e por fim (iv) a divulgação, pelas RSUs, da nova lista de reputação aos veículos. Verifica-se que, quando maior o fluxo de veículos, mais rápido ocorre a detecção e identificação do veículo malicioso e descartar seus alertas.

A escalabilidade da *blockchain* foi outro experimento realizado onde os resultados evidenciam que mesmo em um período 8 anos de armazenamento dos blocos com as transações das reputações, o crescimento da *blockchain* não é expressiva. Além disso, caso seja necessário reduzir o tempo de gravação do bloco (parametrizável no sistema) ou armazenar por um maior período, o processo de poda na *blockchain* pode ser implementado aumentando mais a sua escalabilidade.

Ao avaliar a eficácia do sistema proposto com relação à taxa do número de veículos que identificaram erroneamente um nó malicioso como confiável foi verificado que, com criticidade alta da mensagem e valor de reputação definido em 0,7 foi o fluxo esparso que apresentou o maior número de falso-negativos (10,2%), quando comparado aos demais fluxos simulados neste trabalho. Esta taxa explica-se pelo fato do veículo malicioso possuir uma boa reputação na *blockchain* e, consequentemente, necessitar de um tempo maior para o decaimento de sua reputação até que os demais veículos o considerem malicioso. Neste cenário, como os veículos estavam mais distantes uns dos outros, o BRS4VANETs necessitou de um tempo maior para que os veículos passassem pelo local do evento, emitissem as mensagens de validação, contabilizasse as experiências negativas e para que a reputação do veículo reduzisse até ser considerado malicioso.

Por fim, por meio dos resultados e análises apresentados neste capítulo, confirma que essa abordagem consegue identificar de maneira eficaz a presença de nós maliciosos e neutralizar suas ações, mesmo diante de nós desconhecidos.

6 CONCLUSÕES

Este capítulo conclui a tese abordando, primeiro, uma revisão das motivações e objetivos traçados. Na sequência, uma visão geral do desenvolvimento do trabalho é apresentada. Depois são delimitados o escopo do trabalho e suas principais contribuições. Por fim, são discutidos alguns trabalhos futuros.

6.1 REVISÃO DAS MOTIVAÇÕES E OBJETIVOS

Apesar dos STI apresentarem um vasto universo de possibilidade e integrações de novas tecnologias e de inovações, eles trazem consigo uma enorme quantidade de desafios. No contexto das redes veiculares, diversas ameaças e vulnerabilidades surgem, e a proposta de novas soluções de segurança que busquem a proteção dos participantes se justificam. Os sistemas de gerenciamento de confiança tornaram-se uma importante alternativa para garantir a confiabilidade e a troca segura de mensagens em redes veiculares, pois permitem que os veículos avaliem o comportamento dos demais veículos, e só então decidam se confiarão ou não nas mensagens enviadas por estes. Contudo, mesmo com o surgimento desses sistemas, encontrar um equilíbrio entre segurança, eficiência e requisitos de rede continua sendo um desafio em aberto.

De modo a orientar a pesquisa, foi identificado o seu objetivo geral e alguns objetivos específicos. O objetivo geral consistiu na proposta de combinar diferentes técnicas para analisar e armazenar o comportamento dos veículos para detectar a presença de nós maliciosos, mitigar seu comportamento e contribuir para a tomada de decisões. Os objetivos específicos envolviam a utilização da tecnologia *blockchain* para registrar o comportamento dos veículos; gerenciar e armazenar uma lista de reputação com os dados dos veículos suspeitos e maliciosos; excluir veículos maliciosos da rede veicular através de uma abordagem descentralizada; mitigar problemas de ataque de conluio e aumentar a segurança na rede através de um sistema de votação. Objetivou-se também, criar um ambiente para validar a proposta, mensurar seu desempenho, verificar os riscos causados por mensagens falsas e o impacto do uso do sistema na rede.

6.2 VISÃO GERAL DO TRABALHO

Os métodos de pesquisa utilizados foram separados em quatro fases. Na primeira fase, foi executada uma pesquisa bibliográfica para realizar a fundamentação teórica e buscar trabalhos correlatos que abordam a área de redes veiculares, aplicações que utilizam redes veiculares, sistemas de reputação e gerenciamento de

confiança. Nessa fase, foram levantadas as demandas e lacunas existentes nas atuais pesquisas.

A partir do estudo inicial, na segunda fase, a abordagem proposta foi definida e seus algoritmos, equações e mensagens foram descritos. Na terceira fase, a abordagem proposta foi implementada, denominada BRS4VANETs, utilizando dois simuladores (rede e de tráfego) bidirecionalmente acoplados. Por fim, na quarta fase, diferentes experimentos simulados foram realizados visando avaliar a abordagem no que se refere à eficiência e eficácia do sistema de reputação para identificar nós maliciosos e os impactos do seu uso, bem como uma análise da viabilidade do armazenamento na *blockchain*.

O sistema BRS4VANETs empregou a tecnologia *blockchain* e contratos inteligentes para fornecer aos veículos, informações inalteradas e confiáveis. No processo de consenso da rede *blockchain*, as RSUs atuam como agregadores de dados, bem como validadores. O mecanismo PoA foi usado para a determinação do consenso devido às suas vantagens em redes permissionadas. Um mecanismo de votação também foi empregado para garantir que a tomada de decisão dos veículos pudesse ser realizada com mais segurança ao relatar incidentes e mitigar ataques de conluio de veículos maliciosos na rede.

Simulações foram realizadas para avaliar o desempenho do sistema envolvendo dois cenários de rede. O primeiro cenário buscou avaliar as consequências da disseminação de mensagens falsas sem um mecanismo de reputação. Entre elas, a redução da velocidade e o aumento do tempo gasto pelos veículos durante o trecho simulado. Verificou-se que o BRS4VANETs teve um baixo *overhead* em termos de aumento do número de mensagens enviadas.

O segundo cenário de simulação buscou analisar as mudanças no comportamento do veículo devido à inclusão de um sistema de reputação, e com base nos resultados pôde-se confirmar que o BRS4VANETs é eficiente em termos de falso-negativos. Considerando que o sistema possui uma abordagem otimista, na qual os veículos são considerados confiáveis ao se integrarem inicialmente na rede, o índice de falso-negativos obtido se manteve em valores considerados baixos nos cenários simulados.

Como diferentes concessionárias podem gerenciar as RSUs ao longo da rodovia, a tecnologia *blockchain* desempenha um papel importante, fornecendo um mecanismo descentralizado para manter a integridade das informações. No entanto, esses mecanismos têm custos que precisam ser cuidadosamente analisados para avaliar se os benefícios superam esses custos. No que diz respeito ao crescimento da *blockchain* para armazenar as reputações e registros históricos, análises efetuadas mostraram a viabilidade de se implementar o sistema nas RSUs, mesmo por um longo período.

6.3 ESCOPO DO TRABALHO E CONTRIBUIÇÕES

O escopo desta tese envolveu o uso de algumas tecnologias e protocolos, sem a pretensão de contribuir no desenvolvimento destes. Como exemplo, apesar de ser notório que determinados protocolos de difusão de dados confiáveis para VANETs são mais adequados que outros dependendo do contexto dos seus usos, estava fora do escopo deste trabalho propor um novo protocolo, ou mesmo comparar protocolos e escolher o melhor deles. De forma semelhante, não estava nos objetivos deste trabalho contribuir com o estado-da-arte da teoria de *blockchains*.

O emprego de *blockchains* no contexto de aplicações de STI implica na necessidade de se garantir não apenas a implantação dessa tecnologia, mas também sua manutenção ao longo do tempo. As concessionárias que operam as RSUs e a *blockchain* precisam prover manutenção com investimentos contínuos em infraestrutura. Essa questão, pode ser tema de trabalhos futuros, mas estava fora do contexto desta tese. Finalmente, apesar de reconhecer que uma avaliação experimental do sistema através de protótipos em rodovias reais seria de grande utilidade para levantar *overheads* que as vezes são desconsiderados durante simulações, esse tipo de avaliação não era objetivo deste trabalho.

Dentre as principais contribuições desta tese podem ser destacadas as seguintes:

- O desenvolvimento de um sistema de gerenciamento de confiança descentralizado de reputação usando *blockchain* (chamado BRS4VANETs) para analisar e armazenar dados sobre o comportamento dos veículos. Este sistema envolve recompensar veículos honestos e punir aqueles que se comportam mal;
- Uma abordagem descentralizada para excluir veículos maliciosos da rede veicular revogando seu certificado;
- Mitigar problemas de ataques de conluio por veículos maliciosos e garantir a segurança das decisões sobre punir os veículos na rede através de um sistema de votação adotado;
- Análise para verificar a melhora da segurança ao detectar veículos maliciosos e mitigar o problema de disseminação de informações falsas na rede veicular com o uso do BRS4VANETs.

6.4 PERSPECTIVAS DE ATIVIDADES FUTURAS

Para dar continuidade a presente tese, há ainda uma série de oportunidades a serem exploradas por nós ou por outros pesquisadores interessados neste campo de pesquisa.

6.4.1 Questões abertas de pesquisa

Algumas questões de pesquisas em aberto podem ser abordadas em atividades futuras. Entre essas, como maximizar a segurança e privacidade das aplicações que usam a solução BRS4VANETs sem comprometer métricas de desempenho da rede, como latência e escalabilidade em determinados cenários. Como utilizar melhor outras tecnologias, como inteligência artificial e aprendizado de máquina, para facilitar a tomada de decisões e melhorar os sistemas de reputação também é foco de pesquisas futuras. Explorar soluções de escalabilidade da *blockchain* para reduzir os custos computacionais e latência envolvidos é outro ponto de pesquisa em aberto a ser investigado.

6.4.2 Extensões Imediatas da Proposta nesta Tese

Além dessas questões abertas de pesquisa elencadas na Seção 6.4.1, existem outras extensões que podem ser aplicadas diretamente para os propósitos deste trabalho. Como desdobramento desta tese, podem ser considerados os seguintes pontos:

- Experimentos em diferentes áreas geográficas podem ser realizados para avaliar a eficiência e escalabilidade do BRS4VANETs em outros contextos.
- Estender o BRS4VANETs para que este possa ser adaptado (configurável) para outras categorias de aplicações de segurança no trânsito e cenários (urbano, por exemplo), através de uma interface, e com isso poder avaliar a sua integração a outras aplicações.
- Explorar o uso de dados biométricos para vincular os dados do motorista ao validar as informações do veículo, agregando assim valor de reputação aos motoristas para rastrear seu comportamento na rede veicular.
- Estender o algoritmo de consenso adotado para que o líder (RSU) eleito seja sempre aquele mais próximo do evento do alerta, visando maior eficiência nas transações.
- Desenvolver um sistema de gestão de identidades específico para redes veiculares para prover a identificação, autenticação e autorização de veículos a fim de viabilizar a implantação do BRS4VANETs.

REFERÊNCIAS

ALHARTHI, Abdullah; NI, Qiang; JIANG, Richard. A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET. **IEEE Access**, IEEE, v. 9, p. 87299–87309, 2021.

AN, An Cong *et al.* Building a product origins tracking system based on blockchain and PoA consensus protocol. *In:* IEEE. 2019 International Conference on Advanced Computing and Applications (ACOMP). [S.l.: s.n.], 2019. P. 27–33.

AWAIS HASSAN, Muhammd *et al.* A secure message-passing framework for inter-vehicular communication using blockchain. **International Journal of Distributed Sensor Networks**, SAGE Publications Sage UK: London, England, v. 15, n. 2, p. 1550147719829677, 2019.

BACH, LM; MIHALJEVIC, Branko; ZAGAR, Mario. Comparative analysis of blockchain consensus algorithms. *In:* IEEE. 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). [S.l.: s.n.], 2018. P. 1545–1550.

CACHIN, Christian. Architecture of the hyperledger blockchain fabric. *In:* WORKSHOP on distributed cryptocurrencies and consensus ledgers. [S.l.: s.n.], 2016.

CACHIN, Christian; VUKOLIĆ, Marko. Blockchain consensus protocols in the wild. **arXiv preprint arXiv:1707.01873**, 2017.

CASTRO, Miguel; LISKOV, Barbara *et al.* Practical Byzantine fault tolerance. *In:* OSDI. [S.l.: s.n.], 1999. P. 173–186.

CEDER, Avishai. Urban mobility and public transport: Future perspectives and review. **International Journal of Urban Sciences**, Taylor & Francis, v. 25, n. 4, p. 455–479, 2021.

CELES, A Asline; ELIZABETH, N Edna. Verification based authentication scheme for bogus attacks in VANETs for secure communication. *In:* IEEE. 2018 International Conference on Communication and Signal Processing (ICCSP). [S.l.: s.n.], 2018. P. 0388–0392.

CHALAEMWONGWAN, Nutthakorn; KURUTACH, Werasak. State of the art and challenges facing consensus protocols on blockchain. *In:* IEEE. 2018 International Conference on Information Networking (ICOIN). [S.l.: s.n.], 2018. P. 957–962.

CHENG, JiuJun *et al.* Routing in internet of vehicles: A review. **IEEE Transactions on Intelligent Transportation Systems**, IEEE, v. 16, n. 5, p. 2339–2352, 2015.

CODECA, Lara *et al.* Luxembourg sumo traffic (lust) scenario: Traffic demand evaluation. **IEEE Intelligent Transportation Systems Magazine**, IEEE, v. 9, n. 2, p. 52–63, 2017.

COLQUHOUN, Heather L *et al.* Scoping reviews: time for clarity in definition, methods, and reporting. **Journal of clinical epidemiology**, Elsevier, v. 67, n. 12, p. 1291–1294, 2014.

CUI, Jie *et al.* RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks. **IEEE Internet of Things Journal**, IEEE, v. 6, n. 4, p. 6417–6428, 2019.

CUNHA, André Luiz; BESSA, José Elievam; SETTI, José Reynaldo. Genetic algorithm for the calibration of vehicle performance models of microscopic traffic simulators. *In:* SPRINGER. PORTUGUESE Conference on Artificial Intelligence. [S.l.: s.n.], 2009. P. 3–14.

CUNHA, Felipe *et al.* Data communication in VANETs: Protocols, applications and challenges. **Ad Hoc Networks**, Elsevier, v. 44, p. 90–103, 2016.

DENNIS, Richard; OWEN, Gareth. Rep on the block: A next generation reputation system based on the blockchain. *In:* IEEE. 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). [S.l.: s.n.], 2015. P. 131–138.

ENGOULOU, Richard Gilles *et al.* A decentralized reputation management system for securing the internet of vehicles. *In:* IEEE. 2019 International Conference on Computing, Networking and Communications (ICNC). [S.l.: s.n.], 2019. P. 900–904.

ETSI, TS. **102 636-4-1:" Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality" V1. 1.1 (2011-06)**. [S.l.: s.n.], 2011.

FINCK, Michèle. Blockchains and data protection in the european union. **Eur. Data Prot. L. Rev.**, HeinOnline, v. 4, p. 17, 2018.

FITAH, A *et al.* Performance of DSRC and WIFI for Intelligent Transport Systems in VANET. **Procedia Computer Science**, Elsevier, v. 127, p. 360–368, 2018.

GAO, Jianbin *et al.* A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks. **IEEE Internet of Things Journal**, IEEE, v. 7, n. 5, p. 4278–4291, 2019.

GAO, Yuefei; NOBUHARA, Hajime. A proof of stake sharding protocol for scalable blockchains. **Proceedings of the Asia-Pacific Advanced Network**, v. 44, p. 13–16, 2017.

GARG, Sahil *et al.* Edge computing-based security framework for big data analytics in VANETs. **IEEE Network**, IEEE, v. 33, n. 2, p. 72–81, 2019.

GAYATHRI, M; GOMATHY, C. A deep survey on types of cyber attacks in VANET. **J Crit Rev**, v. 8, n. 01, p. 1029–1039, 2021.

GAZDAR, Tahani; ALBOQOMI, Ohoud; MUNSHI, Asmaa. A Decentralized Blockchain-Based Trust Management Framework for Vehicular Ad Hoc Networks. **Smart Cities**, MDPI, v. 5, n. 1, p. 348–363, 2022.

GRANDISON, Tyrone; SLOMAN, Morris. A survey of trust in internet applications. **IEEE Communications Surveys & Tutorials**, IEEE, v. 3, n. 4, p. 2–16, 2000.

GREVE, Fabíola Greve *et al.* Blockchain e a Revolução do Consenso sob Demanda. **Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos**, 2018.

GUERRERO-IBÁÑEZ, Juan; ZEADALLY, Sherali; CONTRERAS-CASTILLO, Juan. Sensor technologies for intelligent transportation systems. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 18, n. 4, p. 1212, 2018.

HEIJDEN, Rens W van der *et al.* Blackchain: Scalability for resource-constrained accountable vehicle-to-x communication. *In:* ACM. PROCEEDINGS of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. [S.l.: s.n.], 2017. P. 4.

HOY, Matthew B. An introduction to the blockchain and its implications for libraries and medicine. **Medical reference services quarterly**, Taylor & Francis, v. 36, n. 3, p. 273–279, 2017.

HU, Jiangyi; BURMESTER, Mike. Cooperation in mobile ad hoc networks. *In:* GUIDE to Wireless Ad Hoc Networks. [S.l.]: Springer, 2009. P. 43–57.

INEDJAREN, Youssef *et al.* Blockchain-based distributed management system for trust in VANET. **Vehicular Communications**, Elsevier, v. 30, p. 100350, 2021.

IQBAL, Razi *et al.* Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions. **International Journal of Distributed Sensor Networks**, SAGE Publications Sage UK: London, England, v. 15, n. 1, p. 1550147719825820, 2019.

JAKUBIAK, Jakub; KOUCHERYAVY, Yevgeni. State of the art and research challenges for VANETs. *In:* IEEE. CONSUMER communications and networking conference, 2008. CCNC 2008. 5th IEEE. [S.l.: s.n.], 2008. P. 912–916.

JAVAID, Uzair; AMAN, Muhammad Naveed; SIKDAR, Biplab. A scalable protocol for driving trust management in internet of vehicles with blockchain. **IEEE Internet of Things Journal**, IEEE, v. 7, n. 12, p. 11815–11829, 2020.

KADHIM, Ahmed Jawad; NASER, Jaber Ibrahim. Toward electrical vehicular ad hoc networks: E-VANET. **Journal of Electrical Engineering & Technology**, Springer, v. 16, n. 3, p. 1667–1683, 2021.

KANG, Jiawen *et al.* Blockchain for secure and efficient data sharing in vehicular edge computing and networks. **IEEE Internet of Things Journal**, IEEE, 2018.

KANG, Jiawen *et al.* Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. **IEEE Transactions on Vehicular Technology**, IEEE, v. 68, n. 3, p. 2906–2920, 2019.

KCHAOU, Amira; ABASSI, Ryma; GUEMARA, Sihem. Toward a distributed trust management scheme for VANET. *In:* ACM. PROCEEDINGS of the 13th International Conference on Availability, Reliability and Security. [S.l.: s.n.], 2018. P. 53.

KEELE, Staffs *et al.* **Guidelines for performing systematic literature reviews in software engineering**. [S.l.], 2007.

KERRACHE, Chaker. **Malicious messages detection and exclusion mechanisms in Vehicular Networks (VANETs)**. Jan. 2017. F. 34. Tese (Doutorado) – University Amar Telidji.

KERRACHE, Chaker Abdelaziz *et al.* Trust management for vehicular networks: An adversary-oriented overview. **IEEE Access**, IEEE, v. 4, p. 9293–9307, 2016.

KERRACHE, Chaker Abdelaziz *et al.* UAV-assisted technique for the detection of malicious and selfish nodes in VANETs. **Vehicular Communications**, Elsevier, v. 11, p. 1–11, 2018.

KHALID, Adia *et al.* A blockchain based incentive provisioning scheme for traffic event validation and information storage in VANETs. **Information Processing & Management**, Elsevier, v. 58, n. 2, p. 102464, 2021.

KILLAT, Moritz *et al.* Enabling efficient and accurate large-scale simulations of VANETs for vehicular traffic management. *In:* ACM. PROCEEDINGS of the fourth ACM international workshop on Vehicular ad hoc networks. [S.l.: s.n.], 2007. P. 29–38.

KOSBA, Ahmed *et al.* Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *In:* IEEE. 2016 IEEE symposium on security and privacy (SP). [S.l.: s.n.], 2016. P. 839–858.

KOSCH, Timo. Local danger warning based on vehicle ad-hoc networks: Prototype and simulation. *In:* PROCEEDINGS of 1st International Workshop on Intelligent Transportation (WIT 2004). [S.l.: s.n.], 2004.

KUDVA, Sowmya *et al.* A scalable blockchain based trust management in VANET routing protocol. **Journal of Parallel and Distributed Computing**, Elsevier, v. 152, p. 144–156, 2021.

LEE, Eun-Kyu *et al.* Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs. **International Journal of Distributed Sensor Networks**, SAGE Publications Sage UK: London, England, v. 12, n. 9, p. 1550147716665500, 2016.

LIN, Iuon-Chang; LIAO, Tzu-Chun. A Survey of Blockchain Security Issues and Challenges. **IJ Network Security**, v. 19, n. 5, p. 653–659, 2017.

LIU, Kai *et al.* Cooperative data scheduling in hybrid vehicular ad hoc networks: VANET as a software defined network. **IEEE/ACM Transactions on Networking (TON)**, IEEE Press, v. 24, n. 3, p. 1759–1773, 2016.

LIU, Xuejiao *et al.* HDRS: A Hybrid Reputation System With Dynamic Update Interval for Detecting Malicious Vehicles in VANETs. **IEEE Transactions on Intelligent Transportation Systems**, IEEE, 2021.

LU, Zhaojun *et al.* A privacy-preserving trust model based on blockchain for VANETs. **IEEE Access**, IEEE, v. 6, p. 45655–45664, 2018.

MANIVANNAN, Dakshnamoorthy; MONI, Shafika Showkat; ZEADALLY, Sherali. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). **Vehicular Communications**, Elsevier, v. 25, p. 100247, 2020.

MINGXIAO, Du *et al.* A review on consensus algorithm of blockchain. *In:* IEEE. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). [S.l.: s.n.], 2017. P. 2567–2572.

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. **1**, Working Paper, 2008.

NAKAMOTO, Satoshi. **Bitcoin: A peer-to-peer electronic cash system**. [S.l.], 2009.

NEM, T. Nem technical reference. **URL https://nem. io/wpcontent/themes/nem/files/NEM_techRef. pdf**, 2018.

PALM, Emanuel. **Implications and impact of blockchain transaction pruning**. [S.l.: s.n.], 2017.

PANDA, Sandeep Kumar. **Blockchain Technology: Applications and Challenges**. [S.l.]: Springer Nature, 2021.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho cientifico: metodos e tecnicas da pesquisa e do trabalho academico**. [S.l.]: Editora Feevale, 2013.

REYNA, Ana *et al.* On blockchain and its integration with IoT. Challenges and opportunities. **Future Generation Computer Systems**, Elsevier, v. 88, p. 173–190, 2018.

SAMARA, Ghassan. Intelligent reputation system for safety messages in VANET. **arXiv preprint arXiv:2007.12717**, 2020.

AL-SHAREEDA, Mahmood A *et al.* Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. **IEEE Access**, IEEE, 2021.

SHRESTHA, Rakesh *et al.* A new type of blockchain for secure message exchange in VANET. **Digital communications and networks**, Elsevier, v. 6, n. 2, p. 177–186, 2020.

SULTAN, Shahid *et al.* Collaborative-trust approach toward malicious node detection in vehicular ad hoc networks. **Environment, Development and Sustainability**, Springer, p. 1–19, 2021.

TOMAR, Ravi. Maintaining trust in VANETs using blockchain. **ACM SIGAda Ada Letters**, ACM New York, NY, USA, v. 40, n. 1, p. 91–96, 2020.

TSCHORSCH, Florian; SCHEUERMANN, Björn. Bitcoin and beyond: A technical survey on decentralized digital currencies. **IEEE Communications Surveys & Tutorials**, IEEE, v. 18, n. 3, p. 2084–2123, 2016.

WANG, Danxin *et al.* A privacy-preserving trust management system based on blockchain for vehicular networks. *In:* IEEE. 2021 IEEE Wireless Communications and Networking Conference (WCNC). [S.l.: s.n.], 2021. P. 1–6.

WANG, Peng; LIU, Yining. SEMA: Secure and efficient message authentication protocol for VANETs. **IEEE systems journal**, IEEE, v. 15, n. 1, p. 846–855, 2021.

WEIL, Tim. Service management for ITS using WAVE (1609.3) networking. *In:* IEEE. GLOBECOM Workshops, 2009 IEEE. [S.l.: s.n.], 2009. P. 1–6.

YANG, Rebecca *et al.* Public and private blockchain in construction business process and information integration. **Automation in construction**, Elsevier, v. 118, p. 103276, 2020.

YANG, Yao-Tsung *et al.* Blockchain-Based Traffic Event Validation and Trust Verification for VANETs. **IEEE Access**, IEEE, v. 7, p. 30868–30877, 2019.

YANG, Zhe *et al.* A blockchain-based reputation system for data credibility assessment in vehicular networks. *In:* IEEE. PERSONAL, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on. [S.l.: s.n.], 2017. P. 1–5.

YUAN, Yong; WANG, Fei-Yue. Towards blockchain-based intelligent transportation systems. *In:* IEEE. 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). [S.l.: s.n.], 2016. P. 2663–2668.

ZHANG, Jie. A survey on trust management for VANETs. *In:* IEEE. 2011 IEEE International Conference on Advanced Information Networking and Applications. [S.l.: s.n.], 2011. P. 105–112.

ZHANG, Rui; XUE, Rui; LIU, Ling. Security and privacy on blockchain. **ACM Computing Surveys (CSUR)**, ACM New York, NY, USA, v. 52, n. 3, p. 1–34, 2019.

ZHENG, Zibin *et al.* An overview of blockchain technology: Architecture, consensus, and future trends. *In:* IEEE. 2017 IEEE international congress on big data (BigData congress). [S.l.: s.n.], 2017. P. 557–564.

ZHENG, Zibin *et al.* Blockchain challenges and opportunities: A survey. **Work Pap.–2016**, 2016.

APÊNDICE A – REVISÃO SISTEMÁTICA

Uma revisão sistemática da literatura é um estudo que segue um processo de pesquisa metodologicamente definido para identificar, analisar e interpretar as evidências disponíveis relacionadas a pesquisas relevantes de maneira imparcial e reprodutível.

Segundo (KEELE *et al.*, 2007), são necessárias quatro etapas para realizar uma revisão sistemática da literatura: (a) identificação dos recursos (questão de pesquisa, palavras-chave e fontes); (b) seleção dos estudos; (c) extração de dados; e (d) análise de dados.

Estabelecer a questão de pesquisa é a parte mais importante de uma revisão sistemática. O processo de revisão visa encontrar e analisar estudos primários que respondam à questão de pesquisa que foi formulada. Para identificar e selecionar esses estudos, um protocolo de busca foi definido e realizado.

Este apêndice apresenta o protocolo de busca para realização da RSL, que visa identificar trabalhos que apresentem (descrevem) gerenciamento de confiança e reputação em redes veiculares utilizando *blockchain*, as tecnologias e padrões utilizados, o ambiente nos quais a solução proposta foi aplicada, como os trabalhos foram desenvolvidos e avaliados e possíveis questões em aberto. Ao decorrer deste apêndice serão descritos os resultados da revisão sistemática e a descrição, quais filtros foram aplicados para chegar ao resultado final, resultando em uma lista de trabalhos relacionados.

A.1 PLANEJAMENTO DA RSL

A.1.1 Objetivo

Esta revisão sistemática procura identificar, analisar e avaliar trabalhos encontrados na literatura que utilizam gerenciamento de confiança e/ou reputação no contexto das redes veiculares utilizando tecnologia *blockchain*.

A.1.2 Questões de Pesquisa

Um protocolo de busca foi definido e executado em dezembro de 2021 para localizar e selecionar os trabalhos visando responder à seguinte questão de pesquisa:

- Questão Principal: Quais os modelos de confiança e/ou reputação são mais abordados na literatura atualmente utilizando a tecnologia de *blockchain* em redes veiculares?

Para complementar os resultados e definir de forma mais sucinta o escopo deste trabalho, também são definidas as seguintes questões secundárias:

- Questão Secundária 1: Que problemas eles procuram resolver?
- Questão Secundária 2: Que métricas foram utilizadas na avaliação do seu desempenho?
- Questão Secundária 3: Que problemas não foram abordados?

A.1.3 Protocolo de Busca

Nesta etapa foi necessária a definição e combinação de palavras-chave e *queries* como estratégia de busca de artigos nas bases de dados. Com base na questão de pesquisa, apenas os estudos publicados na língua inglesa foram considerados de acordo com a *string* de busca desenvolvida:

("vanet"OR "vehicular ad hoc network") AND ("blockchain") AND ("trust"OR "trustworthiness"OR "Reputation")

A execução do protocolo de busca foi realizada no mês de dezembro de 2021. Para tanto, foram consideradas as cinco fontes mais relevantes na área, sendo estas (organizadas em ordem alfabética):

- ACM Digital Library: http://portal.acm.org
- IEEExplore: http://ieeexplore.ieee.org
- Science Direct: http://www.sciencedirect.com/
- Scopus: http://www.scopus.com/
- Springer http://link.springer.com/

A Figura 27 apresenta o fluxograma das atividades executadas na RSL. Para obter a primeira lista de possíveis trabalhos, executou-se a *string* de busca nas fontes citadas, considerando título e resumo e, em caso de dúvidas na seleção, foi lida sua introdução. Visando um refinamento da seleção dos estudos, todos os artigos, previamente selecionados, foram lidos na íntegra para confirmar que estes realmente respondem à questão de pesquisa.

A.1.4 Critérios de inclusão e exclusão

Os critérios pré-definidos para inclusão e exclusão de trabalhos nesta revisão sistemática são apresentados na Tabela 18. Entre os artigos analisados foram excluídos aqueles não escritos em inglês, com publicações repetidas, *surveys* e trabalhos nos quais títulos e resumos apresentavam informações conflitantes, ou seja, o título referia-se a um assunto e o resumo a outro.

Devido às diferenças entre as ferramentas de busca para cada base selecionada, a *string* de busca foi adequada para cada execução. As buscas no título e *abstract*

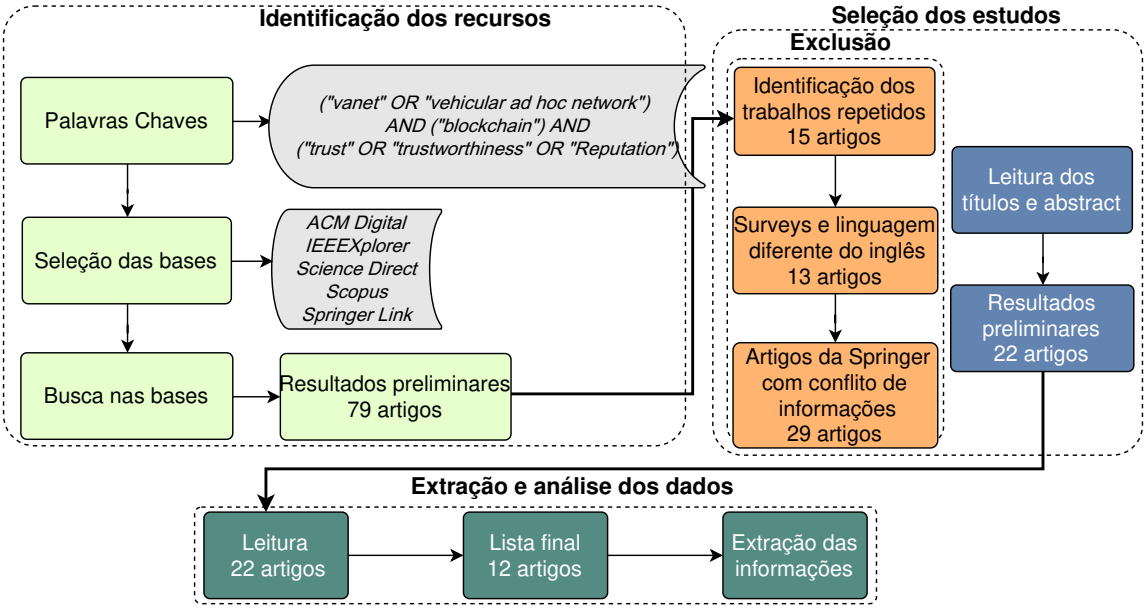


Figura 27 – Fluxograma da Revisão Sistemática

foram realizadas nas bases de dados da *ACM, IEEE e Science Direct*. Na *Scopus*, as buscas são realizada por título, resumo e palavras-chave, enquanto na *Springer Link*, as buscas são feitas em texto completo devido às limitações da ferramenta. Esta limitação resultou em um grande número de trabalhos, pois as palavras são encontradas em diversas partes do texto, que não satisfazem o contexto buscado devido ao ruído resultante.

Tabela 18 – RSL – Critérios de inclusão e exclusão

Critério	**Decisão**
As palavras-chave da string de busca foram encontradas no título/resumo do artigo.	Inclusão
O artigo evidência sistemas de reputação que utilizaram tecnologia blockchain.	Inclusão
O artigo não está acessível.	Exclusão
O artigo não está escrito em inglês.	Exclusão
O artigo é um survey.	Exclusão
O artigo está duplicado na pesquisa.	Exclusão
O artigo apresenta título e resumo com informações conflitantes.	Exclusão

A.1.5 Processo de refinamento da seleção dos estudos primários

Todos os trabalhos previamente selecionados na etapa anterior foram lidos na íntegra para confirmar que estes realmente respondem à questão de pesquisa. Verificou-se também, se a solução proposta está bem referenciada.

Após a leitura dos artigos previamente selecionados, as informações foram extraídas com os seguintes dados:

- Informação para referência bibliográfica;
- Problema alvo;
- Solução proposta;
- Metodologia utilizada; e
- Resultados obtidos;

APÊNDICE B – SMART CONTRACT

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "./ABDKMath64x64.sol";

contract RsuReputation {
    uint public carsCount;
    uint public votesCount;
    uint currentMappingVersion;
    address public owner;
    mapping(address => int128[]) public reputations;
    int128 public RepActual;
    mapping(uint => WM) public wms;
    mapping(uint => WVM[]) public wvms;
    mapping(uint => uint) public wvmCount;
     mapping(uint => string) public statusEvent;
    constructor() payable {
       carsCount = 0;
       owner = msg.sender;
    }

     struct WM {
        uint idMsg;
        address assig;
        uint256 idAlert;
        bool active;
        uint256 timstamp;
    }

    struct WVM {
        address car;
        uint idMsg;
        address assig;
        uint256 idAlert;
        bool ack;
        uint256 timstamp;
    }

    event RWM(
        uint idMsg
    );
      event RWVM(
        string idMsg
    );
      event LogAck(
        int128 ack
    );
      event LogNack(
        int128 nack
    );

     event Valido(
        int128 valido
    );
     event Reputation(
        int128 reputation
    );
    event ReputationCount (
        uint rep
    );

    function registerWM(uint _idMsg,uint256 _idAlert) public {
        wms[_idMsg] = WM(
            _idMsg,
            msg.sender,
            _idAlert,
            true,
            block.timestamp
        );

        emit RWM(_idMsg);
    }
```

```
    function registerWVM(uint _idMsg,uint256 _idAlert, bool _confirmation) public {
       //string memory key = concatenate(uint2str(_idMsg),string(abi.encodePacked("-", msg.sender)));
       // string memory key = string(abi.encodePacked(msg.sender));
       wvms[_idMsg].push(WVM(
           msg.sender,
           _idMsg,
           msg.sender,
           _idAlert,
           _confirmation,
           block.timestamp
       ));
       if(this.totalWVMByIdWM(_idMsg) >= 10){
           //emit RWVM("igual ou maior que 10");
         int128 ack = this.getAck(_idMsg);
         int128 nack = this.getNack(_idMsg);
         emit LogAck(ack);
         emit LogNack(nack);
         int128 valorVerificador = ABDKMath64x64.div(ack,ack+nack);
         setNewReputation(_idMsg,valorVerificador);
         if(valorVerificador > 8310000000000000000 && valorVerificador < 10149000000000000000){
             //aqui neutro
             statusEvent[_idMsg] = "UNDEFINED EVENT";

           emit Valido(valorVerificador);

         }

       }
       emit RWVM("vai");
   }
   function setNewReputation(uint _idMsg, int128 valorVerificador) internal {
       //0 - true event
       if(valorVerificador > 10149000000000000000) {
                statusEvent[_idMsg] = "TRUE EVENT";
           if(reputations[wms[_idMsg].assig].length > 0){
            int128 repActual = reputations[wms[_idMsg].assig][reputations[wms[_idMsg].assig].length-1];
            int128 valor1 = ABDKMath64x64.mul(repActual,valorVerificador);
            int128 valor2 = valor1-ABDKMath64x64.mul(ABDKMath64x64.mul(repActual,repActual),
valorVerificador);
            int128 newValue = repActual+valor2;
            reputations[wms[_idMsg].assig].push(newValue);
            RepActual = newValue;
            emit ReputationCount(reputations[wms[_idMsg].assig].length);
            emit Reputation(newValue);
           } else {
               reputations[wms[_idMsg].assig].push(valorVerificador);
               emit Valido(valorVerificador);
           }
       }
       //bogus event
        if(valorVerificador < 8310000000000000000) {
            statusEvent[_idMsg] = "BOGUS EVENT";
            if(reputations[wms[_idMsg].assig].length > 0){
              int128 repActual = reputations[wms[_idMsg].assig][reputations[wms[_idMsg].assig].length-1];
             //  int128 newRep = ABDKMath64x64.div(repActual+(repActual*valorVerificador),2);
              //reputations[wms[_idMsg].assig].push(newRep);
             } else {
                 reputations[wms[_idMsg].assig].push(valorVerificador);
                  RepActual = valorVerificador;
             }
       }
   }
   function totalWVMByIdWM(uint _idMsg) external view returns (uint256) {
        uint countMsg = 0;
        for (uint i = 0; i < wvms[_idMsg].length; i++) {
            if(wvms[_idMsg][i].idMsg == _idMsg){
                countMsg++;
            }
        }
       return countMsg;
```

```
    }

     function getAck(uint _idMsg) external view returns (int128) {
         int128 countAck = 1;
         for (uint i = 0; i < wvms[_idMsg].length; i++) {
             if(wvms[_idMsg][i].ack){
                 countAck++;
             }
         }
         return countAck;
    }
   function getNack(uint _idMsg) external view returns (int128) {
         int128 countNack = 1;
         for (uint i = 0; i < wvms[_idMsg].length; i++) {
             if(!wvms[_idMsg][i].ack){
                 countNack++;
             }
         }
         return countNack;
    }

    function concatenate(string memory s1, string memory s2) public pure returns (string memory) {
        return string(abi.encodePacked(s1, s2));
    }

    function uint2str(uint _i) internal pure returns (string memory _uintAsString) {
        if (_i == 0) {
            return "0";
        }
        uint j = _i;
        uint len;
        while (j != 0) {
            len++;
            j /= 10;
        }
        bytes memory bstr = new bytes(len);
        uint k = len;
        while (_i != 0) {
            k = k-1;
            uint8 temp = (48 + uint8(_i - _i / 10 * 10));
            bytes1 b1 = bytes1(temp);
            bstr[k] = b1;
            _i /= 10;
        }
        return string(bstr);
    }
}
```

Anexos

ANEXO A – VALORES DE GANHO — CALIBRAÇÃO

Uma análise de sensibilidade foi efetuada neste trabalho para fazer a calibração dos valores de ganho usados pelo BRS4VANETs. Esse anexo apresenta de forma gráfica os valores obtidos durante essa análise.

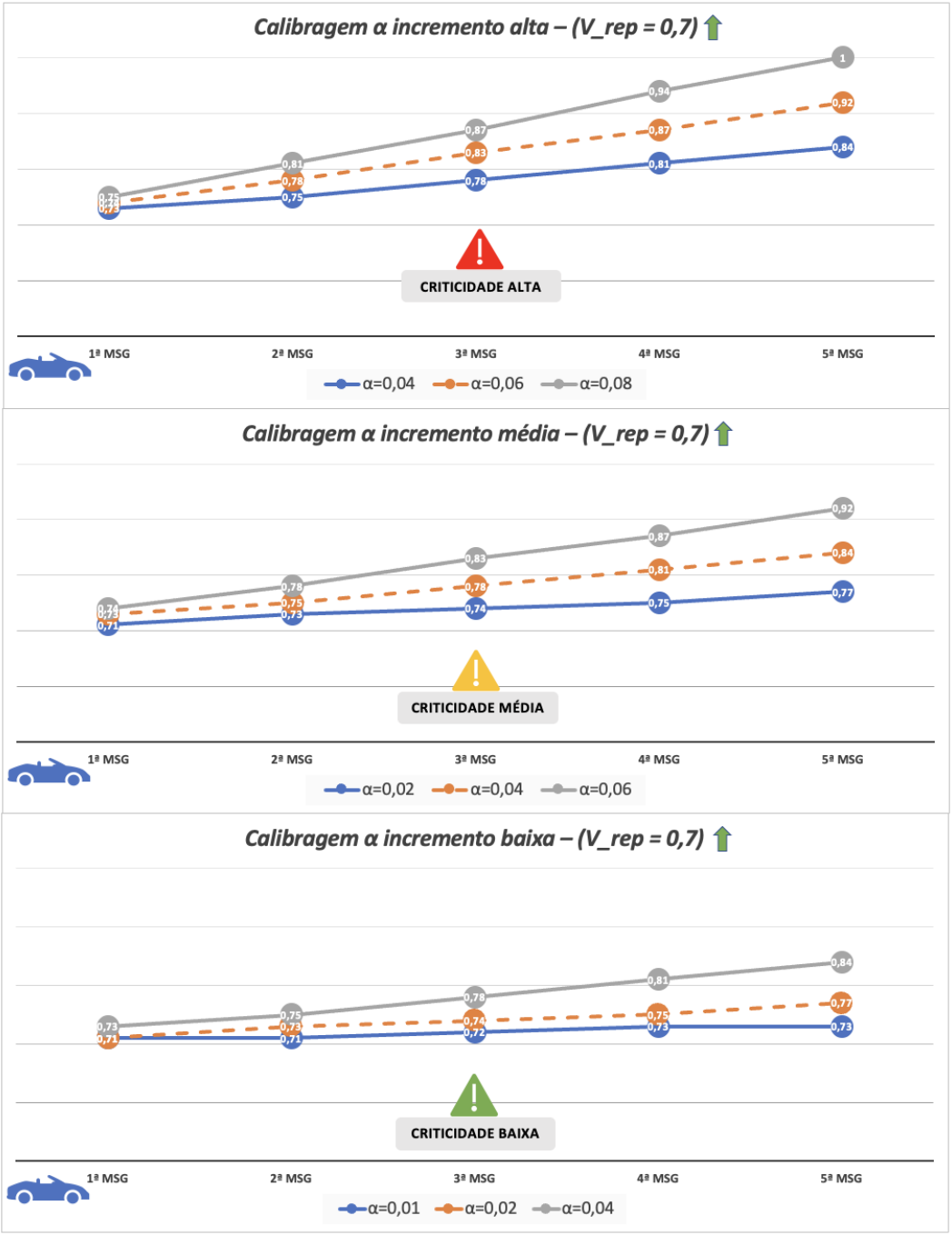


Figura 28 – Calibragem α V_rep=0,7

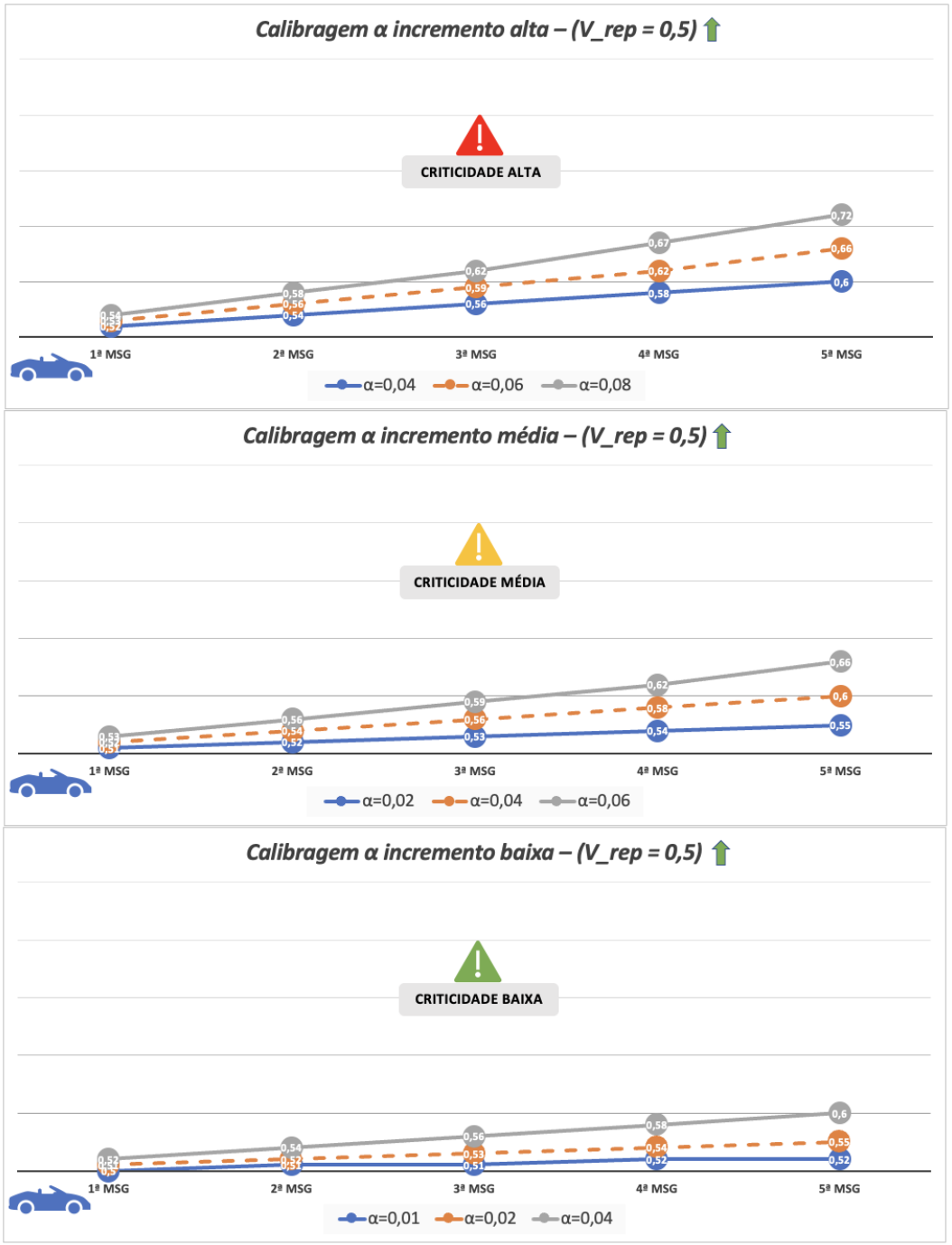


Figura 29 – Calibragem α V_rep=0,5

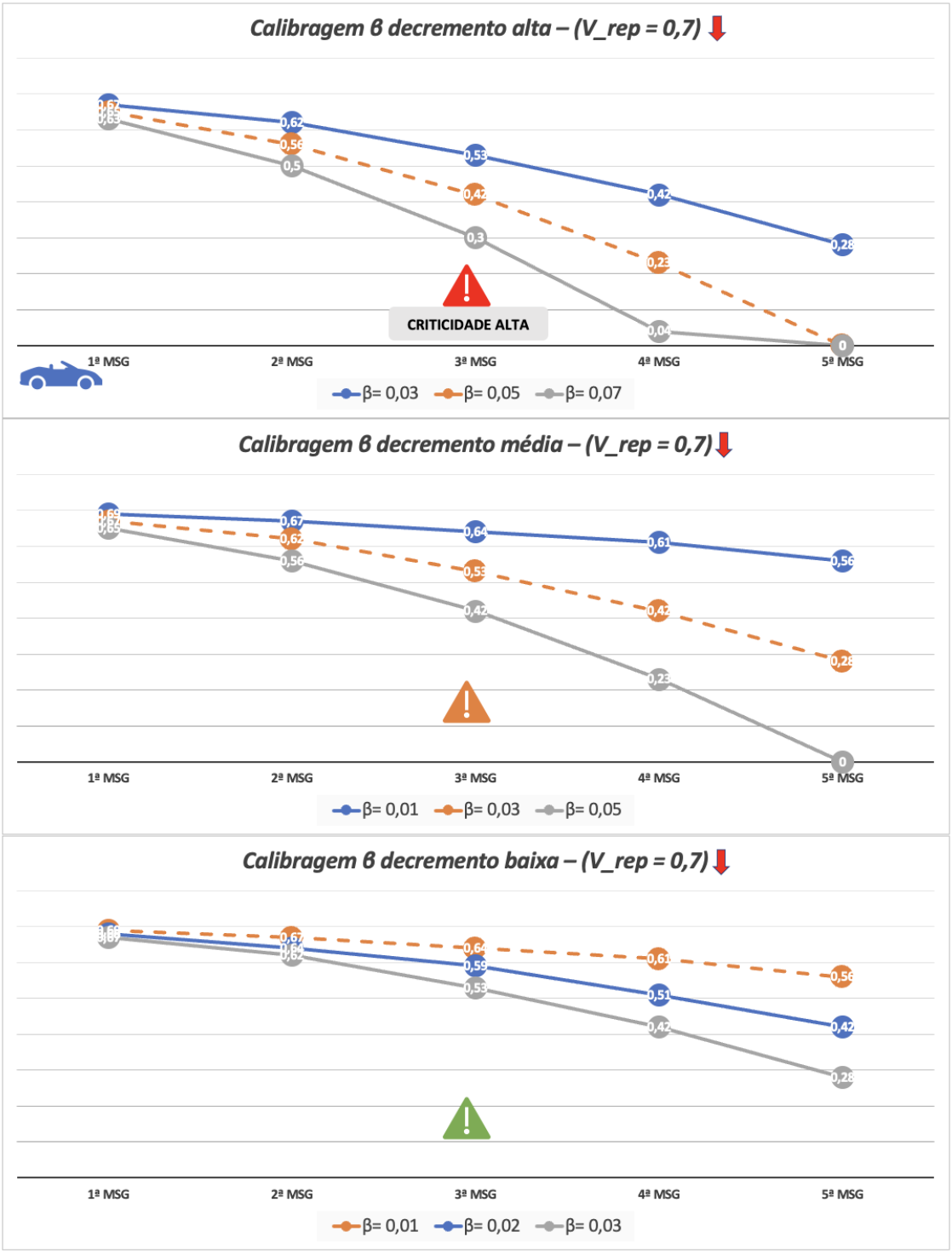


Figura 30 – Calibragem β V_rep=0,7

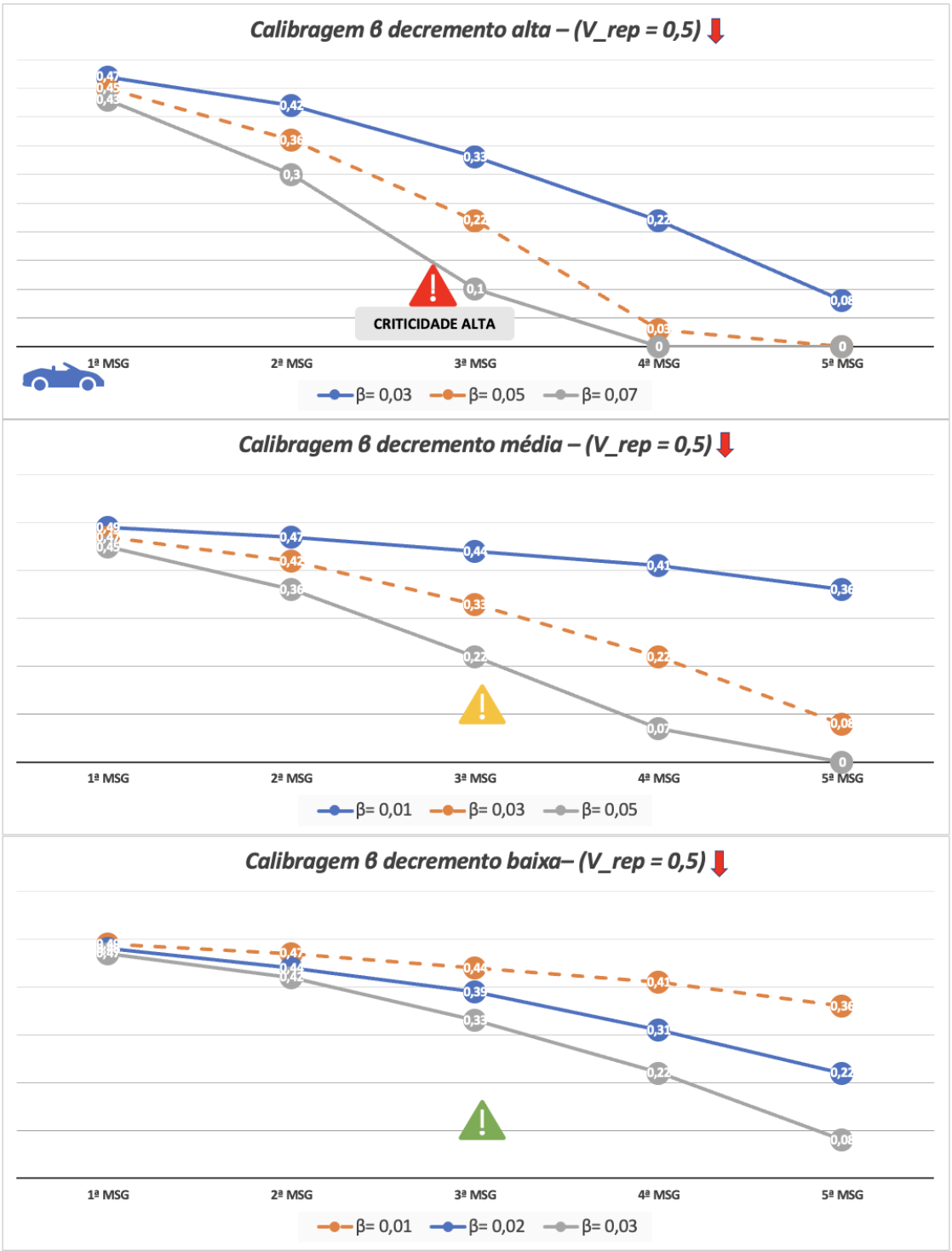


Figura 31 – Calibragem β V_rep=0,5