Um sistema de reputação baseado em Blockchain contra ataques de mensagens falsas em VANETs

Claudio Piccolo Fernandes[1,2], Carlos Montez[2], Daniel Domingos Adriano[3], Michelle Silva Wangham[3]

[1]Centro Universitário Estácio de Santa Catarina - São José, SC, Brasil

[2]Universidade Federal de Santa Catarina - UFSC, Florianópolis, SC, Brasil

[3]Universidade do Vale do Itajaí - UNIVALI, São José, SC, Brasil

Abstract. *One of the main threats to a vehicular network is malicious vehicles that generate false or inappropriate messages. Incoming messages, such as information about accidents, congestion, etc., need to be verified before action is taken. This paper proposes a consortium blockchain-based reputation system using smart contracts to analyze vehicle reliability, identify malicious ones and contribute to decision making. Simulation results show the impact that false messages have on vehicular networks without using a reputation system and the feasibility of using blockchain technology to store reputations.*

Resumo. *Uma das principais ameaças a uma rede veicular são os veículos maliciosos que geram mensagens falsas ou impróprias. As mensagens recebidas, tais como informações sobre acidentes, congestionamento, entre outras, precisam ser verificadas antes que uma ação seja tomada. Este trabalho propõe um sistema de reputação baseado em blockchain de consórcio e uso de contrato inteligente de forma a analisar a confiança dos veículos, identificar os maliciosos e contribuir para a tomada de decisão. Resultados de simulações demostram o impacto provocado por mensagens falsas nas redes veiculares sem a utilização de um sistema de reputação e a viabilidade do uso da tecnologia blockchain no armazenamento das reputações.*

1. Introdução

Sistema de Transportes Inteligentes (STI) é um conceito genérico que designa categorias de aplicações que são integradas com tecnologias de comunicações, controle e processamento de informações do sistema de transporte [Garg et al. 2019]. As redes veiculares ou VANETs (*Vehicular Ad hoc Network*), juntamente com os avanços tecnológicos incorporados aos veículos automotivos, formam a espinha dorsal da nova geração dos STIs.

As VANETs possuem como objetivo melhorar as condições de tráfego urbano e rodoviário de forma segura e eficiente, garantindo a comunicação entre os diversos nós inseridos na rede, oferecendo as condições necessárias para que aplicações, com diferentes requisitos, sejam desenvolvidas [Baza et al. 2020]. Para isso, é fundamental que os nós da rede tenham confiança nas informações trocadas com seus vizinhos, pois decisões tomadas com base em informações erradas ou manipuladas podem levar à diminuição da segurança no trânsito [Feng et al. 2017].

Uma das soluções propostas para lidar com esses problemas são os sistemas de reputação. Um sistema de reputação robusto para redes veiculares deve ser capaz de reagir a possíveis ataques, reduzindo a reputação de veículos maliciosos para minimizar seus

efeitos. Contudo, a detecção de ações e comportamentos de nós maliciosos é um problema complexo [Gong et al. 2019]. Minimizar os ataques e as consequências de comportamentos maliciosos é muito importante em soluções que necessitam da cooperação e da honestidade dos nós, tais como as aplicações de segurança no trânsito, dado que, devido à sua topologia dinâmica e efêmera, o estabelecimento de relações de confiança entre os nós em redes veiculares torna-se um desafio. Dentro da categoria de comportamentos maliciosos, este trabalho endereça os ataques de mensagens de alerta falsos (*Bogus attack*), no qual um veículo malicioso cria uma situação específica de tráfego para enganar outros motoristas através de disseminação de informações falsas [Celes and Elizabeth 2018]. Isso pode criar uma interpretação errônea do cenário real para os veículos próximos, causando consequências como acidentes, congestionamentos e mudanças de percursos.

Pelo fato de possuir uma infraestrutura computacional segura e descentralizada, a tecnologia *blockchain* é reconhecida como uma solução disruptiva para os problemas de privacidade e segurança ao armazenar, monitorar, gerenciar e compartilhar dados na rede. Desse modo, torna-se interessante a sua utilização para a construção de um modelo de gerenciamento de confiança nas redes veiculares [Kang et al. 2018].

Este trabalho apresenta um sistema de gerenciamento de confiança distribuído, utilizando uma *blockchain* de consórcio e contrato inteligente que visa analisar e registrar a reputação e o comportamento dos veículos de forma a identificar a presença de nós maliciosos e contribuir para tomada de decisões. As simulações demonstram que propagação de mensagens falsas na rede veicular causa impactos relevantes e que o uso do sistema de reputação proposto mitiga este tipo de ataque. Além disso, os resultados obtidos indicam um *overhead* aceitável no uso da *blockchain* no armazenamento das reputações, executado nas RSUs (*Road Side Unit*).

O artigo está organizado da seguinte forma. Na Seção 2 são apresentados trabalhos relacionados. Na Seção 3 é detalhado o sistema de reputação proposto. Os resultados da avaliação do sistema são discutidos na Seção 4. A Seção 5 apresenta as conclusões e trabalhos futuros.

2. Trabalhos Relacionados

A literatura tem revelado diferentes abordagens aos sistemas de reputação no contexto das redes veiculares. Esta seção apresenta os trabalhos correlatos encontrados na literatura que utilizam modelos de confiança e/ou sistemas de reputação com o objetivo de avaliar a credibilidade das mensagens e/ou nós, visando evitar ou minimizar os possíveis ataques de nós maliciosos em redes veiculares aplicando tecnologia *blockchain*.

[Yang et al. 2017] propõem um mecanismo de avaliação de credibilidade para a Internet de veículos em que a credibilidade das mensagens recebidas são estimadas com base na reputação do seu remetente e armazenadas em uma *blockchain*. Nesse trabalho, o custo adicional da *blockhain*, para alcançar o consenso, não foi avaliado.

[Lu et al. 2018] apresentam um mecanismo de reputação que determina a credibilidade de um veículo com base em interações históricas para impedir a distribuição de mensagens falsas. O alto custo computacional ocasionado pelo emprego do mecanismo de consenso PoW não foi discutido no trabalho.

Em [Kchaou et al. 2018], um sistema de gerenciamento de confiança com uso de tecnologia *blockchain* é proposto com o foco de estimar a credibilidade das mensagens

Tabela 1. Análise dos trabalhos relacionados

Autores	Solução Proposta	Categoria da Blockchain	Local da Blockchain	Limitações
[Yang et al. 2017]	Evitar a geração de eventos falsos e garantir a credibilidade das mensagens.	Pública	Veículo	Análise da segurança não realizada.
[Lu et al. 2018]	Garantir a privacidade com uso de pseudônimos.	Pública	RSU	Implementação da *blockchain*.
[Kchaou et al. 2018]	Avaliar o comportamento dos veículos através de um gerenciamento de confiança.	Pública	RSU	Preservação da privacidade dos dados.
[Kang et al. 2018]	Avaliar o comportamento dos veículos através de um gerenciamento de confiança.	Consórcio	RSU	Custo computacional em tempo real.
[Yang et al. 2019]	Garantir a confiança e aumentar a segurança nas VANETs.	Pública	RSU	Reputação dos veículos não considerada.
[Shrestha et al. 2020]	Avaliar a credibilidade da mensagem e dos veículos.	Pública	Veículo RSU	Latência e tempo de geração dos blocos.
[Javed et al. 2020]	Garantir a troca de dados segura entre os veículos.	Pública	RSU	Alto custo computacional.
[Khalid et al. 2021]	Garantir a segurança contra ataques maliciosos através de incentivos.	Consórcio	RSU	Custo computacional para formação do consenso (PoW)
Sistema proposto	Garantir a segurança contra ataque de mensagens falsas em redes veiculares.	Consórcio	RSU	Falta de uma analise para definição da área de interesse alinhada ao tamanho da rede de blockhain

disseminadas, com base em um valor de reputação do emissor. Entretanto, não houve avaliação do desempenho deste mecanismo.

[Kang et al. 2018] propõem uma *blockchain* de consórcio e contrato inteligente para construir um sistema de compartilhamento de dados seguros. O sistema de reputação é implementado, usando um modelo lógico subjetivo de três pesos. Nas simulações apresentadas, o processo de autenticação e segurança não obteve bom desempenho na avaliação executada em tempo real.

[Yang et al. 2019] apresentam um mecanismo que visa garantir a confiabilidade dos eventos e confirmar a validade de suas ocorrências com o uso da *blockchain*. Focado na confiabilidade da mensagem, os autores definiram um novo algoritmo de consenso denominado Prova de Evento (PoE). Entretanto, o sistema não considera a reputação dos veículos e seu histórico.

[Shrestha et al. 2020] integram um sistema de confiança, no qual a confiabilidade da mensagem e a confiabilidade do nó são armazenadas em uma *blockchain* utilizando servidores de borda para reduzir a latência na geração dos blocos. Apenas são discutidas a escalabilidade e a sobrecarga de armazenamento da *blockchain*, mas não há nenhuma avaliação experimental.

[Javed et al. 2020] propõem um sistema de recompensa, usando incentivos de contrato inteligente com base no cálculo de valores de reputação do veículo. Um mecanismo de gerenciamento de confiança também é apresentado para calcular os valores de reputação dos nós com base em sua confiança.

[Khalid et al. 2021] propõem um sistema de incentivos, utilizando *blockchain* de consórcio e contrato inteligente para validar os eventos de tráfego. No sistema, a reputação dos veículos é calculada com base em seus eventos anteriores e a *blockchain* é utilizada para armazenar os valores de reputação dos veículos.

Conforme os trabalhos analisados, um dos desafios encontrados nas redes veiculares diz respeito à inserção de novos mecanismos para tornar a rede mais segura e confiável, sem o risco de comprometer o seu desempenho. Alguns aspectos comparativos foram destacados conforme pode ser observado na Tabela 1.

3. Sistema Proposto

No modelo de rede do sistema adotado (Figura 1), os nós são formados por RSUs e veículos com OBUs (*On-Board Units*), os quais trocam mensagens entre si, caracterizando uma comunicação V2V (*Vehicle to Vehicle*) e V2I (*Vehicle to Infrastructure*). O nível de confiança dos veículos varia temporalmente e as RSUs são as entidades responsáveis pelos cálculos e armazenamento destes valores de reputação na *blockchain*. Como diferentes concessionárias podem gerir as RSUs ao longo da via, a *blockchain* tem um importante papel de manter a integridade das informações de reputação. Os veículos são responsáveis pela validação dos eventos ocorridos e propagados por outros veículos, contribuindo desta forma para o processo de composição da reputação.

Além da reputação, a *blockchain* armazena e gerencia o histórico das mensagens enviadas pelos veículos que atestaram o evento referente ao comportamento do veículo emissor das mensagens de alerta. Essa abordagem permite uma posterior análise do comportamento dos nós dentro de um determinado período e implementar. por exemplo, políticas que recompensem aqueles com bom histórico de reputação através de um sistema de recompensas envolvendo redução de valores de pedágio, seguro ou IPVA.

Cada veículo ao ingressar na rede recebe uma tabela (Tab-ID-Rep), enviada pelas RSUs, a qual contém apenas os veículos considerados suspeitos e maliciosos, ou seja, os veículos com reputações menores que o limiar de reputação (*Th_Rep*). O modelo considera ainda uma cadeia de autoridades certificadoras para prover um gerenciamento eficiente da emissão de certificados digitais usados pelos veículos.

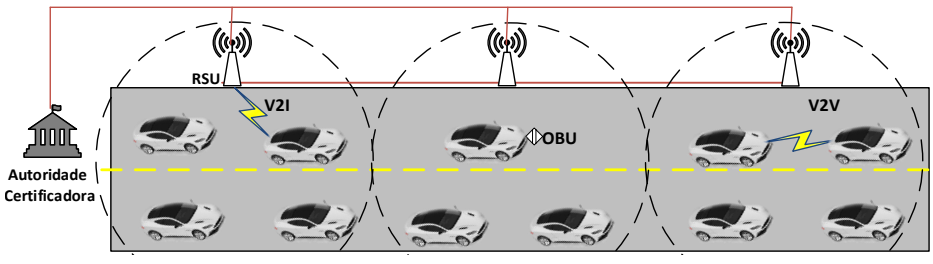

Figura 1. Modelo da rede veicular

A arquitetura do sistema é composta por três módulos. O **módulo registrar veículo** faz o registro junto a uma AC para emitir o certificado digital do veículo e esse possa fazer parte da rede. O **módulo gerenciar mensagens** cria e gerencia duas categorias de mensagens: a WM (*Warning Message*) e a WVM (*Warning Validation Message*). Por fim, o **módulo gerenciar reputação dos veículos**, que é de responsabilidade das RSUs. A Figura 2 ilustra o processo do registro de um veículo, seu ingresso na rede, a criação e disseminação da mensagem WM.

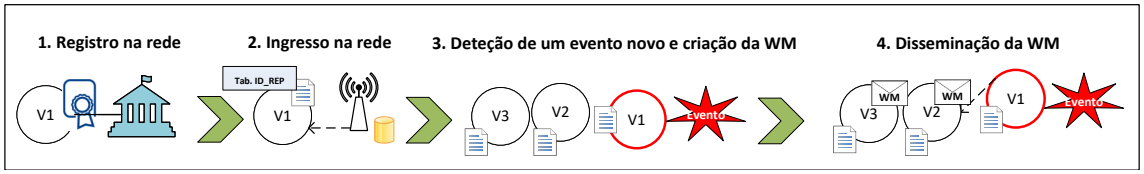

Figura 2. Registro de um veículo e disseminação da WM

Toda vez que o sensor de um veículo detectar um evento na rodovia, uma mensagem WM é criada e distribuída reportando o alerta/perigo, conforme pode ser observado no Algoritmo 1.

Algoritmo 1: Criação da Mensagem de Alerta – WM

```
1  início
2      se (veículo i detectar evento) então
3          x_i ← Obter coordenada do GPS do veículo referente à latitude;
4          y_i ← Obter coordenada do GPS do veículo referente à longitude;
5          ID_A ← Obter o identificador do alerta referente ao evento;
6          TimeStamp ← Obter data e hora do evento;
7          ID_M ← Calcular hash (ID_A, ID_V, x_i, y_i, TimeStamp);
8          Assig ← Assinar ID_M;
9          WM ← GeraMsg(ID_M, Assig, ID_A, ID_V, Crit_A, x_i, y_i, TimeStamp, Cert_v);
10         Enviar WM;
11     fim
12 fim
```

O valor da reputação de um veículo é calculado com base na correção de um evento que este iniciou por meio da WM. Assim, caso o evento já tenha sido relatado por outro veículo anteriormente, este irá validar o alerta por meio da mensagem WVM, confirmando (*Ack*) ou negando a ocorrência (*Nack*) desse evento, conforme Algoritmo 2. A adição desta mensagem visa certificar a confiabilidade das mensagens WM recebidas entre os veículos, e serve posteriormente para identificar eventos falsos relatados por nós maliciosos. O diagrama de atividades ilustrado na Figura 3 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 que serão tomadas.

Algoritmo 2: Verificar Evento – WVM

```
1  início
2      para cada WM recebida faça
3          evento ← WM
4          se ( evento=true ) então
5              Ack ← 1;    /* Campo de WVM que confirma que o evento relatado na WM foi
                 detectado pelo sensor do veículo */
6          fim
7          senão
8              Nack ← 1;    /* Campo de WVM que confirma que o evento relatado na WM não
                 foi detectado pelo sensor do veículo */
9          fim
10         Enviar WVM;    /* Envia WVM à RSU mais próxima */
11     fim
12 fim
```

A RSU mais próxima consolida as informações, as quais contêm as assinaturas

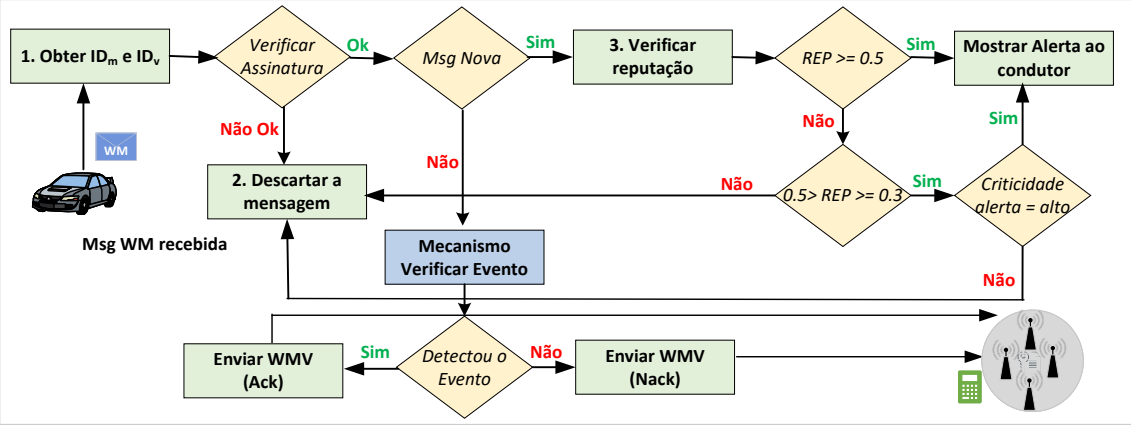

Figura 3. Diagrama de tratamento da mensagem WM recebida

de cada veículo, com base nos números de *Acks* e *Nacks* recebidos. Cada veículo possui um valor de reputação que reflete o seu comportamento na rede. O cálculo da agregação das n mensagens WMV recebidas (*Acks ou Nacks*) é realizado pela Equação 1, e esse valor denominado Rep_V irá compor o valor de reputação do veículo a ser armazenado posteriormente na *blockchain*.

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

As opiniões sobre o comportamento dos veículos são sinalizadas por veículos vizinhos que verificam a confiabilidade das mensagens de alerta geradas. A reputação de um veículo aumenta à medida que este se comporta de maneira correta e reduz com suas ações maliciosas. Desta forma, as RSUs têm a função de consolidar e armazenar as opiniões recebidas dos veículos, por meio da Equação 1 e, a partir dos resultados consolidados, a reputação do veículo emissor do alerta será alterada e gravada na rede *blockchain*. Entretanto, tendo em vista aumentar a segurança das decisões tomadas, o sistema proposto recorre a um mecanismo de votação que mitiga ataques de conluio de veículos maliciosos. Assim, é realizada uma coleta de informações (*Acks/Nacks*) pelas RSUs, dentro do seu raio de cobertura, para calcular a confiabilidade da mensagem e, a partir desses resultados, as seguintes ações são tomadas (Algoritmo 3):

- **Evento Verdadeiro (*True Event* - TE):** Se a maioria dos veículos destinatários validar o evento da mensagem de alerta (linha 10), este é considerado como verdadeiro (linha 12) e a pontuação da reputação do veículo emissor do alerta será aumentada e posteriormente gravada na *blockchain* (linha 13)
- **Evento Falso (*Bogus Event* - FE):** Se a maioria dos destinatários não validar o evento da mensagem de alerta (linha 15), este é considerado falso (linha 17) e a pontuação da reputação do veículo será decrementada e posteriormente gravada na *blockchain* (linha 18).
- **Evento Indefinido (*Undefined Event* - UE)**: Caso o total dos veículos que validaram o evento como verdadeiro seja próximo dos que o validaram como falso (linha 20), este é considerado como indefinido (linha 22), pois não há evidências suficientes que o possa validar. Assim, a RSU não altera a reputação.

Algoritmo 3: Sistema de votação e atualização da Reputação

```
1  início
2      para cada WVM recebida pela RSU faça
3          x ← x+1;
4          se x > 10 então
5              Ack ← Ack(WVM)    /* Campo Ack da mensagem WVM */
6              Nack ← Nack(WVM) /* Campo Nack da mensagem WVM */
7              Ack ← Ack +1;
8              Nack ← Nack +1;
9              Calcular Rep_V usando Equação 1;
10             se (Rep_V ≥ 0.55 ) então
11                 /* A nova reputação do emissor do alerta é incrementada */
12                 Status_Evento ← True Event;
13                 Calcular Rep_New usando Equação 2;
14             fim
15             se (Rep_V ≤ 0.45 ) então
16                 /* A nova reputação do emissor do alerta é decrementada */
17                 Status_Evento ← Bogus Event;
18                 Calcular Rep_New usando Equação 3;
19             fim
20             se (Rep_V > 0.45) e (Rep_V < 0.55) então
21                 /* Não calcula nova reputação: não há evidências conclusivas sobre o evento */
22                 Status_Evento ← Undefined Event;
23             fim
24         fim
25     fim
26 fim
```

Após o mecanismo de votação, caso o valor da Equação 1 for $Rep_V \geq 0.55$, isso indica que a maioria dos veículos atestou como verdadeiro o evento e o valor da reputação do veículo emissor da mensagem de alerta (WM) será incrementado, conforme a Equação 2 e armazenado na *blockchain* para disseminação aos veículos na rede:

$$Rep_{New} = Rep_{Act} + (Rep_{Act} * Rep_V) - ((Rep_{Act})^2 * Rep_V) \tag{2}$$

onde Rep_{Act} refere-se à reputação atual do veículo emissor do alerta armazenada na *blockchain*, Rep_V corresponde ao cálculo de agregação dos *feedbacks* recebidos pelos veículos (Equação 1) e, por fim, Rep_{New} representa a nova reputação do veículo.

Caso o resultado da Equação 1 for $Rep_V \leq 0.45$, o valor da reputação do veículo será drasticamente reduzido. Nesse sentido, sua redução se dará pela metade, conforme a Equação 3, pois a maioria dos veículos não confirmou o evento relatado.

$$Rep_{New} = \frac{Rep_{Act} + (Rep_{Act} * Rep_V)}{2} \tag{3}$$

Como pode ser observado, o sistema proposto reduz a reputação de um veículo que esteja enviando mensagens falsas na rede, e aumenta gradativamente a sua reputação quando este envia mensagens verdadeiras. De modo a avaliar o nível de confiança do veículo, o limiar de reputação (*Th_Rep*) é uma variável parametrizável do sistema. O sistema segue uma abordagem otimista, ou seja, todo veículo ao ingressar na rede pela primeira vez terá seu valor de reputação inicial definido com o valor do *threshold* de reputação.

Para fins de tomada de decisão, conforme a criticidade da mensagem de alerta (WM), o veículo irá mostrar ou descartar a mensagem recebida ao condutor com base no limiar de reputação (*Th_Rep*) do veículo emissor. O Algoritmo 4 apresenta os passos a

serem executados após o recebimento da mensagem considerando um *Th_Rep* = 0.5.

Algoritmo 4: Tomada de decisão para Mensagem de Alerta recebida;

```
1  WM_i : Mensagem de alerta recebida pelo veículo i
2  Th_Rep : Limiar de reputação
3  Tab-ID-Rep : Lista de reputação recebida da RSU
4  Crit_Msg : Criticidade da WM
5  início
6      para cada WM recebida faça
7          Th_Rep ← Tab-ID-Rep
8          se ( Th_Rep ≥ 0.5 ) então
9              /* Veículo considerado confiável */
10             Mostrar a mensagem de alerta ao condutor;
11             se ( Th_Rep > 0.3 e Th_Rep ≤ 0.5 e Crit_Msg=alta) então
12                 /* Veículo considerado suspeito */
13                 Mostrar a mensagem de alerta ao condutor;
14                 senão
15                     Descartar a mensagem de alerta sem mostrar ao condutor;
16                 fim
17             fim
18         fim
19         senão
20             /* Veículo considerado malicioso */
21             Descartar a mensagem de alerta sem mostrar ao condutor;
22         fim
23     fim
24 fim
```

Neste exemplo, um veículo com $Th\_Rep \geq 0.5$ será considerado confiável. Veículos com $Th\_Rep < 0.5$ podem ser categorizados em dois tipos: veículo suspeito ou veículo malicioso. Um veículo é considerado suspeito quando este possuir $Th\_Rep > 0.3$ e $Th\_Rep \leq 0.5$ e veículos com $Th\_Rep < 0.3$ serão considerados maliciosos. As RSUs propagam a tabela contendo apenas os veículos com limiar de reputação abaixo de 0.5, ou seja, somente veículos considerados suspeitos ou maliciosos.

3.1. Sistema da Blockchain

O sistema proposto utiliza uma *blockchain* de consórcio, empregando tecnologias de contratos inteligentes (*smart contracts*), conforme pode ser observado na Figura 4, visto que oferece um alto nível de segurança em ambientes de compartilhamento de dados e menores custos nos seus processos de mineração.

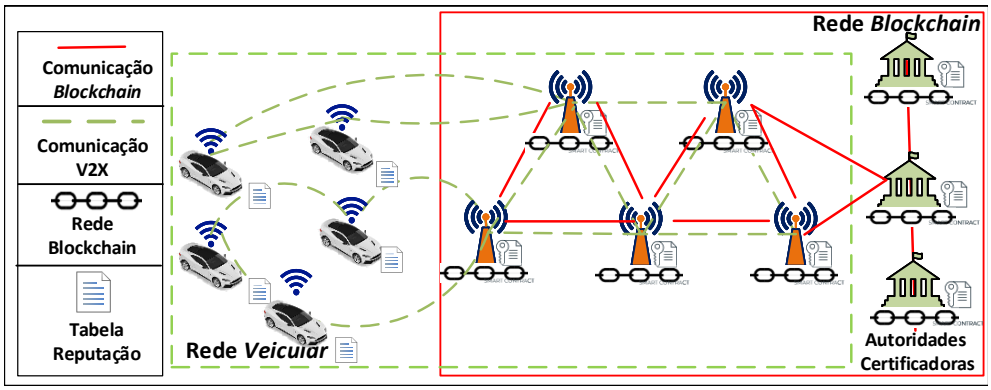

Figura 4. Arquitetura geral da rede *blockchain*

A blockchain de consórcio é uma *blockchain* específica na qual um conjunto selecionado de nós são responsáveis por validar e manter os dados compartilhados e distribuídos. Neste trabalho, os nós pré-selecionados são as RSUs, as quais têm o direito de controlar o processo de consenso e escrever na *blockchain* veicular, sendo responsáveis por compartilhar o valor de reputação dos veículos sem depender de terceiros confiáveis.

As informações do evento, como engarrafamentos e acidentes rodoviários, são relevantes para uma determinada localização geográfica, não sendo de interesse para outras regiões. Desta forma, o sistema proposto adota uma *blockchain* local que registra reputações e históricos de mensagens apenas de veículos em uma determinada rodovia, amenizando assim, os problemas de escalabilidade na rede.

Devido às restrições de recursos dos veículos, a *blockchain* é implementada apenas nas RSUs. Entretanto, os veículos participantes da rede veicular são mensageiros externos, responsável por contribuir no processo do cálculo de reputação, executado pelas RSUs antes da gravação do bloco, com os novos valores de reputação através de um sistema de votação.

O sistema adota o algoritmo de consenso PoA (*Proof of Authority*) devido ao seu desempenho e benefícios, quando usado em redes permissionadas, como o número reduzido de trocas de mensagens e baixo *overhead*. Neste mecanismo, usa-se um *pool* de nós (RSUs) de validação, chamado validadores, para determinar se um bloco proposto é adequado para adição à cadeia. Assim, uma RSU é selecionada arbitrariamente como proponente e torna-se responsável por construir um bloco e compartilhá-lo com as demais RSUs na rede. Se a maioria considerar o bloco válido, então esse é adicionado à *blockchain*. Os detalhes são descritos a seguir:

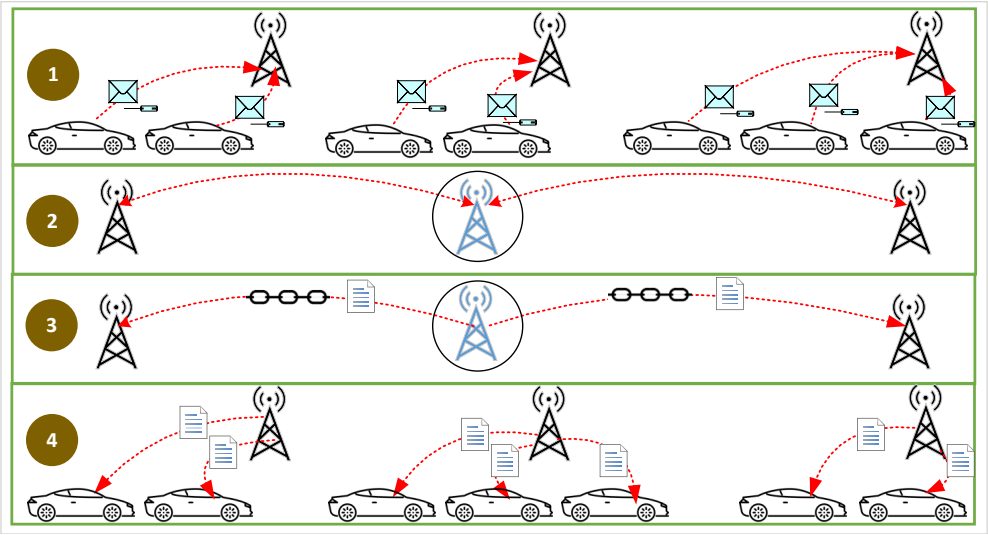

Figura 5. Formação do consenso

1. Os veículos são atores externos que participam do mecanismo de consenso, por votações encaminhadas a RSU, através das mensagens de validação de eventos (WVM);
2. Um líder é escolhido arbitrariamente entre as RSUs participantes da rede tornando-se responsável por construir um bloco e compartilha-lo com as outras RSUs;

3. Como consequência do processo de consenso, se a maioria atestar o bloco como válido, a RSU líder faz a gravação deste na *blockchain* e envia a Tabela de Reputação (*Tab-ID-Rep*) às demais RSUs;
4. Por fim, as RSUs disseminam a Tabela de Reputação (Tab-ID-Rep) aos veículos contendo os valores de reputações abaixo do limiar 0.5.

A *blockchain* de consórcio do sistema proposto, denominada *Reputation-BC*, é responsável pelo registro e armazenamento dos valores de reputação dos veículos que fazem parte da rede veicular. Todas as informações contidas na *blockchain* são armazenadas e compartilhadas via RSU. A *Reputation-BC* também armazena e gerencia o histórico das mensagens referente ao comportamento do veículo no tratamento das mensagens de alerta. Com o objetivo de ser uma prova permanente, as mensagens referentes aos comportamentos maliciosos são registradas na *blockchain*.

4. Simulação e análise dos resultados

Esta seção descreve o projeto de experimentos usado para avaliar a solução proposta e apresenta os resultados das simulações com suas respectivas análises. As avaliações visam a detecção de ataques de mensagens falsas (*bogus attack*), considerando tanto a eficiência no consumo de recursos quanto a eficácia na detecção de veículos maliciosos.

Nos experimentos, foram utilizados o simulador de redes OMNeT++ e a ferramenta geradora de cenários de mobilidade SUMO (*Simulation of Urban Mobility*). As interfaces do OMNeT++ e do SUMO foram aplicadas em conjunto com o *framework* Artery, permitindo a configuração do modelo de modo mais rápido e com execução de simulações interativas. A Tabela 2 apresenta os principais parâmetros usados na simulação de redes.

Tabela 2. Parâmetros do simulador de redes

Parâmetro	Valor	Parâmetro	Valor
MAC	IEEE 802.11p	Frequência do rádio	5.9 GHz
Tempo de simulação	900 segundos	Potência da antena	25mW
Tempo de *warmup*	200 segundos	Tamanho do beacon	32 bytes
Repetições	30	Período de envios de beacons	3s

Buscando reproduzir padrões de mobilidade com uma demanda real de tráfego, as avaliações realizadas incluem *traces* reais de mobilidade. Nesse sentido, foi usado o cenário *Luxembourg SUMO Traffic (LuST)* [Codeca et al. 2017], o qual inclui dados de tráfego de 24 horas em uma área de 155.95 km^2. Para delimitar o estudo em um cenário mais controlado, foi realizado um recorte e escolhida uma região deste cenário com a área definida de 5 km de extensão com três pistas e de 8,1 Km, quando do desvio dos veículos por um percurso alternativo.

O desenvolvimento do cenário de mobilidade utilizado nos experimentos 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; (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 3 são apresentados os cenários dos fluxos da rodovia usados na simulação.

O *smart contract* foi desenvolvido na plataforma *Hyperledger Besu* no qual foi utilizada a linguagem de programação *Solidity* com o *framework Truffle* para o ambiente

Tabela 3. Características dos cenários simulados

Cenário	Horário do fluxo	Nós/900s	Nós/hora	Nós/minuto
Muito esparso	3 h	125	500	8,3
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

de desenvolvimento de testes na *blockchain*. De modo a compilar e implementar chamadas de funções, foi utilizada a IDE *online* Remix.

4.1. Cenários de Ataque e Métricas de Desempenho

Dois cenários foram usados: (i) **sem mecanismos de reputação** e (ii) **com mecanismo de reputação**. O primeiro busca verificar os impactos provocados pela disseminação de informações falsas na rede, sem a utilização de um sistema de reputação, onde um veículo malicioso propaga informações falsas a respeito de um bloqueio parcial de pista. O segundo procura estimar os custos da utilização do sistema de reputação na rede veicular e, através de análises, mostrar a viabilidade de uso e sua eficácia.

Com o objetivo de verificar o comportamento da rede e mensurar os impactos dos ataques, as seguintes métricas foram utilizadas. **Tempo médio de aumento do percurso dos veículos**: aumento do tempo de percurso de veículos provocado pela disseminação da mensagem de alerta falsa. **Taxa média de redução de velocidade**: média da redução de velocidade de veículos, a partir do recebimento da mensagem até a chegada ao local do evento falso. **Taxa de veículos com mudança de percurso**: taxa de veículos que alteraram a sua rota em razão da mensagem falsa de alerta recebida. **Aumento do número de mensagens na rede**: acréscimo no número de mensagens enviadas decorrentes do mecanismo de reputação. **Tamanho do armazenamento da *blockchain*:** tamanho resultante do armazenamento na *blockchain* pelo mecanismo de reputação proposto.

4.2. Análise dos Resultados

Nesta seção são discutidos resultados de simulações com diferentes cenários de tráfego, onde há uma propagação de mensagem falsa de alerta de bloqueio parcial da via.

Cenário sem mecanismos de reputação: Para observar-se o impacto das mensagens falsas no sistema, inicialmente foram realizadas medições com a pista livre. Depois, repetiram-se os experimentos com a propagação da mensagem falsa. Na Tabela 4, são apresentados os resultados para percorrer o recorte simulado da autoestrada de 5,08 km e quando do desvio dos veículos por um percurso alternativo, aumentando assim o trajeto para 8,1 Km.

Tabela 4. Impactos da mensagem falsa sem sistema de reputação

	Sem mensagem falsa		Com mensagem falsa		Impactos		
Cenário	Velocidade média (Km/h)	Tempo médio (segundos)	Velocidade média (Km/h)	Tempo médio segundos	Taxa de redução de velocidade	Taxa do aumento p/ desvio	Taxa de mudança percurso
Muito esparso	129,19	143,05	123,37	149,75	4,50%	302,20%	90,40%
Esparso	129,94	142,03	120,47	153,36	7,29%	298,01%	92,70%
Normal	124,12	148,05	101,77	181,52	18,00%	280,72%	80,91%
Denso	118,53	155,86	90,85	201,25	23,35%	279,56%	50,05%

Com base na Tabela 4, observa-se que em todos os cenários simulados houve redução na velocidade média, sendo o impacto maior nos cenários com maior densidade.

Como consequência, há um aumento do tempo para percorrer o trecho simulado. No que se refere ao número de veículos que alteram o percurso, esse é menor quando as densidades são maiores, visto que com o fluxo maior de veículos, ao receberem a mensagem, um número significativo já passou do local para desvio e estão em velocidade reduzida no congestionamento. Entre os veículos que confiaram na mensagem falsa, os que tomaram o caminho alternativo sofreram um impacto significativo do tempo decorrido em razão do aumento da distância percorrida e por passarem por trechos urbanos com velocidades menores. Portanto, é possível verificar os impactos ocasionados pela disseminação de mensagem falsa sem um mecanismo de reputação.

Cenário com mecanismo de reputação: Inicialmente, foi feito um teste de desempenho do sistema que consistiu em analisar o aumento do armazenamento da *blockchain* conforme o número de blocos criados. Um bloco vazio (somente cabeçalho), no sistema proposto, possui o tamanho de 843 *bytes* e o valor da reputação gravada de cada veículo na *blockchain* tem o seu tamanho em 12 *bytes*.

A Tabela 5 apresenta o crescimento da *blockchain* conforme o número de blocos gravados em decorrência do número de veículos com suas reputações armazenadas. A gravação na *blockchain* é efetuada a cada dez minutos, tempo esse parametrizável no sistema, que corresponde à passagem de 416 veículos em média no cenário de fluxo normal e de 666 veículos no cenário denso (ver Tabela 3). O valor máximo definido na simulação é de 524.000 blocos, que caracteriza um total de dez anos de reputações armazenadas.

Tabela 5. Análise do crescimento da *blockchain*

Nº de blocos	Tamanho de armazenamento (*bytes*)				
	Bloco vazio	100 veículos	500 veículos	1.000 veículos	10.000 veículos
1	843	2.043	6.843	12.843	120.843
1.000	843.000	2.043.000	6.043.000	12.843.000	120.843.000
50.000	42.150.000	102.150.000	342.150.000	642.150.000	6.042.150.000
100.000	84.300.000	204.300.000	684.300.000	1.284.300.000	12.084.300.000
524.000	441.732.000	1.070.000.000	3.585.732.000	6.729.732.000	63.321.732.000

Se considerarmos um cenário de fluxo normal no qual cerca de 24% dos veículos (100 veículos) propagam mensagens de alerta WM, será necessário um espaço de armazenamento na *blockchain* de 2.043 *bytes* para cada bloco, e de 1,07GB após 10 anos. Mesmo em um cenário denso onde cerca de 75% dos veículos (500 veículos) tenham seu valor de reputação atualizado, o tamanho máximo de armazenamento será de 3,58GB. Consequentemente, pode-se concluir que o sistema de *blockchain* que se executa nas RSUs é viável, ainda que considerando um largo espaço de tempo.

Um segundo teste de desempenho consistiu em analisar o aumento do número de mensagens vinculadas com a utilização do mecanismo de sistema de reputação. A Tabela 6 apresenta a quantidade de mensagens propagadas na rede veicular com e sem o mecanismo de reputação e o impacto do uso do sistema nesta métrica.

Tabela 6. Nº de mensagens (sem contabilizar os *beacons*)

Cenário	Sem reputação	Com reputação	Impacto
Muito esparso	626	690	10,22%
Esparso	1.308	1.462	9,48%
Normal	11.535	12.390	7,41%
Denso	31.558	32.696	3,61%

Em decorrência da adição da mensagem *WVM* do sistema de reputação, há

um acréscimo no número de mensagens propagadas na rede. Todavia, mesmo com o acréscimo de mensagens, não há prejuízo significativo na eficiência do sistema. Observa-se, no cenário denso, um impacto menor em razão do grande fluxo de veículos, o qual ocasiona congestionamentos e faz que a grande parte dos veículos não chegue ao local do evento, em tempo hábil, para gerar a mensagem WVM durante o tempo simulado.

5. Conclusões e trabalhos futuros

Este trabalho buscou contribuir com a segurança em redes veiculares por meio do desenvolvimento de um sistema de gerenciamento de confiança distribuído, que combina diferentes técnicas para garantir a confiabilidade e a troca segura de mensagens. O sistema proposto utiliza os benefícios da tecnologia de *blockchain* e contratos inteligentes, como imutabilidade e segurança dos dados armazenados, para fornecer aos veículos informações inalteradas e confiáveis. Mostrou-se, através de simulações, a eficácia e a viabilidade da implementação do sistema proposto.

Como trabalhos futuros, pretende-se avaliar a eficácia do sistema de reputação proposto em relação às taxas de falsos negativos e falsos positivos em diferentes densidades de veículos. Os valores do limiar de reputação (*Th_Rep*) foram definidos empiricamente, portanto, outras técnicas precisarão ser estudadas em trabalhos futuros. Pretende-se também avaliar os custos computacionais e recursos de *hardware* dos veículos ao obterem uma cópia da *blockchain*, armazenada localmente, quando do seu ingresso à rede. Além disso, mais experimentos considerando diferentes áreas geográficas de interesse podem ser realizados para aprimorar o sistema proposto.

Agradecimentos

Os autores gostariam de agradecer as valiosas contribuições de Billy Pinheiro (Amachains) e Bruno Medeiros Costa.

Referências

Baza, M., Nabil, M., Mahmoud, M. M. E. A., Bewermeier, N., Fidan, K., Alasmary, W., and Abdallah, M. (2020). Detecting sybil attacks using proofs of work and location in vanets. *IEEE Transactions on Dependable and Secure Computing*.

Celes, A. A. and Elizabeth, N. E. (2018). Verification based authentication scheme for bogus attacks in vanets for secure communication. In *2018 International Conference on Communication and Signal Processing (ICCSP)*, pages 0388–0392. IEEE.

Codeca, L., Frank, R., Faye, S., and Engel, T. (2017). Luxembourg sumo traffic (lust) scenario: Traffic demand evaluation. *IEEE Intelligent Transportation Systems Magazine*, 9(2):52–63.

Feng, X., Li, C.-y., Chen, D.-x., and Tang, J. (2017). A method for defensing against multi-source sybil attacks in vanet. *Peer-to-Peer Networking and Applications*, 10(2):305–314.

Garg, S., Singh, A., Kaur, K., Aujla, G. S., Batra, S., Kumar, N., and Obaidat, M. S. (2019). Edge computing-based security framework for big data analytics in vanets. *IEEE Network*, 33(2):72–81.

Gong, C., Xu, C., Zhou, Z., Zhang, T., and Yang, S. (2019). A reputation management scheme for identifying malicious nodes in vanet. In *2019 IEEE 20th International Conference on High Performance Switching and Routing (HPSR)*, pages 1–6. IEEE.

Javed, M. U., Rehman, M., Javaid, N., Aldegheishem, A., Alrajeh, N., and Tahir, M. (2020). Blockchain-based secure data storage for distributed vehicular networks. *Applied Sciences*, 10(6):2011.

Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., and Zhang, Y. (2018). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal*, 6(3):4660–4670.

Kchaou, A., Abassi, R., and Guemara, S. (2018). Toward a distributed trust management scheme for vanet. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pages 1–6.

Khalid, A., Iftikhar, M. S., Almogren, A., Khalid, R., Afzal, M. K., and Javaid, N. (2021). A blockchain based incentive provisioning scheme for traffic event validation and information storage in vanets. *Information Processing & Management*, 58(2):102464.

Lu, Z., Liu, W., Wang, Q., Qu, G., and Liu, Z. (2018). A privacy-preserving trust model based on blockchain for vanets. *IEEE Access*, 6:45655–45664.

Shrestha, R., Bajracharya, R., Shrestha, A. P., and Nam, S. Y. (2020). A new type of blockchain for secure message exchange in vanet. *Digital communications and networks*, 6(2):177–186.

Yang, Y.-T., Chou, L.-D., Tseng, C.-W., Tseng, F.-H., and Liu, C.-C. (2019). Blockchain-based traffic event validation and trust verification for vanets. *IEEE Access*, 7:30868–30877.

Yang, Z., Zheng, K., Yang, K., and Leung, V. C. (2017). A blockchain-based reputation system for data credibility assessment in vehicular networks. In *IEEE 28th annual int. symp. on personal, indoor, and mobile radio communications (PIMRC)*, pages 1–5.