

A Sinfonia Integrada: Otimização de Sistemas de Visão Computacional em Redes Veiculares (VANETs) Através de Offloading Inteligente e Segurança Baseada em Identidade

Pedro Augusto Polegário Alves da Silva (INATEL)

Instituto Nacional de Telecomunicações – INATEL, Av. João de Camargo, 510 – Centro – Santa Rita do Sapucaí - 37536-001

Resumo — Sistemas de Transporte Inteligentes (ITS) modernos dependem da integração eficiente entre Visão Computacional (VC) e Redes Veiculares (VANETs), um cenário complexo devido à alta mobilidade e às restrições rigorosas de tempo real. Aplicações de VC, como o Reconhecimento Automático de Placas de Licença (ALPR) e a Classificação Veicular de Granularidade Fina (FGVC), geram grandes volumes de dados e requerem computação complexa, que excede a capacidade a bordo dos veículos. O Offloading Computacional em Vehicular Edge Computing (VEC) surge como a solução primária para mitigar as limitações de processamento local, delegando tarefas para infraestruturas externas como edge servers, UAVs e nós veiculares. Para gerenciar as decisões dinâmicas de offloading, o Deep Reinforcement Learning (DRL) é empregado como um framework de tomada de decisão adaptativa. Paralelamente, a natureza sensível dos dados veiculares exige mecanismos de segurança robustos. A Autenticação Baseada em Identidade (IBA) é fundamental para verificar a legitimidade das entidades e garantir a privacidade condicional e a rastreabilidade de atores maliciosos nas comunicações V2V e V2I. Este artigo estrutura a análise da otimização de sistemas de VC em arquiteturas VEC/DRL e aborda os requisitos críticos de segurança necessários para o desenvolvimento de VANETs eficientes e confiáveis.

Palavras-chave — Sistemas de Transporte Inteligentes (ITS); Redes Veiculares (VANETs); Computação de Borda Veicular (VEC); Visão Computacional; Aprendizado por Reforço Profundo (DRL); Classificação Veicular de Granularidade Fina (FGVC).

I. INTRODUÇÃO

A indústria automotiva passou por uma mudança transformadora com a integração de sensores embarcados, unidades de processamento a bordo e tecnologias de comunicação sem fio [1]. Esses avanços permitiram a implantação de aplicações orientadas a dados que melhoraram a segurança, a eficiência e o conforto dos veículos [1]. Nesse contexto, os Sistemas de Transporte Inteligentes (ITS) emergiram para mitigar problemas como congestionamentos e melhorar a eficiência do tráfego, utilizando Redes Veiculares (VANETs) como um pilar fundamental para a comunicação entre veículos e infraestruturas [2].

Aplicações ITS, como a direção autônoma e Sistemas Avançados de Assistência ao Motorista (ADAS), geram volumes substanciais de dados e exigem computações complexas com alta sensibilidade ao atraso [1]. No entanto, a natureza móvel e dinâmica dos ambientes veiculares impõe

desafios operacionais, incluindo condições de canal variáveis e recursos computacionais e energéticos limitados a bordo [1].

Para superar as limitações de processamento local, o Offloading Computacional permite que os veículos deleguem tarefas intensivas para infraestruturas mais poderosas, como o Mobile Edge Computing (MEC) ou o Vehicular Edge Computing (VEC) [1]. O VEC localiza recursos de computação próximos aos veículos, utilizando Roadside Units (RSUs) ou módulos de bordo, reduzindo a latência ponta a ponta [1].

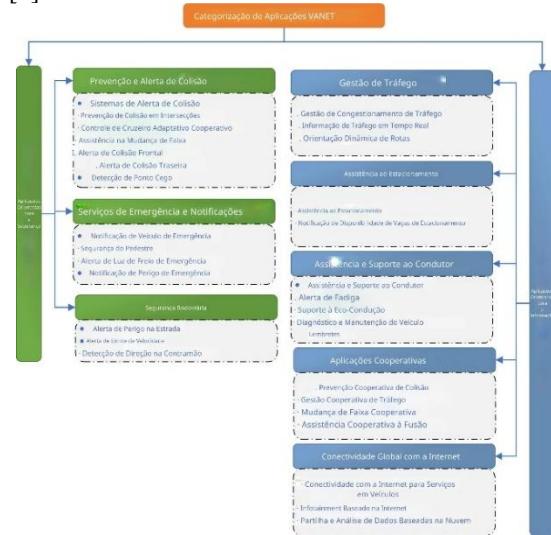


Figura 1: Categorização de aplicações VANET

Simultaneamente, a Visão Computacional (VC) desempenha um papel central na percepção do ITS. Sistemas de identificação veicular baseados em Reconhecimento Automático de Placas de Licença (ALPR) são vitais para o gerenciamento de tráfego, mas enfrentam erros em condições reais desafiadoras, como pouca luz ou obstruções [3]. A integração da Classificação Veicular de Granularidade Fina (FGVC), focada na identificação da marca do veículo, surge como uma medida de validação cruzada para aumentar a confiabilidade do ALPR [3].

A gestão eficiente e segura desse ecossistema exige frameworks avançados, como o Deep Reinforcement Learning (DRL) para offloading adaptativo [1], e protocolos robustos de autenticação, como a Autenticação Baseada em Identidade

(IBA), para garantir a segurança da rede contra-ataques e preservar a privacidade [2].

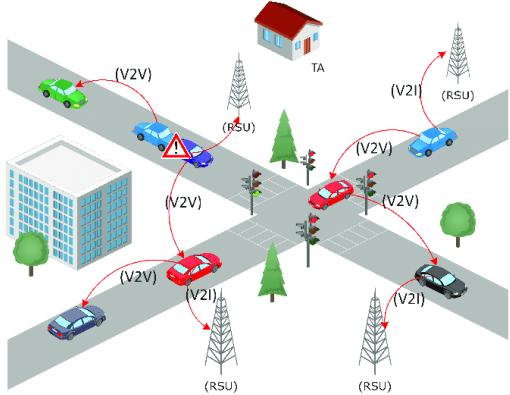


Figura 2: Comunicação VANET

A presente revisão busca abordar esses aspectos com profundidade e rigor acadêmico.

II. FUNDAMENTAÇÃO TEÓRICA

O avanço dos Sistemas de Transporte Inteligentes (ITS) depende intrinsecamente da capacidade de processamento e comunicação das Redes Veiculares (VANETs), que geram volumes substanciais de dados com requisitos rigorosos de tempo real [1]. Para atender a essa demanda, o *Vehicular Edge Computing* (VEC) emprega múltiplos paradigmas de computação que superam as limitações de latência do modelo centralizado de *Cloud Computing*, frequentemente causado pela distância física dos usuários móveis [1]. Surgem, assim, paradigmas "Edge-Cêntricos", como o *Mobile Edge Computing* (MEC), que aloca recursos de computação em estações base ou *Roadside Units* (RSUs) [1], e o *Fog Computing* (FC), que introduz uma camada intermediária para coordenação descentralizada [1]. Paralelamente, o paradigma "Ubíquo e Móvel" explora recursos ociosos através de *Vehicular Cloudlets* (OVS) e utiliza Veículos Aéreos Não Tripulados (UAVs) como plataformas de computação móveis para estender a cobertura em áreas sem infraestrutura [1].

A orquestração desses recursos ocorre através de arquiteturas de rede distintas. A arquitetura centralizada, tipicamente gerida por um servidor na *Macro Base Station* (MBS), simplifica o controle, mas gera gargalos de escalabilidade [1]. Em contraste, a arquitetura distribuída permite que múltiplos nós *edge* colaborem no gerenciamento de carga, aumentando a tolerância a falhas [1]. Uma abordagem híbrida e promissora é a arquitetura hierárquica, que integra recursos locais (veículos), regionais (*fog*) e centrais (*cloud*), mapeando tarefas dinamicamente conforme sua urgência e complexidade, sendo ideal para o *offloading* de tarefas complexas e particionáveis [1].

Para otimizar a tomada de decisão nesses ambientes dinâmicos, utiliza-se o *Deep Reinforcement Learning* (DRL), que modela o problema como um Processo de Decisão de Markov (MDP), definido pela tupla (S, A, P, R, γ) [1]. O agente aprende uma política para maximizar recompensas cumulativas, otimizando objetivos como latência e energia [1]. Algoritmos como *Deep Q-Network* (DQN) são aplicados para

ações discretas [1], enquanto métodos *Actor-Critic*, como *Proximal Policy Optimization* (PPO) e *Deep Deterministic Policy Gradient* (DDPG), lidam com espaços de ação contínuos [1]. Em cenários complexos de VANETs, a abordagem *Multi-Agent* (MARL) é frequentemente necessária, adotando o paradigma de Treinamento Centralizado com Execução Descentralizada (CTDE). Isso permite que algoritmos como MADDPG (Multi-Agent DDPG) e COMA (Counterfactual Multi-Agent Policy Gradient) utilizem informações globais durante o treinamento, mantendo a execução descentralizada e escalável [1].

Uma das aplicações críticas suportadas por essa infraestrutura é o Reconhecimento Automático de Placas de Licença (ALPR), essencial para o ITS, mas suscetível a falhas em condições adversas como má iluminação ou oclusão [2]. Para mitigar esses erros, propõe-se a integração da Classificação Veicular de Granularidade Fina (FGVC), focada na identificação da marca do veículo, servindo como uma validação cruzada para restringir o espaço de busca do ALPR [2]. Modelos de *Deep Learning* como ViT b16, ResNet-34 e EfficientNetV2 têm sido aplicados com sucesso para essa classificação [2]. A precisão desses sistemas é aprimorada por técnicas como a Predição Seletiva, que rejeita inferências de baixa confiança (*softmax-response rejection*) [2], e a Redução de Classes, que agrupa marcas menos frequentes para minimizar erros e manter a representatividade dos dados [2].

Por fim, a integridade de todo esse ecossistema depende de requisitos rigorosos de segurança nas comunicações V2V e V2I, como autenticação, integridade e disponibilidade [3]. A Autenticação Baseada em Identidade (IBA) oferece uma solução eficiente ao utilizar identificadores únicos ou pseudônimos para verificação descentralizada, eliminando a complexidade de infraestruturas de chave pública (PKI) tradicionais [3]. Para equilibrar segurança e privacidade, a IBA deve ser integrada a mecanismos de privacidade condicional. Isso permite o uso de pseudônimos temporários para proteger a identidade dos usuários contra rastreamento não autorizado, ao mesmo tempo que garante a rastreabilidade de entidades maliciosas por uma Autoridade Confiável (TA) em casos de auditoria ou incidentes [3]. Complementarmente, para garantir a eficiência da rede, sistemas de gerenciamento de tráfego como o ICARUS são propostos para controlar congestionamentos e mitigar problemas inerentes às VANETs, como o *broadcast storm* e a sincronização do padrão IEEE 802.11p [4].

III. METODOLOGIA

A abordagem metodológica proposta integra a otimização de recursos computacionais em redes veiculares com o refinamento de sistemas de percepção visual. Inicialmente, aplica-se *Deep Reinforcement Learning* (DRL) para formular políticas de *offloading* no contexto do *Vehicular Edge Computing* (VEC), visando a otimização conjunta de desempenho, latência e consumo de energia. O ambiente é modelado matematicamente como um Processo de Decisão de Markov (MDP), definido por uma tupla que recompensa estocásticas do cenário veicular: os estados capturam as condições do canal sem fio, atributos da tarefa e

disponibilidade de recursos; as ações determinam a seleção do servidor e a frequência computacional; e a função de recompensa é projetada para ser inversamente proporcional ao atraso total e à energia consumida, guiando o agente para decisões ótimas [1].

A arquitetura do sistema DRL é selecionada com base na escala e complexidade do ambiente. Em cenários hierárquicos de múltiplas camadas, o processamento é distribuído dinamicamente entre veículos, *Roadside Units* (RSUs), *fog* e *cloud* [1]. Para coordenar as decisões entre múltiplos servidores de borda ou veículos autônomos, empregam-se frameworks de *Multi-Agent Reinforcement Learning* (MARL), adotando o paradigma de Treinamento Centralizado com Execução Descentralizada (CTDE). Isso permite que agentes aprendam políticas cooperativas utilizando informações globais durante o treinamento, mantendo a autonomia na execução [1]. Complementarmente, para lidar com a contenção de recursos e a otimização de múltiplos usuários, utilizam-se técnicas como a Decomposição Hierárquica, que divide problemas complexos em subproblemas convexos coordenados por DRL, e a integração de Teoria dos Jogos com MARL [1].

Paralelamente à otimização da infraestrutura, a metodologia foca no refinamento da Visão Computacional, especificamente na Classificação Veicular de Granularidade Fina (FGVC) para integração com sistemas de Reconhecimento Automático de Placas de Licença (ALPR). A preparação dos dados utiliza o conjunto Rodosol-ALPR adaptado, onde imagens de motocicletas são excluídas para focar na classificação de carros. O modelo YOLOv10 é empregado para a detecção e recorte preciso dos veículos, enquanto informações da base de dados da Secretaria Nacional de Trânsito (SENATRAN) são utilizadas para rotular automaticamente 9.553 imagens em 29 classes de marcas de veículos [2].

O treinamento dos modelos de *Deep Learning* (incluindo ViT b16, ResNet-34, EfficientNetV2 e MobileNetV3) segue uma abordagem de *transfer learning*, inicializando as redes com pesos pré-treinados. Para garantir a generalização e lidar com o desbalanceamento dos dados, adota-se um protocolo de treinamento (p2) que utiliza *oversampling* para equilibrar a representatividade das classes minoritárias [2]. Para aprimorar a robustez do sistema em condições desafiadoras, implementam-se duas técnicas de refinamento principais: a Redução de Classes, que simplifica o problema avaliando apenas as 11 marcas mais prevalentes e agrupando as demais em uma categoria "Outros" — sendo a abordagem de Redução Estática (retreinamento) a mais eficaz; e a Predição Seletiva, que aplica o método de rejeição baseado na resposta *softmax*, onde o modelo se abstém de emitir uma classificação caso a confiança da predição esteja abaixo de um limiar pré-definido, reduzindo assim a taxa de falsos positivos [2].

IV. RESULTADOS

A validação da arquitetura proposta integra a análise de desempenho em frentes críticas que abrangem desde a precisão da identificação veicular até a eficiência da infraestrutura e a segurança da rede. Inicialmente, a avaliação experimental das técnicas de Classificação Veicular de Granularidade Fina

(FGVC) utilizou o dataset RodoSol-ALPR modificado para estabelecer uma linha de base. O modelo **ViT b16**, treinado sob o protocolo de *oversampling*, demonstrou o melhor desempenho de referência (*baseline*) entre as arquiteturas testadas, superando modelos como ResNet-34 e EfficientNetV2, conforme detalhado na **Tabela I**.

Tabela I: Métricas Globais Alcançadas pelos Modelos de Classificação de Marca

Modelo	Top-1 Acurácia	Top-2 Acurácia	Precisão	Recall	F1-Score
ViT b16	65.4%	73.8%	53.0%	65.4%	56.8%
ResNet-34	49.4%	61.8%	33.9%	49.4%	36.9%
EfficientNetV2	49.4%	60.2%	31.7%	49.4%	33.8%
MobileNetV3	50.7%	61.8%	37.7%	50.7%	41.2%

Fonte: Adaptado de Santos et al. [2].

A aplicação de estratégias de refinamento sobre este *baseline* resultou em ganhos significativos de performance. A técnica de **Redução de Classes**, que agrupa fabricantes menos frequentes em uma categoria genérica, demonstrou eficácia superior na abordagem Estática (que envolve o retreinamento do modelo) em comparação à abordagem online. Como evidenciado na **Tabela II**, a Redução Estática elevou a precisão *Top-1* em 8 pontos percentuais, mitigando a confusão entre classes de menor prevalência.

Tabela II: Comparação de Acurácia ViT b16 com Redução de Classes

Método	Top-1 Acurácia	Top-2 Acurácia
Baseline (29 classes)	65.4%	73.8%
Redução de Classes Estática	73.4%	85.0%
Redução de Classes Online	71.1%	81.5%

Fonte: Adaptado de Santos et al. [2].

A eficácia dessa redução pode ser visualizada através das matrizes de confusão. A **Figura 3** ilustra como o retreinamento (matriz b) limpa a dispersão de erros observada no método *baseline* (matriz a), concentrando as previsões na diagonal principal e confirmando a redução de falsos positivos entre marcas similares.

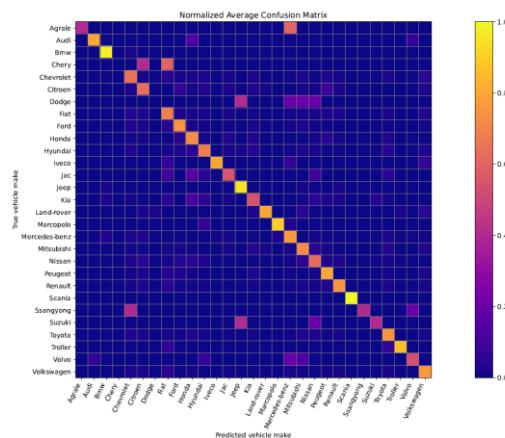
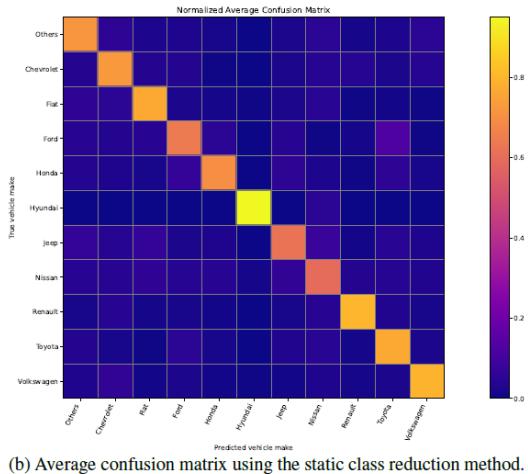


Figura 3: Matriz de confusão média usando o método baseline



(b) Average confusion matrix using the static class reduction method.

Figura 4: Matriz de confusão média usando o método de redução de classes estática.

Nota: A matriz (b) apresenta uma diagonal mais definida em comparação à (a), indicando que o agrupamento de classes raras reduz significativamente a dispersão de classificações errôneas. Fonte: [2].

Resultados ainda mais expressivos foram obtidos através da combinação de **Predição Seletiva** com a Redução de Classes Online. A análise dos dados apresentados na **Tabela III** indica que o aumento do limiar de confiança melhora a precisão, mas eleva proporcionalmente a taxa de rejeição. Ao definir um limiar de confiança de **0,5**, o sistema alcançou um equilíbrio notável, atingindo **90,2%** de precisão *Top-1*. Contudo, essa melhoria impõe um *trade-off* operacional crítico: uma taxa de rejeição de 44,7% das amostras, o que exige um balanceamento cuidadoso para garantir a disponibilidade do serviço em aplicações de tempo real.

Tabela III: Impacto da Predição Seletiva Combinada com Redução de Classes Online

Limiar Confiança	de Imagens Rejeitadas (Taxa)	Top-1 Acurácia	Top-2 Acurácia
0.1	0 (0.0%)	71.1%	81.6%
0.3	207 (17.3%)	78.6%	87.6%
0.5	534 (44.7%)	90.2%	94.6%
0.7	770 (64.5%)	95.8%	97.4%
0.9	1013 (84.8%)	88.5%	88.8%

Fonte: Adaptado de Santos et al. [2].

Para suportar tal processamento intensivo, a arquitetura de rede em *Vehicular Edge Computing* (VEC) desempenha um papel fundamental. A análise comparativa das topologias, apresentada na **Tabela IV**, indica que as arquiteturas hierárquicas superam as abordagens puramente centralizadas ou distribuídas, oferecendo o suporte robusto à mobilidade e a escalabilidade necessárias para ambientes veiculares dinâmicos.

Tabela IV: Comparação de Topologias de Redes Veiculares Edge

Topologia	Latência	Supor te à Mobilidade	Escalabilidade	Complexidade de Controle
MEC Centralizado	Baixa (Alta sob carga)	Médio	Baixa	Baixa
MEC Distribuído	Muito Baixa	Alto	Alta	Média
MEC Hierárquico	Variável	Alto	Alta	Alta
MEC Ad-hoc	Muito Baixa	Muito Alto	Média	Muito Baixa

Fonte: Adaptado de Uddin et al. [1].

Essa estrutura multinível viabiliza esquemas de *offloading* avançados baseados em *Deep Reinforcement Learning* (DRL). Conforme sumarizado na **Tabela V**, algoritmos multi-agente como o MADDPG conseguem distribuir tarefas complexas entre camadas Locais, de Borda (*Edge*) e Nuvem (*Cloud*), otimizando latência e energia simultaneamente, superando as limitações de agentes únicos em cenários de alta densidade.

Tabela V: Esquemas de Offloading DRL em Sistemas Hierárquicos (Seleção)

Tipo de Agente	Objetivo de Otimização	Fonte de Computação	Técnica Chave
Single Agent (DQN)	Energia, Latência	Local, Edge, Cloud	<i>Distributed RL</i>
Single Agent (DDPG)	Energia	Local, Edge, Cloud	Otimização Convexa com FCNN
Multi Agent (MADDPG)	Latência	Local, Edge, Cloud	Treinamento Centralizado, Execução Descentralizada (CTDE)
Multi Agent (Double DQN)	Energia, Latência	Local, Edge, Cloud	<i>Offloading Seguro Baseado em Confiança</i>

Fonte: Adaptado de Uddin et al. [1].

A viabilidade operacional desse ecossistema depende, finalmente, da integração entre eficiência de tráfego e segurança. O sistema ICARUS demonstrou eficácia no gerenciamento de mobilidade, obtendo uma redução no tempo de viagem de pelo menos **32%** e uma redução no tempo de congestionamento de **88%** ao mitigar problemas de comunicação como o *broadcast storm* [4]. Paralelamente, a integridade do sistema é assegurada pela Autenticação Baseada em Identidade (IBA). A **Tabela VI** abaixo destaca que a IBA preenche lacunas essenciais de não-repudião e rastreabilidade que outros protocolos falham em garantir.

Tabela VI: Comparação de Requisitos de Segurança Atingidos por Protocolos Recentes

Referência Original	Autenticação da Fonte	Autenticação da Mensagem	Privacidade	Rastreabilidade	Não-Repúdio
[5]	N/A	N/A	N/A	✓	N/A
[6]	✓	✓	N/A	✓	✓
[7]	X	X	N/A	✓	X
[8]	✓	✓	✓	X	✓

Legenda: (✓) Atingido, (X) Não Atingido, (N/A) Não informado/Aplicável. Fonte: Adaptado de Manasrah et al. [3].

A implementação da IBA exige um equilíbrio com a privacidade condicional. A **Tabela VII** compara abordagens de segurança, evidenciando que soluções baseadas em pseudônimos oferecem um equilíbrio superior entre anonimato e *accountability*, permitindo que uma Autoridade Confiável (TA) revogue o anonimato apenas em incidentes críticos, embora desafios de gestão de chaves em alta mobilidade persistam.

Tabela VII: Análise Comparativa de Abordagens de Segurança em VANETs

Pesquisa	Preservação de Privacidade e Anonimato	Complexidade e Escalabilidade	Centralização
[9]	Privacidade condicional com divulgação de identidade quando necessário.	Desafios com consistência de dados e complexidade de Criptografia baseada em Identidade.	Dependência de RSUs pode limitar a escalabilidade.
[10]	Privacidade condicional, revelando identidades apenas conforme necessário.	Similar ao CPAS em consistência de dados e complexidade criptográfica.	Depende de componentes de infraestrutura que podem não ser universalmente acessíveis.
[11]	Equilibra anonimato e responsabilização com pseudônimos autogerados.	Potencial complexidade devido a múltiplos pseudônimos.	Requer infraestrutura para autenticação.

Fonte: Adaptado de Manasrah et al. [3]

V. PROJETOS FUTUROS

Com base na análise das lacunas atuais em Sistemas de Transporte Inteligentes (ITS), propõem-se três frentes de pesquisa integradas para avançar a segurança e eficiência das redes veiculares. A primeira foca em um *framework* hierárquico de *offloading* colaborativo, motivado pelo fato de que, embora o *offloading* reduza a latência, o uso de modelos pesados de visão computacional como o ViT b16 e o envio de imagens cruas para RSUs geram desafios de largura de banda e privacidade. A metodologia sugere particionar a rede neural para enviar apenas vetores de características para a nuvem ou RSU, otimizados via algoritmos MARL que utilizam técnicas de Redução de Classes para aliviar a carga local, e protegidos

por Autenticação Baseada em Identidade (IBA) para garantir a anonimização dos dados antes da transmissão. A segunda frente visa a orquestração de tráfego resiliente a ataques *Sybil*, nos quais identidades falsas simulam eventos na rede, validando os alertas de congestionamento emitidos por sistemas de gerenciamento como o ICARUS através de confirmação visual cruzada. Utiliza-se a técnica de Predição Seletiva para garantir que apenas classificações visuais de alta confiança sirvam como prova de trabalho, isolando nós que falhem na verificação IBA ou cuja validação visual contradiga o alerta. Por fim, a terceira proposta aborda a adaptação rápida de modelos de *offloading* via *Meta-Learning*, visto que agentes treinados em condições específicas frequentemente falham ao generalizar para novos ambientes, como centros urbanos congestionados. O sistema propõe simular múltiplos cenários de tráfego baseados em padrões reais para treinar um modelo base capaz de ajustar pesos rapidamente sob novas condições de interferência, utilizando a identificação da marca e modelo do veículo vizinho como *input* para inferir a capacidade computacional disponível e acelerar a convergência da política de *offloading*.

VI. CONCLUSÃO

A convergência entre a Visão Computacional avançada e o Vehicular Edge Computing (VEC) representa um marco fundamental para a evolução dos Sistemas de Transporte Inteligentes (ITS). Este estudo demonstrou que a integração de técnicas de Classificação Veicular de Granularidade Fina (FGVC) atua como um mecanismo robusto de validação para sistemas de Reconhecimento Automático de Placas de Licença (ALPR), mitigando erros em cenários adversos. Os resultados experimentais confirmaram que arquiteturas de Deep Learning como o ViT b16, quando refinadas por estratégias de Predição Seletiva e Redução de Classes, podem elevar a acurácia de identificação para patamares superiores a 90%, desde que o trade-off entre precisão e taxa de rejeição seja cuidadosamente calibrado para manter a disponibilidade do serviço.

No entanto, a viabilidade de implantar tais modelos intensivos em dados depende intrinsecamente de uma infraestrutura de computação resiliente e distribuída. A análise das arquiteturas de VEC evidenciou que abordagens hierárquicas, que orquestram recursos desde o veículo até a nuvem, são superiores em escalabilidade e suporte à mobilidade quando comparadas a modelos puramente centralizados. A aplicação de Deep Reinforcement Learning (DRL), especificamente através de frameworks Multi-Agente (MARL) com treinamento centralizado e execução descentralizada (CTDE), provou-se essencial para gerenciar o offloading de tarefas em ambientes dinâmicos, embora a modelagem precise dos custos energéticos de transmissão e a adaptação a novos ambientes permaneçam desafios abertos.

Paralelamente à eficiência operacional, a segurança e a privacidade emergem como requisitos inegociáveis. A Autenticação Baseada em Identidade (IBA) consolidou-se como uma solução eficiente para garantir a legitimidade das comunicações V2V e V2I sem a sobrecarga de infraestruturas de chave pública tradicionais. A implementação da privacidade

condicional dentro da IBA é crítica, assegurando que o anonimato dos usuários seja preservado via pseudônimos, ao mesmo tempo que permite a responsabilização de agentes maliciosos por Autoridades Confiáveis em casos de incidentes ou ataques à rede. Além disso, a estabilidade da rede depende de protocolos de gerenciamento de tráfego capazes de mitigar problemas físicos de comunicação, como o broadcast storm e a dessincronização de canais, garantindo que alertas de segurança sejam disseminados com baixa latência.

Em suma, a plena realização de ITS autônomos e seguros não reside em uma única tecnologia, mas na orquestração sinérgica entre percepção visual precisa, alocação inteligente de recursos na borda e protocolos de segurança robustos. Trabalhos futuros devem focar no desenvolvimento de frameworks de offloading colaborativo que priorizem a privacidade dos dados visuais, na validação cruzada de eventos de tráfego para resistir a ataques Sybil e na aplicação de Meta-Learning para acelerar a adaptação de políticas de controle em cenários urbanos heterogêneos.

VII. REFERÊNCIAS

- [1] A. Uddin, N. Zhang, and A. H. Sakr, "Intelligent Offloading in Vehicular Edge Computing: A Comprehensive Review of Deep Reinforcement Learning Approaches and Architectures," 2025.
- [2] E. Santos, G. E. Lima, R. Laroca, E. Nascimento Jr., and D. Menotti, "Enhancing Vehicle Identification in Challenging Conditions Through Fine-Grained Classification," in Conference on Graphics, Patterns and Images (SIBGRAPI), 2024.
- [3] A. Manasrah, Q. Yaseen, H. Al-Aqrabi, and L. Liu, "Identity-Based Authentication in VANETs: A Review," IEEE Transactions on Intelligent Transportation Systems, 2025.
- [4] A. M. de Souza and L. A. Villas, "Controle de Congestionamento de Veículos Utilizando Sistemas de Transporte Inteligentes," in 30º CTD-Concurso de Teses e Dissertações, 2018.
- [5] S. Prajapat et al., "Secure lattice-based aggregate signature scheme for vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 73, no. 9, pp. 12370–12384, Sep. 2024.
- [6] M. Bayat, M. Barmshoory, S. M. Pournaghi, M. Rahimi, Y. Farjami, and M. R. Aref, "A new and efficient authentication scheme for vehicular ad hoc networks," J. Intell. Transp. Syst., vol. 24, no. 2, pp. 171–183, 2020.
- [7] J. Cui, W. Xu, Y. Han, J. Zhang, and H. Zhong, "Secure mutual authentication with privacy preservation in vehicular ad hoc networks," Veh. Commun., vol. 21, Jan. 2020, Art. no. 100200.
- [8] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," Comput. Commun., vol. 112, pp. 154–164, Nov. 2017.
- [9] K.-A. Shim, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," IEEE Trans. Veh. Technol., vol. 61, no. 4, pp. 1874–1883, 2012.
- [10] H. Lu, J. Li, and M. Guizani, "A novel ID-based authentication framework with adaptive privacy preservation for VANETs," in Proc. Comput. Commun. Appl. Conf., Jan. 2012, pp. 345–350.
- [11] V. C. Sharmila, K. M. Jamuna, K. Jeevitha, I. Kalam, and V. Vennila, "A novel authentication framework with conditional privacy preservation and non-repudiation for fog-VANET," Ann. Romanian Soc. Cell Biol., vol. 25, no. 3, pp. 8353–8363, 2021.