Autenticação com suporte à Computação de Borda 5G para a Internet de Veículos

Anderson Queiroz[1], **Eduardo Oliveira**[1], **Maria Barbosa**[1], **Kelvin Dias**[1]

[1]Centro de Informática – Universidade Federal de Pernambuco (UFPE)
Av. Jornalista Aníbal Fernandes, s/n – Cidade Universitária.
CEP: 50.740-560 Recife-PE – Brasil

aalq,ehammo,mksb,kld@cin.ufpe.br

Abstract. *Security support is of paramount importance for the success and widespread adoption of connected and autonomous cars on the Internet of Vehicles (IoV) Era. To this end, Intelligent Transportation Systems (ITS) require effective access control and trustworthiness solutions while considering the latency and throughput requirements of current and upcoming vehicular applications. With the advent of 5G and edge computing, such requirements can be attained by leveraging on processing closer to the vehicles. Despite recent proposals benefit from blockchain-based security for IoV, studies remain unclear regarding its comparative performance against traditional centralized systems for specific scenarios in terms of QoS metrics. This paper proposes and compares centralized and distributed architectures for IoV authentication. First, a Trust Authority (TA) scheme is devised. A Blockchain-based Authentication architecture for IoV is also proposed. Finally, performance evaluation through simulations is conducted to quantify the pros and cons of both approaches.*

Resumo. *O suporte de segurança é de suma importância para o sucesso e a ampla adoção de carros conectados e autônomos na era da Internet dos Veículos (IoV). Para isso, os Sistemas Inteligentes de Transporte (ITS - Intelligent Trasnportation Systems) demandam soluções eficazes de controle de acesso e confiabilidade, considerando os requisitos de latência e vazão das aplicações veiculares atuais e futuras. Com o advento do 5G e da computação de borda, esses requisitos podem ser alcançados dispondo do processamento mais próximo dos veículos. Apesar de propostas recentes se beneficiarem da segurança baseada em Cadeia de Blocos (Blockchain) para IoV, os estudos com avaliação de desempenho ainda são incipientes quanto à análise comparativa com sistemas de autenticação centralizados tradicionais em termos de métricas de QoS. Este artigo propõe e compara arquiteturas centralizadas e distribuídas para autenticação em IoV. Primeiro, um esquema de Autoridade de Confiança (TA - Trust Authority) é desenvolvido. Uma arquitetura de autenticação baseada em Blockchain para IoV também é proposta. Por fim, a avaliação de desempenho por meio de simulações é realizada para quantificar os prós e contras de ambas as abordagens.*

Palavras Chave - Internet de Veículos, Autenticação, Autoridade de Confiança, Cadeia de Blocos, Computação de Borda e 5G.

1. Introdução

A *Internet* de Veículos (IoV) surgiu como uma das aplicações da IoT (Internet of things) e uma evolução das Redes Veiculares *Ad-hoc* (VANETs). Suas características são mais abrangentes no que se refere à disponibilização de serviços, compartilhamento de dados e segurança das aplicações no contexto de Sistemas Inteligentes de Transporte (ITS - *Intelligent Transportation Systems*). Segundo dados apresentados pela revista *Business Insider Intelligence*[1], o número de veículos conectados deverá sofrer um aumento de 133% em 8 anos, ultrapassando a marca dos 77 milhões de unidades até 2025. Portanto, cresce a responsabilidade com os requisitos relacionados à eficiência das soluções de segurança para cenários envolvendo comunicação interveicular. A IoV permite diferentes modos de comunicação para veículos e objetos conectados: *Vehicle-to-Infrastructure*(V2I), *Vehicle-to-Vehicle*(V2V) e *Vehicle-to-Everything*(V2X), como suporte aos contextos de conectividade para o ecossistema ITS [Jianbin Gao et al. 2019].

O ambiente da IoV possui diferentes elementos constituintes: estações de comunicação, postos de fiscalização, pedágios, unidades de salvaguarda, equipamentos de sinalização, veículos e pedestres. As IoVs são formadas por um conjunto tecnológico de Centro de Dados, Aplicações, Unidades de Acostamento(RSU-Road Side Unit), Estações Base(BS-Base Stations), Sensores, Câmeras, Semáforos, Placas Interativas, Unidades Computadorizadas de Bordo(OBU-OnBoard Unit), além de múltiplas tecnologias de comunicação nos padrões 802.11p, 802.15, 3G, 4G/LTE (Long Term Evolution) e 5G/NR (New Radio) [XiaoDong Zhang 2018].

Com a implantação atual das redes 5G ao redor do mundo, a IoV terá um impulso significativo com os benefícios da comunicação ultra-confiável e de baixa latência (URLLC - *Ultra Reliable and Low Latency Communication*). Taxas de transmissão com a banda larga móvel aprimorada (eMBB - *enhanced Mobile Broadband*) e a comunicação massiva do tipo máquina (mMTC - *massive Machine Type Communication*). De forma a compor o ambiente 5G, soluções baseadas em computação de borda (MEC - Multi-access Edge Computing) e softwarização de rede baseada em SDN (Software-Defined Networking) e NFV (Network Functions Virtualization) têm sido empregadas para otimizar a utilização dos recursos disponíveis. A programabilidade e processamento mais próximos do usuário ou executando nos próprios dispositivos finais auxilia a redução dos requisitos de latência das aplicações [Nisha Panwar 2016][Fang Liu et al. 2019][Alcardo A. Barakabitze et al. 2020].

Contudo, problemas como a falta de confiança entre veículos nos diversos modos de comunicação, bem como a falta de mecanismos eficientes para lidar com a densidade elevada de veículos e objetos conectados nas futuras cidades inteligentes, precisam ser investigados em profundidade para o sucesso e ampla adoção dos serviços na IoV baseados na infraestrutura 5G. Apesar de propostas recentes se beneficiarem da segurança baseada em *Blockchain*(BC) para IoV, os estudos ainda não estão claros sobre seu desempenho em relação aos sistemas centralizados baseados em Autoridade de Confiança(TA) para IoV. Além disso, não é do nosso conhecimento que existam arquiteturas holísticas em camadas que se beneficiem do arcabouço da *edge* e 5G para provisionamento de autenticação em ambientes IoV.

[1]https://www.businessinsider.com/iot-connected-smart-cars

Os requisitos de qualidade de serviço e experiência das redes 5G podem ser afetados pelos procedimentos de autenticação e segurança no ambiente dinâmico das IoVs. Sendo assim, a proposta desta pesquisa foi realizar o desenvolvimento, implementação e análise das soluções da Autoridade de Confiança e *Blockchain* aplicadas na arquitetura de computação na borda em redes 5G no ambiente IoV. O objetivo é avaliar os desempenhos de cada solução na realização do serviço de Autenticação dos veículos e validação das mensagens com informações de transito no ambiente.

O presente trabalho foi organizado como descrito a seguir. A seção 2 apresenta uma breve descrição dos conceitos de sistemas de autenticação baseados em TA e BC. A seção 3 apresenta os trabalhos relacionados. A proposta da análise avaliativa das soluções de autenticação centralizada e descentralizada no contexto da borda 5G para IoV é apresentada na seção 4. A seção 5 exibe parâmetros, métricas e cenários das simulações. A seção 6 apresenta os resultados da avaliação das soluções e análises sobre suas vantagens e desvantagens e, por fim, a seção 7 conclui e recomenda trabalhos futuros.

2. Fundamentos das Soluções de Autenticação

Um sistema de autenticação com arquitetura centralizada é definido por [Mahmood A. Al-Shareeda and Manickam 2021] como sendo um terceiro altamente confiável, capaz e responsável por registrar os componentes em um ambiente de rede. Por padrão, é conectado aos elementos de comunicação via redes cabeadas, segmentadas e seguras. Opera como ponto central de verificação e autorização, onde os nós usuários que pretendem ingressar no ambiente devem ser registrados e permissionados por tal Autoridade de Confiança (TA - *Trust Authority*). A TA pode conter diversos serviços, ou terceirizá-los para aplicações que estejam localizadas em diferentes provedores. Isto ocorre com as Autoridades Certificadoras (CA - *Certificate Authority*), que por motivos legais são contratadas e utilizadas por diversos serviços e aplicações nas redes. A TA pode conter diversos serviços que envolvem desde operações de cadastros, autenticação, definição de perfis, validação de transações até as funções de geração e gerência de chaves criptográficas e senhas de proteção dos dados na rede.

A solução descentralizada *Blockchain* é um paradigma de computação distribuída que usa estruturas de blocos encadeados por meio da criptografia para validar e armazenar dados, algoritmos de consenso e contratos inteligentes. Os blocos são compostos por transações que são autenticadas e validadas de forma compartilhada, ou seja, sem a necessidade de uma entidade central de confiança. Esta solução foi proposta inicialmente por [Nakamoto 2009] para definir um sistema de autenticação e validação de transações distribuídas e realizadas na rede mundial com a criptomoeda *Bitcoin*. Atualmente, existem três modos para implementação de um sistema de autenticação distribuída empregando a tecnologia da *Blockchain*, pública, privada ou de consórcio [Anderson Queiroz and Dias 2020].

Um ponto relevante a ser considerado em uma Blockchain é sua forma de obtenção da aprovação em grupo para tomadas de decisão de validação dos nós, usuários e transações propostas. Este método democrático de julgamento compartilhado recebe o nome de "mecanismo de consenso", sendo ele um elemento primor-

dial de distinção das demais tecnologias que realizam tomadas de decisão em rede [Farhana Javed et al. 2022].

3. Trabalhos Relacionados

Esta seção apresenta estudos da literatura que contemplam análises entre as soluções da Autoridade de Confiança (TA) e Blockchain (BC) para diferentes ambientes de comunicação. Em geral, algumas das análises apresentadas utilizaram os ambientes da IoV, IoT, nuvem (*Cloud*) e redes veiculares tradicionais (*VANET*). Os padrões de conectividade de rádio com a infraestrutura são baseados em 802.11ac, 802.11p, 3G e 4G/LTE. A Tabela 1 destaca os principais aspectos dos trabalhos relacionados. Os referidos estudos comparativos possuem diferentes objetivos de análises no que se refere ao desempenho, eficiência das autenticações, eficácia dos esquemas de proteção, arquiteturas de comunicação, usabilidade, adulteração de dados e o não repúdio.

Tabela 1. Trabalhos Relacionados (Trust Authority x Blockchain)

Artigo	**Ambiente**	**TAxBC**	**Segurança**	**Proposta**	**Análises**
[Hui Li et al. 2019]	VANET	√	RSA e MD5	*Blockchain* em VANET, redes 802.11p	Parâmetros de privacidade de identidade e localização com base nos algoritmos(UGG, IPP, LPP)
[Rama Yerramilli 2019]	Cloud	√	RSA e SHA1	Autenticação multifator(TAxBC), na Nuvem em serviços eGov	Processos de usabilidade e gestão dos usuários nas arquiteturas centralizadas e distribuídas
[Clemens Brunner et al. 2020]	Cloud	√	RSA DH e AES	Implementação de um esquema PKI baseada em *Blockchain*	Desempenho das aplicações de infraestrutura de chaves centralizadas e distribuídas na *Internet*
[Paul Rimba et al. 2020]	Cloud	√	ECDSA e RSA	Diagnostico econômico das arquiteturas Centralizadas e Descentralizada	Custos financeiros para execução de transações confiáveis entre as soluções *Blockchain Ethereum x Trust Authority AWS*
[Tigang Jiang 2019]	IoV	√	ECDSA e AES	Aplicação da tecnologia da *Blockchain* na *Internet* de Veículos	Comportamento de armazenamento de dados distribuídos seguro para Big Data
[Aydın Yucel et al. 2020]	IoT	∗	ECDH e DLP	Esquema flexível para autenticação de grupo em ambientes IoT	Eficiência energética dos dispositivos e os custos dos mecanismos de segurança centralizada e distribuída
[Proposta de Pesquisa]	**IoV**	√	**ECDH ECDSA AES e SHA512**	**Autenticação com suporte à Computação de Borda 5G para IoV**	**Análise de Desempenho das soluções de Segurança TA e BC com relação aos cenários na IoV**

O estudo [Hui Li et al. 2019] comparou Blockchain e TA em relação aos parâmetros de privacidade e localização, utilizando redes com padrão 802.11p. Além de adotarmos um cenário 5G-MEC, distinto do trabalho relacionado, nossa proposta compara o desempenho em termos de vazão, tempo de autenticação e sobrecarga na troca de mensagens.

Já a pesquisa [Rama Yerramilli 2019] buscou realizar uma comparação dos mecanismos de autenticação centralizados e descentralizados no contexto de aplicações eGov na nuvem. Nossa proposta avalia e compara mecanismo de autenticação no contexto das aplicações na borda das redes 5G no ambiente da IoV.

O estudo [Clemens Brunner et al. 2020], apresentou a implementação de um esquema de infraestrutura de chave pública PKI (*Public Key Infrastructure*), base-

ada em *Blockchain* na nuvem, comparando aspectos da eficácia do serviço com a Autoridade Certificadora centralizada na nuvem. Nossa proposta faz uma análise de desempenho nos tempos de autenticação e validação das informações de trânsito no ambiente da IoV na borda em redes 5G.

O artigo [Paul Rimba et al. 2020] realiza uma análise dos custos econômicos da tecnologia *Blockchain* e da Autoridade de Confiança quando executadas em IaaS(*Infrastructure as a Service*). O referido estudo utilizou os ambientes de serviços na nuvem da *AWS* para TA e da *Ethereum* para BC. Neste caso não foi considerado o ambiente 5G-*Edge*, tampouco cenário da IoV.

Já o estudo [Tigang Jiang 2019] faz uma análise da utilização da *Blockchain* na *Internet* de Veículos. O referido estudo realizou avaliações de desempenho em relação ao armazenamento distribuído de grandes massas de dados *Big Data* em redes 4G/LTE. Apesar do ambiente ser análogo ao desta proposta podemos observar que os objetivos de estudo são diferentes. Enquanto este trabalho relacionado focou nas questões relacionadas aos serviços de armazenamento, esta proposta tem o foco em serviços de autenticação e validação.

Por fim, [Aydın Yucel et al. 2020] propõe uma abordagem para autenticação flexível de grupos (GAS) para IoT em redes 802.11 e dispositivos com recursos limitados. Foi elaborada uma arquitetura adaptável focada na eficiência energética dos dispositivos com atuação centralizada ou distribuída. Nossa proposta objetiva a análise das aplicações de autenticação no contexto da IoV em redes 5G, considerando recursos mais amplos, dispositivos e infraestrutura baseada na tecnologia mais recente para redes móveis celulares 5G.

4. Visão Geral da Arquitetura 5G-Edge para autenticação IoV

A Figura 1 exibe o ambiente da IoV com os serviços de autenticação TA/BC no contexto das redes 5G com a computação de borda. Com o surgimento do *Vehicular Edge Computing*(VEC), pode-se dizer que o processamento e o armazenamento estão cada vez mais próximos dos veículos [Lei Liu et al. 2021]. As camadas da borda e do nevoeiro (*edge/fog*), podem ser empregadas para melhoria do desempenho e da qualidade de transmissão, aliadas à implementação de múltiplas tecnologias de apoio a redes SDN e NFV [Anderson Queiroz and Dias 2020]. Os métodos adequados de segurança na IoV visam minimizar possíveis ações maliciosas que possam causar incidentes ou acidentes no ambiente [Lianhai Liu 2019].

Conforme apresentado na Figura 1, no topo da hierarquia, a camada de nuvem (*Cloud*) consiste de serviços, aplicações e recursos virtualizados e remotos ao ambiente da operadora. A camada da nuvem também pode ser utilizada quando se pretende a formação de federações para os serviços de autenticação. Contudo, no esquema apresentado, consideramos apenas uma operadora para ilustrar a proposta. A camada seguinte é constituída do núcleo (*core*) da operadora, com arquitetura baseada em serviços (SBA - *Service Based Architecture*). O núcleo do 5G é composto por funções de rede tais como, AUSF (*Autenticatication Server Function*) e SMF (*Session Management Function*), entre outras, em uma arquitetura de microsserviços. Para o propósito deste artigo a Autoridade de Confiança é implementada no núcleo podendo estender ou integrar as funções de rede existentes preconizadas

pelo 3GPP (Third Generation Partnership Project).

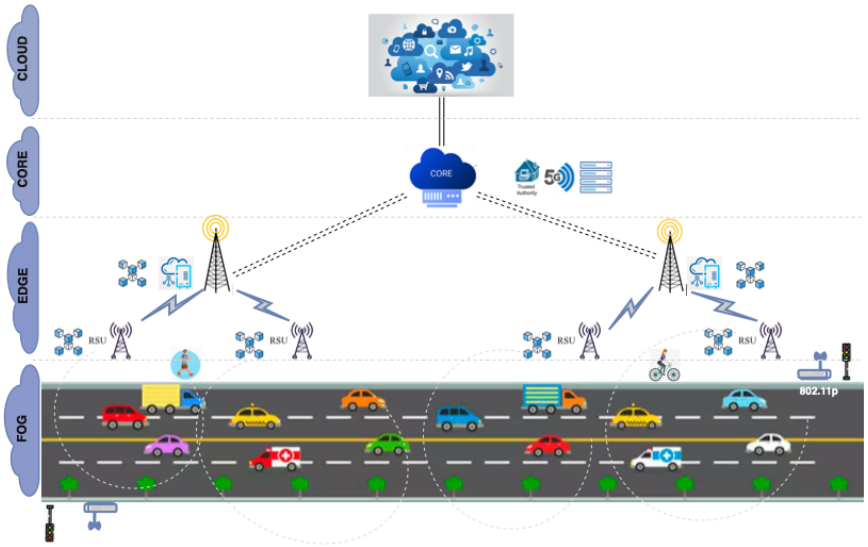

Figura 1. Ambiente IoV - Centralizada(TA) / Descentralizada(BC)
Fonte: Autor

A camada de borda (*edge*) pode conter tanto os serviços virtualizados mais próximos do dispositivo final, como as estações rádio-base de nova geração (gNBs) do 5G. Esta camada pode implementar o plano de controle nas redes definidas por *software*, processamento de aplicações e a atividade de mineração ou consenso da *Blockchain*. Nesta proposta, a arquitetura apresentada é flexível para atendimento das solicitações na borda, mas para fins de avaliação e comparação com *Blockchain* implementada na borda, as simulações consideraram a TA no núcleo com latência negligível no *backhaul*, entre borda e núcleo. A *Blockchain* foi distribuída entre as camadas *edge* e *fog* com suas principais atividades de validação e consenso sendo executadas na camada da borda do ambiente IoV.

4.1. Detalhamento e Implementação do Ambiente

As soluções baseadas em Autoridade de Confiança e *Blockchain* foram desenvolvidas na linguagem de programação *c++*(v17), suas execuções e comportamentos simulados na ferramenta ns-3(v3.34) [2]. Para a implementação dos mecanismos e algoritmos de segurança, como criptografia simétrica e assimétrica, foi aplicada a biblioteca do *crypto++*(v5.6.4) [3]. Com relação ao protocolo de transporte utilizamos o TCP(*Transmission Control Protocol*), visto que no UDP(*User Datagram Protocol*) ocorriam perdas de pacotes e dados que continham as chaves de autenticação, prejudicando o desempenho e funcionamento dos serviços de autenticação o ambiente [Poorzare and Augé 2020].

Para a rede de comunicação proposta, empregamos a biblioteca do projeto 5GLENA[4], no padrão 5G(*Non Standalone*), preservando núcleo 4G/LTE, mas com

[2]https://www.nsnam.org
[3]https://www.cryptopp.com
[4]*CTTC - Centre Tecnològic de Telecomunicacions de Catalunya*

gNBs operando na faixa de 25-39GHz (mmW), conforme implementação já fornecida pelo módulo 5G e definição 3GPP para ondas milimétricas. A Figura 2 apresenta os dois modos de implementação da tecnologia 5G.

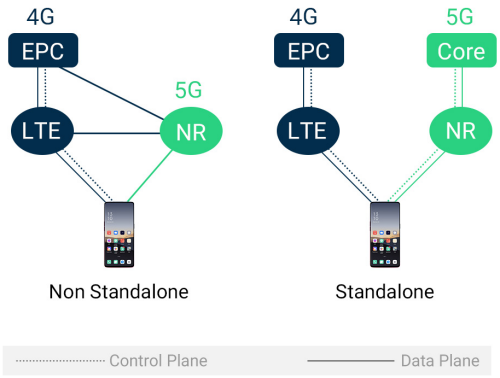

Figura 2. Visão Geral 5G/NSA-SA [oppo.com]

4.2. Esquemas de Suporte à Segurança

Para o atendimento das funcionalidades de proteção e validação dos dados nas aplicações TA e BC, utilizamos as tecnologias criptográficas assimétricas(*Elliptic Curve Diffie–Hellman Key Exchange-ECDH, Elliptic Curve Digital Signature Algorithm-ECDSA*), simétrica(*Advanced Encryption Standard-AES*) e unidirecionais *hash*(*Secure Hash Algorithm-SHA*) [Buchmann 2004].

O algoritmo assimétrico ECDH é utilizado para troca das chaves através do canal inseguro da rede, tornando possível a proteção da chave que será enviada ao veículo. O algoritmo ECDSA tem a função da autenticidade e do não repúdio das mensagens remetidas à rede. O algoritmo simétrico AES é responsável pelas funções da integridade e confidencialidade dos dados e, por fim, a função de compressão unidirecional SHA512 que é responsável pela geração dos códigos de verificação da integridade dos blocos encadeados na *Blockchain*.

4.3. Desenvolvimento da Autoridade de Confiança

As principais funções implementadas pela TA, nesta proposta, são a autenticação, gerenciamento de usuários, geração e revogação das chaves e a validação das mensagens publicadas no ambiente da IoV. A Autoridade de Confiança desenvolvida para este estudo, atua no modelo de arquitetura cliente/servidor tradicional [Lianhai Liu 2019]. Ela esta diretamente conectada na borda da rede onde optamos pela gestão de certificados locais, não terceirizados, realizando também as atividades padrão de uma Autoridade Certificadora (CA).

A Figura 3 apresenta a ordem de comunicação para atividade de autorização e permissão de uso dos serviços e sistemas entre o veículo integrante e a TA na IoV.

A solução TA desenvolvida foi modularizada para possibilitar uma melhor adequação ao ambiente da IoV. Os módulos da TA são:

I (PD) Pacote de Dados - Estrutura os tipos de pacotes: autenticação, certificados, transações e mensagens;

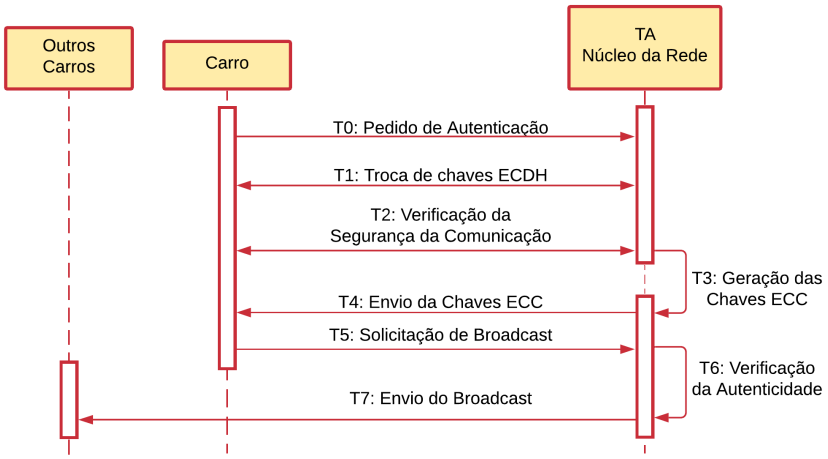

Figura 3. Diagrama de Sequência (TA) - *Core/Edge/Fog*

II (AC) Autoridade Certificadora - Determina e gerência os certificados e as chaves de proteção, determinando os padrões e tecnologias criptográficas;

III (AV) Autenticação e Validação - Obtém as requisições de autenticação e realiza a validação dos entes e suas mensagens na rede;

IV (PP) Parametrização de Perfis - Caracteriza os perfis e os relaciona com as devidas permissões;

V (RD) Registro de Dados - Grava de forma estruturada as informações no sistema de gerenciamento de banco de dados.

4.4. Aplicação da Blockchain

A implementação se baseou em trabalhos publicados [Nakamoto 2009, Wei Hu et al. 2019, Shaoyong Guo et al. 2019], considerando as diferenças de ambiente, arquiteturas e rede. A *Blockchain* opera na arquitetura distribuída [XiaoDong Zhang 2018], seu desenvolvimento teve como base as propriedades de um sistema autônomo, atividades compartilhadas, imutabilidade de registros e consenso das transações. A BC funciona na borda da rede, isto é, as RSUs atuam como mineradores. O algoritmo de consenso implementado foi o PoW(*Proof of Work*).

A Figura 4 apresenta um diagrama de sequência com a ordem na troca de mensagens para a atividade de autorização e permissão de uso dos serviços e sistemas entre o veículo integrante e a BC na IoV.

A solução *Blockchain* desenvolvida foi modularizada para possibilitar uma melhor adequação ao ambiente da IoV. Os módulos da BC são:

I (PD) Pacote de Dados - Estrutura os tipos de pacotes: autenticação, certificados, transações e mensagens;

II (AC) Autoridade Certificadora - Gera e administra os certificados e as chaves de proteção, determinando os padrões das criptográficas;

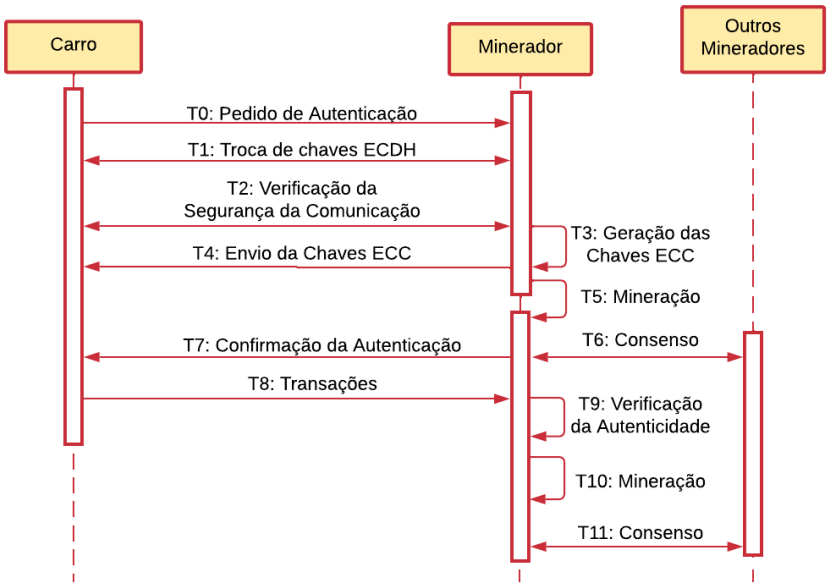

Figura 4. Diagrama de Sequência (BC) - *Edge/Fog*

III (CB) Consenso *Blockchain* - Estabelece os critérios e regras para as decisões comunitárias e compartilhadas na rede;

IV (VB) Veredito *Blockchain* - Delibera sobre as decisões obtidas para aprovação de um novo bloco a ser registrado no sistema;

V (RB) Registro de Bloco - Inclui conjunto de transações aprovadas como novo bloco na cadeia.

5. Avaliação de Desempenho

A Tabela 2 exibe métricas, cenários e configurações definidos para as simulações. O tempo de simulação foi de 100 segundos (linha 1). As simulações foram realizadas considerando o parâmetro 2, Quantidade de Veículos, com valores entre e foram realizadas considerando o parâmetro 2, Quantidade de Veículos, com valores entre 20 e 100 e que foram distribuídos entre as estações rádio base. A linha 3 exibe a tecnologia adotada 5G/NSA. O tamanho do pacote com valor de 1.496 bytes é apresentado na linha 4. Em relação às gNBs, foram utilizadas 4 unidades (linha 5), cujas configurações são apresentadas na linha 6. As configurações das plataformas de *hardware* e *software* que executaram as simulações foram descritas na linha 7. Os esquemas criptográficos utilizados foram indicados na linha 8. As soluções de segurança desenvolvidas e analisadas, Autoridade de Confiança e *Blockchain* são listadas na linha 9. Por fim, as métricas são apresentadas na linha 10 da tabela.

6. Resultados

Explicitamos nesta seção, os resultados das simulações executadas no ambiente da IoV na borda em redes 5G, conforme os parâmetros e configurações elencadas na Tabela 2. Nas figuras 5 e 6 realizamos a avaliação da comunicação centralizada

Tabela 2. Bases da Simulação

1	Tempo de Simulação	100 segundos
2	Quantidade de Veículos	20, 40, 60, 80, 100
3	Tecnologia de Comunicação	5G *Non Standalone*
4	Tamanho dos Pacotes	1496 *Bytes*
5	Número de *gNodeB's*	4 (*mmWave*)
6	Configuração dos enlaces	Vazão: $100e^6$ Mbps e Frequência: $28e^9$Hz
7	Servidores das Aplicações	Intel Xeon CPU E5530 2.40GHz, 12 vCPU, 38GB RAM, HD 80GB, Ubuntu 20.08
8	Equemas Criptográficos	ECDH, ECDSA, AES256, SHA512
9	Aplicações Desenvolvidas	Autoridade de Confiança, *Blockchain*
10	Métricas	Vazão, Atraso, Tempo de autenticação, Número de mensagens

que será utilizada para a aplicação da TA (na cor laranja) no núcleo da rede e a comunicação distribuída na borda que será utilizada pela aplicação da *Blockchain* (na cor verde).

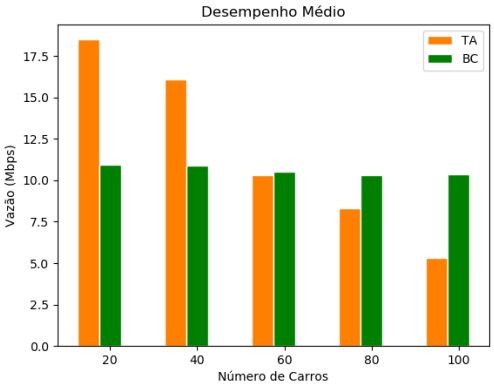

Figura 5. Vazão Cent vs Desc

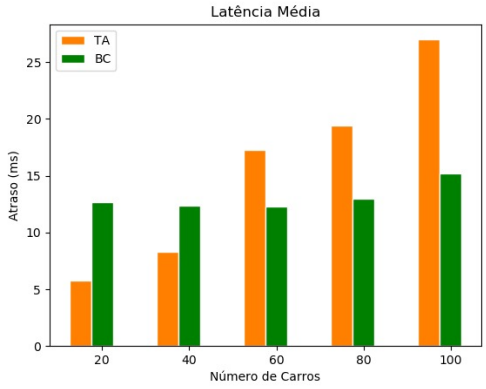

Figura 6. Atraso Cent vs Desc

A Figura 5 apresenta a vazão da rede 5G para as arquiteturas centralizada e distribuída. As variações no número de veículos ficaram entre 20 e 100 com intercalações de 20 e o envio de pacotes entre 10 mil a 52 mil por cenário simulado. A arquitetura centralizada alcançou vazões iguais a 18,74Mbps e 5,29Mbps para os respectivos cenários com 20 e 100 veículos. Em relação à mesma simulação na arquitetura descentralizada obtivemos valores entre 10,96Mbps(20 veículos) a 10,29Mbps(100 veículos), levando-se em conta o mesmo número de pacotes já citados. No resultado da arquitetura centralizada apresentado na Figura 6, os atrasos na arquitetura centralizada variaram entre 5,79ms e 26,97ms. Tal degração ocorreu

à medida que o número de veículos foi aumentando nas simulações. Já a arquitetura descentralizada, novamente se manteve estável, com variação ínfima entre 12,26ms à 15,18ms, considerando a mesma variação do número de veículos da simulação centralizada.

O desempenho do modelo centralizado, em termos de vazão, atingiu valores superiores de transmissão para cenários com 20 e 40 nós, isto é, com menores densidades de veículos. Isso se dá por conta da menor quantidade de requisições para unidade centralizada o que facilita o atendimento da requisição e aumenta a vazão, diminuindo o atraso. À medida que ampliamos o número de veículos o desempenho tende gradativamente, a se deteriorar, chegando ao patamar de 30% de sua vazão e aumento aproximado de 470% em seu atraso com relação os valores iniciais obtidos. Essa é uma característica comum ao modelo centralizado, visto que a TA é responsável por responder a todos os pedidos de autenticação na rede. No modelo descentralizado, constatamos maior regularidade no comportamento do desempenho, não havendo pontos de pico ou de queda acentuada da vazão, o ambiente se mantém estável estável em torno do valor de 10Mbps, dado que a troca de mensagens é distribuída entre os nós.

As Figuras 7 e 8 representam a média de tempo da atividade de autenticação completa para cada veículo nas aplicações, TA e BC. Nota-se uma diferença significativa nestes tempos, com variação aproximada de 150ms, ou 400%, entre os melhores e piores valores obtidos. Para explicar tal discrepância, devemos considerar que a BC necessita submeter as transações de autenticação ao processo de consenso, este procedimento requer maiores recursos computacionais, além de exigir intensa comunicação entre os mineradores, impactando no desempenho global da arquitetura.

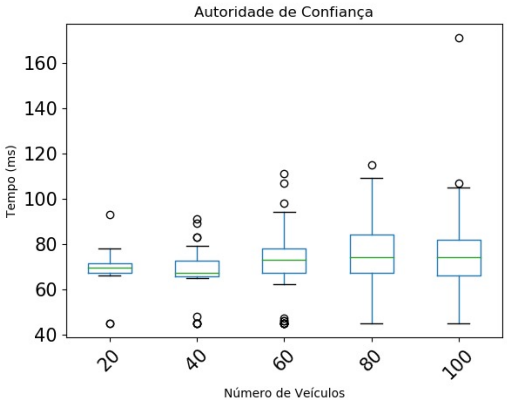

Figura 7. Tempo Autenticação TA

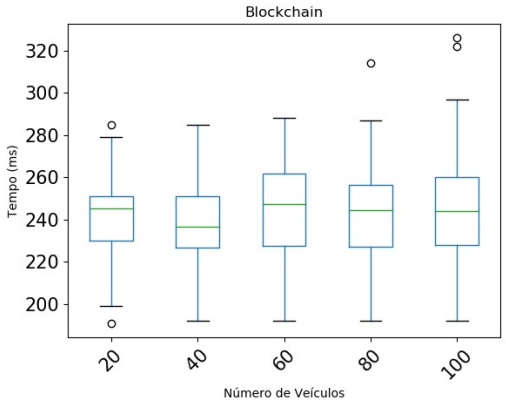

Figura 8. Tempo Autenticação BC

De forma comparativa, podemos observar que a BC, por ser distribuída, novamente apresenta regularidade com poucos *outliers*, enquanto a TA tem uma amplitude interquartil muito menor. Porém, mesmo com estes valores atípicos, quando da comparação entre a TA com 100 veículos e a BC com 20 veículos, o tempo de autenticação no cenário com TA chega a ser 13% mais rápido.

As Figuras 9 e 10 ilustram a execução do envio de mensagens de alertas

de trânsito entre os veículos autenticados no ambiente proposto. O propósito da implementação de uma aplicação específica para trocas de mensagens de tráfego foi medir o desempenho das soluções da Autoridade de Confiança e *Blockchain* durante o processo de validação, encaminhamento e armazenamento das mensagens na rede.

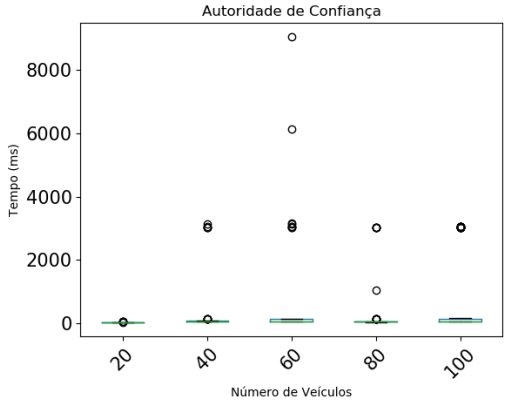

Figura 9. Troca de Mensagens TA

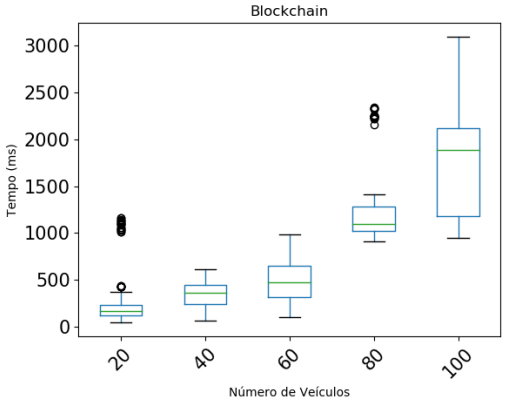

Figura 10. Troca de Transações BC

Neste cenário completo que considera todas as trocas de mensagens, avaliamos a latência total para que um veículo possa submeter avisos de trânsito fim-a-fim, desde a solicitação da autenticação até o envio das mensagens de alerta e recebimento por outro veículo. A aplicação da TA, em média, obteve desempenho superior da vazão para a atividade de propagação e validação das mensagens de trânsito, considerando que a BC precisa tanto validar se a mensagem foi enviada por um veículo autenticado, quanto atingir consenso e veredito para armazenar cada mensagem.

7. Conclusão

Os sistemas inteligentes de transporte (ITS) e a Internet de Veículos representarão importantes blocos construtores para a composição do futuro das cidades inteligentes. Portanto, é fundamental compreender quais soluções de segurança possuem melhores características que satisfaçam aos cenários na Internet de Veículos. Como forma de compreender as execuções no ambiente analisado, foram propostas e desenvolvidas as soluções da Autoridade de Confiança(TA) e da *Blockchain*(BC). Ambas, concebidas no contexto das IoV, baseadas na arquitetura em camadas com computação de borda em redes de comunicação 5G. Para obtenção dos valores coletados das soluções, centralizada TA e distribuída BC, utilizamos o simulador ns-3. Para a rede de comunicação foi aplicada a bibliotecas do Projeto *5G-Lena* e para as funções de criptografia o módulo do *cripto++*.

Os resultados obtidos, evidenciam o melhor desempenho da arquitetura centralizada(TA) nos cenários iniciais de simulação, com 20 a 40 veículos, com vazão valor de vazão máxima de 18,74Mbps contra os 10,96Mbps alcançados no modo distribuído(BC). As simulações demonstraram deterioração de 70% da eficiência da vazão à medida que ocorreram as ampliações nos números de veículos na arquitetura centralizada (TA). A arquitetura descentralizada mostrou-se com desempenho estável, na faixa de vazão dos 10Mbps, com variação de aproximadamente 6%, no

cenário de incremento máximo da quantidade de veículos. Com relação aos atrasos nas simulações a arquitetura descentralizada (BC) se manteve estável, com variação de 2,92ms entre os cenários avaliados. Já a arquitetura centralizada(TA) retratou uma alta variação com 26,97ms de atraso quando do cenário limite com 100 veículos. No que se refere aos tempos de autenticação, a TA obteve desempenho com eficiência superior com média total das simulações de 76,39ms contra os 245,68ms da BC.

No tocante à aplicação de avisos de trânsito, a TA atingiu médias de desempenho superiores aos da BC, uma vez que tais valores são impactados pelos diferentes mecanismos de validação e encaminhamento da aplicação distribuída. As análises demonstraram que, para diferentes cenários, as soluções TA e BC apresentaram comportamentos e desempenhos distintos conforme cada funcionalidade, logo, a adoção de determinada solução de segurança depende da análise do ambiente, levando em consideração as infraestruturas disponibilizadas pelas pelas operadoras e provedores de serviço. Esta pesquisa teve como objetivo propor arquiteturas para segurança no contexto IoV com suporte da computação de borda 5G, bem como nortear e subsidiar pesquisadores, analistas e desenvolvedores no entendimento dos compromissos de desempenho em tais cenários.

Como trabalhos futuros, pretende-se desenvolver versões aprimoradas para a soluções de autenticação centralizada e distribuída, por exemplo, através do balanceamento de solicitações entre diferentes servidores de borda. Nosso estudo preliminar possibilitou apenas atribuição dos veículos ao *grid* do ambiente e sem mobilidade, por conta da limitação da ferramenta 5GLena, que ainda não implementa handover 5G em sua pilha. Mas, cenários com sobreposição de coberturas de rádio serão simulados em trabalhos futuros para explorar o aprimoramento pretendido.

Referências

Alcardo A. Barakabitze, Arslan Ahmad, R. M. et al. (2020). 5g network slicing using sdn and nfv: A survey of taxonomy, architectures and future challenges. *Computer Networks*, 167:106984.

Anderson Queiroz, Eduardo Oliveira, M. B. and Dias, K. (2020). A survey on blockchain and edge computing applied to the internet of vehicles. *IEEE International Conference on Advanced Networks and Telecommunications Systems - Workshop on New Advances on Vehicle-to-Everything (V2X) Communications and Networking*.

Aydın Yucel, Gunes Karabulut, E. O. et al. (2020). A flexible and lightweight group authentication scheme. *IEEE INTERNET OF THINGS JOURNAL*, 07:10277–10287.

Buchmann, J. (2004). *Introduction to Cryptography*, volume 2. Springer Science Business Media.

Clemens Brunner, Fabian Knirsch, A. U. et al. (2020). A comparison of blockchain-based pki implementations. *International Conference on Information Systems Security and Privacy (ICISSP)*, pages 333–340.

Fang Liu, Guoming Tang, Y. L. et al. (2019). A survey on edge computing systems and tools. *Proceedings of the IEEE*, 107:1537 – 1562.

Farhana Javed, Kiril Antevski, J. M. et al. (2022). Distributed ledger technologies for network slicing: A survey. *IEEE Access*, 10:19412–19442. doi: 10.1109/ACCESS.2022.3151150.

Hui Li, Lishuang Pei, D. L. et al. (2019). Blockchain meets vanet: An architecture for identity and location privacy protection in vanet. *Peer-to-Peer Networking and Applications*, 12:1178–1193.

Jianbin Gao, Qi Xia, X. D. et al. (2019). A blockchain sdn enabled internet of vehicles environment for fog computing and 5g networks. *IEEE INTERNET OF THINGS*, 7:4278–4291.

Lei Liu, Chen Chen, Q. P. et al. (2021). Vehicular edge computing and networking: A survey. *Mobile Networks and Applications*, 26:1145–1168.

Lianhai Liu, Yujue Wang, e. a. (2019). A secure and efficient group key agreement scheme for vanet. *Sensors - MDPI*, pages 482–496.

Mahmood A. Al-Shareeda, Mohammed Anbar, I. H. H. and Manickam, S. (2021). Survey of authentication and privacy schemes in vehicular ad hoc networks. *IEEE SENSORS*, 21-2:2422–2432.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf*.

Nisha Panwar, Shantanu Sharma, A. K. (2016). A survey on 5g: The next generation of mobile communication. *Physical Communication*, 18:64–84.

Paul Rimba, Xiwei Xu, I. W. et al. (2020). Quantifying the cost of distrust: Comparing blockchain and cloud services for business process execution. *Information Systems Frontiers*, 22:489–507.

Poorzare, R. and Augé, A. C. (2020). Challenges on the way of implementing tcp over 5g networks. *IEEE Access*, 8:176393–176415.

Rama Yerramilli, N. K. S. (2019). A comparative study of traditional authentication and authorization methods with block chain technology for egovernance services.

Shaoyong Guo, Xing Hu, Z. Z. et al. (2019). Trust access authentication in vehicular network based on blockchain. *IEEE - China Communications*, 16:19–30.

Tigang Jiang, Hua Fang, H. W. (2019). Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. *IEEE INTERNET OF THINGS JOURNAL*, 06:4640–4649.

Wei Hu, Y. H. et al. (2019). A blockchain-based byzantine consensus algorithm for information authentication of the internet of vehicles. *BIG DATA TECHNOLOGY AND APPLICATIONS IN INTELLIGENT TRANSPORTATION - IEEE ACCESS*, 07:139703–139711.

XiaoDong Zhang, Ru Li, B. C. (2018). A security architecture of vanet based on blockchain and mobile edge computing. *IEEE International Conference on Hot Information-Centric Networking*, page 258–259.