Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.083828

ARTICLE

Context-Aware Identity Validation for UAV-Assisted Urban Mobility and Traffic Monitoring Environments

Kuldashbay Avazov[1], Kudratjon Zohirov[2], Alpamis Kutlimuratov[3], Charos Khidirova[4], Jasur Sevinov[5,6], Urishev Omadjon[7], Adilbek Dauletov[8], Akmalbek Abdusalomov[4,5,9] and Young Im Cho[1,*]

[1]Department of Computer Engineering, Gachon University, Sujeong-Gu, Seongnam-Si, Gyeonggi-Do, Republic of Korea
[2]Department of Software and Technical/Hardware Support of Computer Systems, Karshi State Technical University, Karshi, Uzbekistan
[3]Department of Applied Informatics, Kimyo International University in Tashkent, Uzbekistan
[4]Department of Computer Systems and Artificial Intelligence, Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi, Tashkent, Uzbekistan
[5]Department of Information Processing and Control Systems, Tashkent State Technical University, Tashkent, Uzbekistan
[6]Department of Computer Engineering, University of Tashkent for Applied Sciences, Tashkent, Uzbekistan
[7]Department of Electronics and Instrumentation, Fergana State Technical University, Fergana, Uzbekistan
[8]Department of Digital Technologies, Alfraganus University, Yukori Karakamish Street 2a, Tashkent, Uzbekistan
[9]Department of Artificial Intelligence, Tashkent State University of Economics, Tashkent, Uzbekistan

*Corresponding Author: Young Im Cho. Email: yicho@gachon.ac.kr

Received: 11 April 2026; Accepted: 26 May 2026; Published: 23 July 2026

ABSTRACT: Unmanned aerial vehicles (UAVs) are becoming a common solution to urban mobility, and traffic monitoring as well, owing to their ability to be deployed flexibly, ability to see a broader area and real-time sensing. However, the reliability of UAV-assisted traffic systems can be compromised through identity spoofing, Sybil attacks, false data injection, and trajectory manipulation. Current authentication techniques primarily verify cryptographic identities but often cannot detect when a claimed identity is inconsistent with physical movement patterns and settings. To overcome this drawback, this paper presents a context-aware identity validation system, CIV-UAV, for UAV-based urban traffic surveillance. The paradigm combines a model of cryptographic validation, model mobility, on-the-fly visual, road-network, temporal continuity, anomaly scoring, and multi-UAV consensus into a cohesive trust-based validation model. The risk-adaptive policy also adjusts the validation strictness based on the seriousness of the situation and the level of uncertainty. The outcomes of simulations indicate that CIV-UAV enhances identity validation, lowers the false detection and false acceptance rates, and reinforces the detection of spoofing, Sybil behaviour, path forgery, injection of fake events, and vision-communication mismatch attacks. The suggested architecture provides an identity validation system that is easy to implement and can be upgraded to a next-generation UAV-intelligent transportation network.

KEYWORDS: Context-aware identity validation; UAV-assisted traffic monitoring; urban mobility security; multi-UAV cooperation; trust management; intelligent transportation systems

1 Introduction

The transport systems of cities are becoming more complex, leading to a high demand for smart, real-time, and large-scale traffic monitoring [1]. The relevant unmanned aerial vehicles (UAVs) have

demonstrated the feasibility of intelligent urban mobility, as it provides deployability, flexible coverage, and an aerial view that is complementary to the road shed unit, as well as ground-based cameras and other coverage schemes [2,3]. They are highly flexible and can be applied in modern traffic monitoring applications because they can track traffic levels, detect congestion, and support rapid incident analysis.

Although these advantages apply, the entry of UAVs into urban mobility environments brings up serious security issues. The traffic monitoring procedure employs UAVs to sustain the continuous communication between UAVs, vehicles, road-view framework, and edge or cloud frameworks to solve the threats of identity spoofing, weaponized data assaults, replay assaults, Sybil assaults, and path manipulation assaults [4]. In these safety-sensitive environments, using a false identity may lead to inaccurate traffic patterns and misjudged work decisions [5]. Despite studies on authentication, privacy, and trust management, most solutions continue to conceptualize identity primarily as a cryptographic notion [6]. Consequently, they are not able to set standards for determining the consistency of any claimed identity with actual physical and environmental behavior.

To overcome this limitation, this study proposes a CIV-UAV scheme for the UAV-assisted urban mobility and traffic surveillance setting. The framework generated integrates cyber credentials with mobility behavior, visual evidence, road network limitations, temporal continuity, and joint multi-UAV observations. This makes identity validation transcend message authentication and is resolved by traffic in reality. This will enable the system to not only reject invalid credentials but also to reject valid-looking, contextually erroneous identity claims. The key value additions of this paper are:

- This study proposes a context-aware identity validation framework, named CIV-UAV, for UAV-assisted urban mobility and traffic monitoring environments. The framework validates vehicle identities by combining cryptographic credentials with physical and environmental evidence.
- This work develops a cross-modal trust scoring model that integrates cryptographic validity, mobility consistency, visual observation, road-network constraints, temporal continuity, anomaly behavior, and multi-UAV consensus into a unified identity validation decision.
- The proposed framework introduces a risk-adaptive validation strategy to dynamically adjust the strictness of identity verification according to anomaly severity, contextual uncertainty, and mobility inconsistency, thereby balancing security, reliability, and computational efficiency.
- To assess the proposed framework under realistic adversarial conditions, this study designs a traffic-specific evaluation model covering identity spoofing, Sybil attacks, trajectory forgery, fake event injection, and vision-communication mismatch attacks.

The rest of this paper is structured as follows. Section 2 provides a review of the relevant literature and identifies the research gap this study will address. Section 3 provides the context for urban mobility environments by explaining the problem setting for CIV-UAV using UAVs. Section 4 develops a proposed identity validation model and determines the key context, trust components, and decision components. Section 5 gives the performance analysis, simulation, and analysis under various attack and traffic conditions. Lastly, the paper concludes with Section 6, which outlines potential future research directions.

2 Related Work

In recent years, intelligent transportation systems have been enhanced through machine learning, visual sensing, and UAV-assisted monitoring for mobility management in urban transportation. Ref. [7] demonstrated that machine learning can be applied to aid the analysis of transport infrastructure connectivity and conflict resolution in a complex mobility environment. Similarly, traffic prediction research using visual attributes, a traffic space-time graph learning model, and heterodox traffic flow modeling has enhanced

understanding of dynamic traffic states [8–10]. Flexible coverage, wide-area traffic monitoring, and real-time monitoring are also the reasons why UAV-based traffic surveillance has become important. Swin Transformer with recurrent neural networks was used by [11] to implement UAV-based intelligent traffic surveillance. The majority of traffic monitoring studies, however, have investigated the accuracy of detection, prediction, and surveillance, and identity claims of vehicles are yet to be validated in context.

The second class of studies concerns modeling, predicting, and modeling risk-aware driving behavior. However, Ref. [12] introduced a twisted Gaussian risk model based on longitudinal and lateral motion, and Ref. [13] analyzed the short-term lateral reasoning behavior based on driver preview characteristics. Ref. [14] created Trajectory Prediction by using Lane Crossing Behavior and Good driving styles. These studies are significant as identity validation for UAV-assisted traffic systems will be necessary to confirm that the claimed identity is compatible with realistic motion, lane handling, and road network restrictions. They primarily focus on prediction and planning, however, and do not specifically consider malicious attempts to manipulate identities, spoof, Sybil attacks, or mobility lies. The perception of images and the combination of different sources of information and images are also in focus for intelligent mobility systems today. Causal intervention for target-driven visual navigation has been used by Refs. [15,16] proposed a re-projection multi-task multi-sensor fusion system for autonomous driving 3D object detection and occupancy perception. Localization robustness in challenging city environments has also been recently studied in the field of GNSS/IMU and urban navigation [17–19]. These works employ various spatial, visual, and temporal consistency checks for traffic monitoring using UAVs. However, they do not involve visual observations, identity authentication in multi-UAV consensus, or anomaly scoring within a unified validation framework.

In recent research related to UAVs and aerial networks, deployment, beamforming, resource control, and task offloading have been studied in the context of advanced communications. The deployment and edge association of aerial vehicles for energy-efficient FL were presented by [20], and predictive beamforming based on radar was studied by [21] for the UAV-assisted network. Other works addressed UAV-assisted ISAC systems, full-duplex ISAC for covert communication, ISAC for trajectory control of multiple UAVs, and 6G resource allocation [22,23]. These studies demonstrate the need for UAV-assisted communication and sensing; they focus mainly on network performance, resource efficiency, and/or trajectory optimization, while context-dependent identity trustworthiness of UAVs is rather neglected. There are other studies that offer background context to context-aware traffic intelligence, namely, crash hotspot and road-risk studies. To find out road clusters and intersections with high crash rates, Refs. [24,25] applied spatial data mining and spatial weight matrices. The results of these works indicate that the structure of the road network and spatial context are important for mobility risk analysis. In the case of identity validation, it could involve determining whether it is feasible for a vehicle, given its location and trajectory, to be using a specific road segment, whether this is in line with the road at that time, and/or whether it is spatially consistent. However, these studies have not been geared toward UAV identity verification or aggressive traffic-monitoring environments.

In terms of related literature, traffic monitoring, traffic prediction, trajectory modeling, visual perception, urban navigation, and UAV-assisted communication have advanced, but three gaps remain. First, many studies treat traffic monitoring as a perception or prediction task and do not consider attacks from an identity perspective. Second, authentication-based methods only accept credentials and take no account of physical movement, appearance, travel space limitations, and time continuity. Finally, none of the current UAV-assisted systems are readily integrated to incorporate multiple adaptive trust factors such as cryptographic validation, mobility consistency, visual matching, map constraints, anomaly scoring, and multi-UAV consensus. To fill these gaps, CIV-UAV's design is to validate a vehicle's identity using Cyber credentials and the physical and environmental context, helping detect spoofing, Sybil attacks, trajectory forgery, fake event injection, and mismatches in vision-communication.

3 System Model

This section presents the system architecture, key elements, and mathematical model of the proposed CIV-UAV framework for UAV-enabled urban mobility and traffic monitoring scenarios. Fig. 1 illustrates the integration of UAV and vehicle layers with context-aware trust evaluation, optimization constraints, and risk-adaptive identity validation for secure decision-making. The system model of the UAV-assisted urban traffic monitoring environment is also given in this section. It specifies the key components of the system, such as vehicles, UAVs, RSUs or edge nodes, and the road network in the city, as well as the information exchanged between these components. This section aims to outline the functioning at the monitoring environment and the available observations for identity validation. The mathematical trust computation, validation, decision and optimization formulation are independently performed in Section 4.

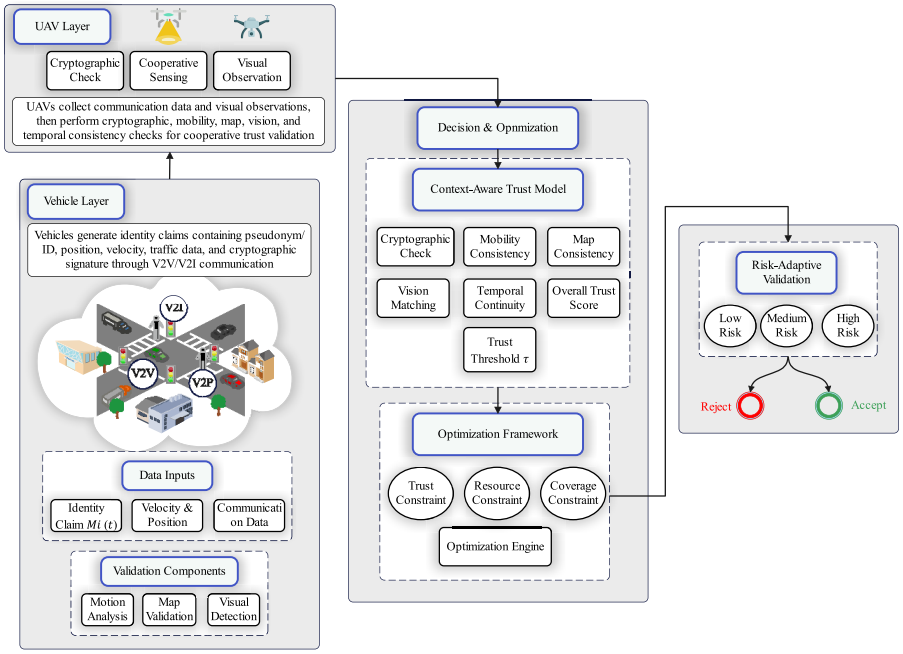

Figure 1: Overall system context of UAV-assisted urban traffic monitoring and interaction among the vehicle layer, UAV layer, and decision-support components.

We consider an urban traffic monitoring system consisting of UAVs, vehicles, roadside units (RSUs) or edge nodes, and an urban road network. Let $\mathcal{U} = \{1, 2, \ldots, U\}$ denote the set of UAVs serving as aerial sensing and validation agents, $\mathcal{V} = \{1, 2, \ldots, N\}$ the set of vehicles generating mobility data and identity claims, and $\mathcal{R} = \{1, 2, \ldots, R\}$ the set of RSUs or edge nodes supporting validation and coordination. The urban road network is modeled as a graph:

$$\mathcal{G} = (\mathcal{L}, \mathcal{E}), \tag{1}$$

in Eq. (1), $\mathcal{L}$ represents road segments or lanes and $\mathcal{E}$ denotes their connectivity. The system operates over discrete time slots $t \in \mathcal{T} = \{1, 2, \ldots, T\}$. At each time slot, every vehicle $i \in \mathcal{V}$ periodically transmits an identity message containing its claimed identity, motion state, application data, and cryptographic proof:

$$M_i(t) = \{ID_i(t), \mathbf{x}_i(t), \mathbf{v}_i(t), d_i(t), \sigma_i(t)\}, \tag{2}$$

in Eq. (2), $ID_i(t)$ denotes the claimed identity or pseudonym, $\mathbf{x}_i(t) = \big(x_i(t), y_i(t)\big)$ is the spatial position, $\mathbf{v}_i(t)$ is the velocity vector, $d_i(t)$ is the reported traffic-related data, and $\sigma_i(t)$ is the attached cryptographic signature. Each UAV $u \in \mathcal{U}$ observes only a subset of vehicles that fall within its communication or sensing range, denoted by $\mathcal{V}_u(t) \subseteq \mathcal{V}$. Along with received identity messages, each UAV also gathers visual observations from onboard sensing devices such as cameras, represented as $\mathcal{O}_u(t) = \{o_{u,1}(t), o_{u,2}(t), \ldots\}$, where every observation represents an identified object with position and motion-related features. This architecture can concurrently leverage communicated identity assertions and real-time sensing data to perform reliable identity validation in UAV-assisted urban traffic monitoring conditions.

According to the system model, the identity-related communication information of every vehicle is broadcast, such as its purported identity, position, velocity, and traffic data. The UAVs receive external visual data of the area covered. The inputs from these communications and sensors are compared with spatial and motion cues to identify prominent contextual features, including cryptographic validity, mobility consistency, road-network feasibility, visual matching, temporal continuity, and cooperative UAV evidence. The features that are extracted are then put together to produce a trust score, which is used to determine whether a given identity $ID_i(t)$ will be accepted or rejected. Unlike traditional methods that rely on credential verification, the framework determines whether the reported identity matches the physical and environmental conditions there. To represent this decision, a binary validation variable is defined as follows:

$$\delta_i(t) = \begin{cases} 1, & \text{if identity is accepted,} \\ 0, & \text{otherwise,} \end{cases} \tag{3}$$

in Eq. (3), a value of 1 indicates acceptance, while 0 denotes rejection. The final validation yields a context-aware trust score $T_i(t)$, calculated in the following subsection and used to validate identities. In analyzing the authenticity of stated identity, the framework uses several dimensions of context, such as cryptographic, mobility, spatial, visual, temporal, and cooperative evidence. Rather than using a single measure, identity legitimacy is evaluated using a set of complementary context scores that test the consistency between the reported identity and the measured traffic environment. Cryptographic validity verifies whether the received message has a valid digital signature:

$$C_i^{\text{crypto}}(t) = \begin{cases} 1, & \text{if signature } \sigma_i(t) \text{ is valid,} \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

In Eq. (4), $C_i^{\text{crypto}}(t)$ represents the cryptographic validity score of vehicle i at time t, where a value of 1 indicates that the signature $\sigma_i(t)$ is valid and a value of 0 indicates an invalid signature. Mobility consistency evaluates whether the reported motion follows physically feasible dynamics. It is modeled as an exponential function of the deviation between reported and predicted velocity:

$$C_i^{\text{mob}}(t) = \exp\left(-\alpha_1 \left\|\mathbf{v}_i(t) - \hat{\mathbf{v}}_i(t)\right\|\right), \tag{5}$$

in Eq. (5), $\hat{\mathbf{v}}_i(t)$ is the predicted velocity and α_1 controls sensitivity. Map consistency ensures that the reported position lies within valid road segments, i.e., $C_i^{\text{map}}(t) = 1$ if $\mathbf{x}_i(t) \in \mathcal{L}$ and 0 otherwise, with possible extensions to lane and direction constraints. Vision-based consistency compares the reported position with UAV observations:

$$C_i^{\text{vision}}(t) = \max_{o \in \mathcal{O}_u(t)} \exp\left(-\alpha_2 \left\|\mathbf{x}_i(t) - \mathbf{x}_o(t)\right\|\right), \tag{6}$$

in Eq. (6), α_2 controls spatial matching sensitivity. Temporal consistency ensures stability of identity over time by penalizing abrupt position changes:

$$C_i^{\text{temp}}(t) = \exp\left(-\alpha_3 \left\|\mathbf{x}_i(t) - \mathbf{x}_i(t-1)\right\|\right). \tag{7}$$

In Eq. (7), α_3 controls sensitivity to abrupt position changes between consecutive time slots. To improve robustness, multi-UAV consensus aggregates validation evidence from multiple UAVs. Finally, an anomaly score captures suspicious behavior patterns, combining trajectory and behavioral anomalies:

$$A_i(t) = \beta_1 A_i^{\text{traj}}(t) + \beta_2 A_i^{\text{behavior}}(t). \tag{8}$$

In Eq. (8), $A_i^{\text{traj}}(t)$ and $A_i^{\text{behavior}}(t)$ denote trajectory-level and behavior-level anomaly scores, respectively, while β_1 and β_2 control their relative contributions. All these context dimensions represent identity legitimacy in totality by an amalgamation of the communication validity and mobility behavior, visual confirmation, temporal continuity, and cooperative sensing, the foundation of trust computation and decision making. Once the individual contextual components have been derived, the next step is to merge them into at single trust measure to validate identity. In the proposed framework, a total trust score is determined by incorporating aspects of cryptographic validity, mobility consistency, confirmation by vision, map consistency, multi-UAV consensus, and temporal consistency, which penalizes deviant behavior. This provides an integrated assessment of how well a purported identity can be countered by both digital authentication demands and the physical context. The overall trust score is expressed as:

$$T_i(t) = w_1 C_i^{\text{crypto}}(t) + w_2 C_i^{\text{mob}}(t) + w_3 C_i^{\text{vision}}(t) + w_4 C_i^{\text{map}}(t) + w_5 C_i^{\text{cons}}(t) + w_6 C_i^{\text{temp}}(t) - w_7 A_i(t), \tag{9}$$

in Eq. (9), $w_1, w_2, \ldots, w_7$ are weighting parameters that determine the relative importance of each context factor. The anomaly score is subtracted, and an increase in the anomaly score indicates a higher probability of suspicious or malicious behavior. To have equal contribution, the weights meet the condition of normalization $\sum_k w_k = 1$. This construction of trust enables the system to move beyond stand-alone checks and to consider identity legitimacy as a product of heterogeneous evidence in its entirety. Consequently, identities with valid credentials may receive low trust scores when they fail to align with mobility, map, visual, or temporal contexts.

This is the level at which validation is so strict as to balance the false acceptance rate and the false rejection rate. An increased threshold enhances security by reducing the likelihood of accepting malicious identities, but also increases the acceptance of legitimate entities and heightens security risk. The trust score $T_i(t)$ offers the primary view of determining whether a claimed identity is regular to the seen communication, mobility, visual, spatial, temporal, and cooperative surroundings. Nevertheless, the accept/reject rule is not determined at this point, since the level of validation strictness can vary depending on the severity of the anomalies, sensing uncertainty, and the system's risk level. As such, a formal validation decision is developed in Section 4 as a formulation that takes an adaptive threshold. The formulation of the proposed identity validation can be cast as an optimization problem, with the objective of maximizing correct identity validation and minimizing false acceptance and false rejection, subject to trust, resource, and coverage constraints. Based on this framework, the system is trying to find an optimal set of binary validation decisions for all vehicles and time slots:

$$\max_{\delta_i(t)} \sum_{i \in \mathcal{V}} \sum_{t \in \mathcal{T}} \delta_i(t), \tag{10}$$

Eq. (10) represents the optimization objective for selecting validation decisions across all monitored vehicles and time slots. This optimization is subject to several constraints. First, the validation decision must satisfy the trust condition, meaning that an identity can only be accepted if its trust score exceeds the decision threshold:

$$\delta_i(t) \le \mathbb{I}\big[T_i(t) \ge \tau\big], \tag{11}$$

in Eq. (11), $\mathbb{I}[\cdot]$ denotes the indicator function. Each UAV also operates under limited computational or validation capacity. Thus, the total validation cost for all vehicles observed by UAV u at time t must remain within the available resource budget, as expressed by $\sum_{i \in \mathcal{V}_u(t)} c_i(t) \le C_u$, where $c_i(t)$ is the validation cost of vehicle i and C_u is the resource capacity of UAV u. In addition, identity validation can only be performed for vehicles located within the observation or coverage region of a UAV, that is, $i \in \mathcal{V}_u(t)$.

This formulation integrates communication-layer authentication with physical and contextual validation into a single system for identity verification in the context of UAV-assisted traffic monitoring. The framework can also identify context-incongruent identities by introducing mobility consistency, map constraints, visual confirmation, temporal continuity, and collaborative UAV observations and identities, even when credentials appear legitimate.

4 Problem Formulation and Proposed CIV-UAV Framework

This section develops the CIV-UAV problem and gives the proposed framework. Using the system model in Section 3, the identity claims $i \in \mathcal{V}$ produced by each vehicle $M_i(t)$ at time $t \in \mathcal{T}$ are determined by the decision variable $\delta_i(t)$, and the system decides whether to accept or reject the identity claim. As the method of urban traffic monitoring by UAVs involves sensing noise, occlusion, limited UAV resources, dynamic movement, and malicious attacks such as spoofing, forging trajectories, and producing false events, UAV-based identity validation cannot be performed solely using binary authentication. Thus, the problem is modelled as a multi-objective optimization problem that transforms communication and sensing evidence into a set of context scores, compands them into a trust score, and risks adaptive validation to sum up the remembrance of true acceptance to false rejection, false acceptance to the falsely rejected, latency, and resource cost. These are reflected in the objective function as follows:

$$\max_{\delta_i(t)} \sum_{t \in \mathcal{T}} \sum_{i \in \mathcal{V}} \left[\lambda_1 \cdot \mathrm{TP}_i(t) - \lambda_2 \cdot \mathrm{FA}_i(t) - \lambda_3 \cdot \mathrm{FR}_i(t)\right], \tag{12}$$

in Eq. (12), $\mathrm{TP}_i(t)$ is the proper acceptance of a legitimate identity, $\mathrm{FA}_i(t)$ is the improper acceptance of a malicious identity, and $\mathrm{FR}_i(t)$ is an improper rejection of a legitimate identity. The relative weight of these components of performance is determined by the coefficients λ_1, λ_2, and λ_3. All these weights enable this framework to trade-off security and reliability depending on the requirements of the application, which offers a principled approach to optimizing CIV-UAV platforms into new UAV-assisted schemes of urban traffic monitoring.

The offered optimization system can be influenced by a range of factors, and identities can be verified in a UAV-based city traffic control environment. Firstly, there should be a threshold condition of trust in the acceptance or rejection of an asserted identity. The validation decision depends on whether the computed trust score exceeds a predefined threshold that may vary according to system state or risk level:

$$\delta_i(t) = \begin{cases} 1, & T_i(t) \ge \tau(t), \\ 0, & \text{otherwise}, \end{cases} \tag{13}$$

in Eq. (13), $\delta_i(t)$ denotes the final validation decision, $T_i(t)$ is the context-aware trust score, and $\tau(t)$ is the adaptive trust threshold adjusted according to contextual uncertainty and anomaly severity. Each UAV is also constrained by limited computational resources. Since identity validation incurs a processing cost for each monitored vehicle, the total validation effort assigned to UAV u at time t must remain within its available resource budget, that is, $\sum_{i\in\mathcal{V}_u(t)} \kappa_i(t) \le C_u$, where $\kappa_i(t)$ is the validation cost of vehicle i and C_u is the computational resource budget of UAV u.

Moreover, for vision-based validation, the comparison should be between the vehicle under consideration and the object within the UAV's field of view, which imposes a latent restraint on sensing. Communication bandwidth also limits the system, as UAVs have a limited capacity to process and exchange identity and sensing data. This communication constraint is formulated as:

$$\sum_{i\in\mathcal{V}} b_i(t) \le B_u, \tag{14}$$

in Eq. (14), $b_i(t)$ denotes the communication load associated with vehicle i at time t, and B_u represents the communication bandwidth available to UAV u. All of these limitations combine to maintain the proposed framework within reasonable bounds in the trust, sensing, computation, and communication domains, enabling it to be utilized in practical applications for dynamic UAV-based traffic monitoring.

The framework presupposes a risk adaptive strategy, and instead of the standard strategy of every identity claim being validated, dynamically adjusts the strength of validation in accordance with the perceived risk level of each entity. This enables effective resource use by applying lightweight validation to low-risk cases and rigorous validation to high-risk situations. The risk score is defined in Eq. (15) by combining anomaly information with context inconsistencies:

$$R_i(t) = \gamma_1 A_i(t) + \gamma_2\left(1 - C_i^{\text{mob}}(t)\right) + \gamma_3\left(1 - C_i^{\text{map}}(t)\right) \tag{15}$$

where $A_i(t)$ indicates the score in anomaly, and mobility and consistency of the map represent the differences between the desired behaviour and the observed behaviour. The coefficients $\gamma_1, \gamma_2, \gamma_3$ control the contribution of each component. Based on this score, validation is categorized into three levels: low risk ($R_i(t) < \theta_1$), medium risk ($\theta_1 \le R_i(t) < \theta_2$), and high risk ($R_i(t) \ge \theta_2$), with increasing validation strictness across levels. To support this adaptive process, the validation threshold is adjusted according to risk level, as defined in Eq. (16):

$$\tau(t) = \begin{cases} \tau_L, & \text{low risk,} \\ \tau_M, & \text{medium risk,} \\ \tau_H, & \text{high risk.} \end{cases} \tag{16}$$

This algorithmic, risk-adaptive method is more efficient and robust, distributing validation resources based on contextual risk, and better balances security and computational cost in dynamically deployed UAV-assisted traffic monitoring systems. The complete procedural flow of the proposed context-aware identity validation process is summarized in Algorithm 1.

Algorithm 1: CIV-UAV context-aware identity validation algorithm

Require: Vehicle messages $M_i(t)$, UAV observations $\mathcal{O}_u(t)$, road graph $\mathcal{G} = (\mathcal{L}, \mathcal{E})$, trust weights $w_1, \ldots, w_7$, risk weights $\gamma_1, \gamma_2, \gamma_3$, thresholds $\theta_1, \theta_2, \tau_L, \tau_M, \tau_H$

Ensure: Validation decision $\delta_i(t)$ for each identity claim

for each time slot $t \in \mathcal{T}$ **do**
  for each UAV $u \in \mathcal{U}$ **do**
    Collect vehicle messages and visual observations from $\mathcal{V}_u(t)$.
    for each vehicle $i \in \mathcal{V}_u(t)$ **do**
      Compute context scores: $C_i^{\text{crypto}}(t)$, $C_i^{\text{mob}}(t)$, $C_i^{\text{map}}(t)$, $C_i^{\text{vision}}(t)$, $C_i^{\text{temp}}(t)$, and $C_i^{\text{cons}}(t)$.
      Compute anomaly score $A_i(t)$, trust score $T_i(t)$, and risk score $R_i(t)$.
      if $R_i(t) < \theta_1$ **then**
        $\tau(t) = \tau_L$
      else if $\theta_1 \le R_i(t) < \theta_2$ **then**
        $\tau(t) = \tau_M$
      else
        $\tau(t) = \tau_H$
      end if
      Set $\delta_i(t) = 1$ if $T_i(t) \ge \tau(t)$; otherwise set $\delta_i(t) = 0$.
    end for
  end for
end for

The proposed CIV-UAV framework has several significant benefits, such as the ability to identify context-inconsistent identities even in cases where valid credentials are provided, flexibility in the adjustment of the validation efforts to risk, and adaptability due to scalability to multi-UAV cooperation, and the fact that it is consistent with the existing and practical constraints of urban traffic. The proposed formulation is based on a real-life context of mobility and space, unlike traditional authentication-only systems, making it more trustworthy and adaptable to the UAV-assisted smart city use case.

5 Simulation Setup and Performance Evaluation

In this section, the suggested CIV-UAV framework is tested in simulated urban traffic monitoring conditions with discrete-time and agent-based Python simulation. The environment is built with NumPy, NetworkX, and matplotlib, in which vehicles propagate on a graph-based road network, and UAVs are aerial agents for sensing and communication with fixed altitude and range, subject to sensing noise and communication constraints. At the time slot, vehicles send identity messages; the UAVs gather communication and visual data; attacks are introduced; and the CIV-UAV algorithm is used to compute trust scores and decisions for validation. The performance is evaluated based on accuracy, strength, false acceptance/rejection, attack detection, latency, and computational overhead.

We model a dense urban traffic environment as a road graph $\mathcal{G} = (\mathcal{L}, \mathcal{E})$, where N vehicles move under lane and road-network constraints within a 1 km × 1 km area, while U UAVs monitor vehicles within their coverage regions at fixed altitudes. The vehicles in every simulation run will be set up on the valid portion of the road with their respective velocities, and mobility and sensing noise will be introduced to mimic realistic movement and aerial perception uncertainty. These attacks are injected by modifying identity claims, positions, trajectories, or event messages per the attack model. The CIV-UAV algorithm is run at every time slot, and its accept/reject decision is compared with the ground-truth label to evaluate accuracy, FAR, FRR,

detection rate, latency, and computational load. The main simulation parameters are summarized in Table 1. The vehicle motion model is defined in Eq. (17) as:

$$\mathbf{x}_i(t+1) = \mathbf{x}_i(t) + \mathbf{v}_i(t)\Delta t + \epsilon_i\ (t) \tag{17}$$

where $\epsilon_i\ (t)$ represents small random disturbances in motion. Similarly, UAV observations are assumed to be affected by sensing noise, and the observed position is modeled in Eq. (18) as:

$$\mathbf{x}_o(t) = \mathbf{x}_i(t) + \eta(t) \tag{18}$$

where $\eta(t)$ denotes the observation noise. The overall interaction among UAVs and vehicles is illustrated in Fig. 2,

Table 1: Simulation parameters for UAV-assisted urban traffic monitoring.

Parameter	Symbol	Value
Number of vehicles	N	50–300
Number of UAVs	U	3–10
Simulation area	–	1 km × 1 km
Time slots	T	100
UAV altitude	H_u	100–150 m
Communication range	–	200–300 m
Vehicle speed	v_i	0–20 m/s
Noise variance (mobility)	$\epsilon_i\ (t)$	Gaussian $(0, 0.5)$
Sensing noise	$\eta(t)$	Gaussian $(0, 1.0)$
Trust threshold	τ	0.5–0.7

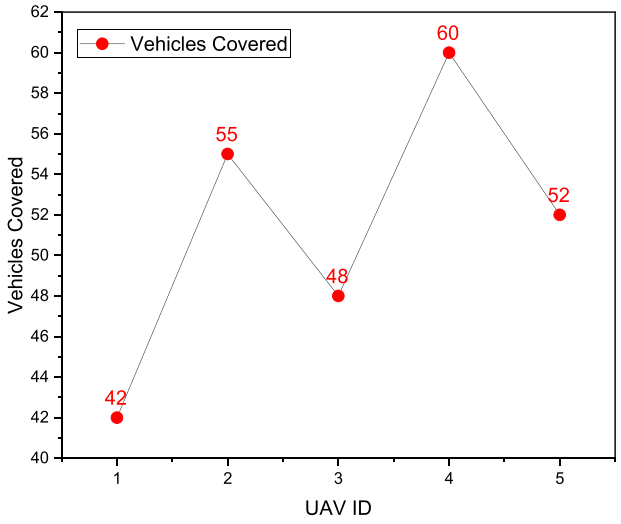

Figure 2: Number of vehicles covered per UAV.

To assess the strength of the suggested framework, several adversarial scenarios are considered, summarized in Table 2. These are identity spoofing, in which malicious entity produces valid credentials and falsifies their location; Sybil attacks, and where a single attacker produces multiple fake identities; trajectory

forgery, where the reported motion is violating of physical or road-network constraints; fake event injection, where false events involving the traffic are reported; and mismatch between vision and communication, where no corresponding UAV observation can be deployed corresponding to a claimed identity. The attack scenarios will model realistic threats in an urban mobility setting and demonstrate how the identified framework can effectively uncover anomalies between digital identity assertions and the physical world.

Table 2: Adversarial attack scenarios in urban traffic monitoring.

Attack Type	Description	Impact
Identity Spoofing	False location with valid credentials	Misleading identity
Sybil Attack	Multiple fake identities	Traffic congestion illusion
Trajectory Forgery	Unrealistic motion reporting	Violates physical constraints
Fake Event Injection	False congestion/accident reports	Wrong traffic decisions
Vision–Communication Mismatch	No visual evidence of claimed entity	Phantom vehicle detection

The proposed CIV-UAV framework is compared with four baseline approaches, as summarized in Table 3. These include Cryptographic Authentication (CA), where identity is only accepted as it is being tested, Location-Based Validation (LBV), where identity is tested as long as it is being observed by the UAV without communication-layer validation, and Trust-Based Model (TBM), where identity is tested according to historic ratings of reputation. These benchmark schemes serve as reference points for comparing the relative effectiveness of the proposed CIV-UAV framework.

Table 3: Comparison of baseline validation approaches.

Scheme	Validation Basis	Strength	Limitation
CA	Digital signature checking	Fast authentication	Ignores physical context
LBV	Location consistency	Detects false positions	Vulnerable to realistic spoofing
TBM	Historical reputation	Detects repeated misbehavior	Slow for new attackers
VOV	UAV visual confirmation	Confirms vehicle presence	Cannot verify identity security
CIV-UAV	Multi-modal contextual validation	Robust identity validation	Moderate complexity

To fully evaluate the effectiveness of the proposed framework, several performance metrics are considered, including identity validation accuracy, false acceptance rate (FAR), false rejection rate (FRR), attack detection rate, validation latency, and computational overhead. These evaluation metrics and their definitions are summarized in Table 4.

The suggested CIV-UAV architecture is critically discussed in various contexts to evaluate its potential to improve identity validation performance, withstand attacks, and conserve computational resources, as presented below. The results are contrasted with baseline schemes and assessed using different performance measures to highlight the benefits of the proposed strategy.

Table 4: Evaluation metrics for identity validation.

Metric	Formula	Description
Accuracy	$\frac{\text{Correct}}{\text{Total}}$	Overall correctness
FAR	$\frac{\text{False Accept}}{\text{Malicious}}$	Security weakness
FRR	$\frac{\text{False Reject}}{\text{Legitimate}}$	Reliability issue
Detection Rate	$1 - \text{FAR}$	Attack detection capability
Latency	$L = \frac{1}{N}\sum t_i$	Decision delay
Overhead	$\sum \kappa_i(t)$	Computational cost

Identity Validation Accuracy: The overall identity validation accuracy of different schemes is presented in Fig. 3. The study findings demonstrate that the proposed CIV-UAV framework is the most accurate at a variety of vehicle and UAV configurations. An accurate improvement of 15%–25% as compared to CA and LBV schemes is realized by CIV-UAV. This may be attributed to the fact that it has incorporated the notion of multi-dimensional context, including consistency in mobility, confirmation of vision, and constraint of map, which minimizes ambiguity and further elaborates on the performance of identity validation.

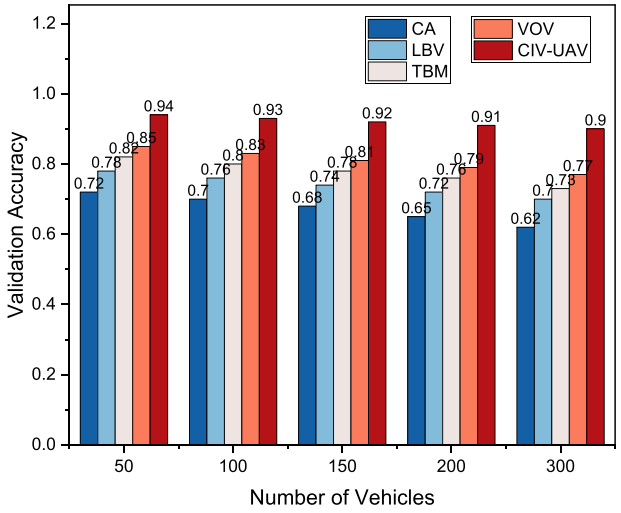

Figure 3: Accuracy comparison under varying traffic density.

False Acceptance Rate (FAR): The false acceptance rate (FAR) performance under different attack scenarios is illustrated in Fig. 4. The CA scheme is characterized by a high FAR, particularly compared to spoofing and Sybil attacks, as it relies solely on cryptographic integrity. On the other hand, the proposed CIV-UAV system will help reduce FAR by 40%–60% by highlighting discrepancies between reported identities and measured context. This has been boosted mainly by cross-modal validation, which synergistically uses communication, vision, and mobility information to more effectively reject malicious identities.

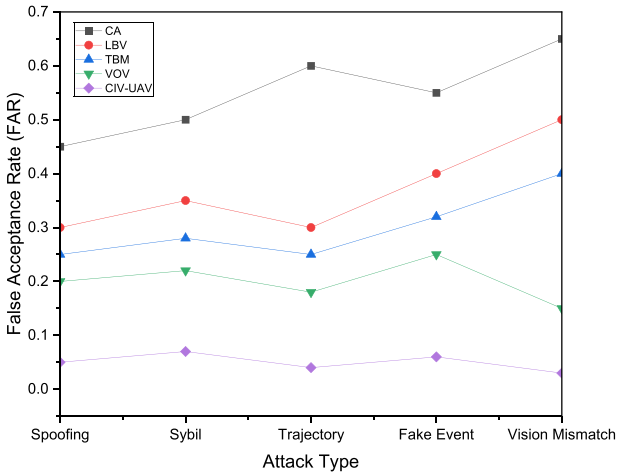

Figure 4: FAR comparison under different attack scenarios.

False Rejection Rate (FRR): Comparison of false rejection rate (FRR) is in Fig. 5. Strict validation schemes may reject valid identities when they are not supposed to, and though the CIV-UAV scheme proposed should have a relatively low FRR, it is risk-adaptive because the validation scheme minimizes risk. Lightweight validation is advantageous in low-risk environments, and stricter validation is offered in high-risk environments to enhance security without compromising honest users. This equal action allows the CIV-UAV to achieve better performance than the TBM and VOV schemes in terms of validation reliability.

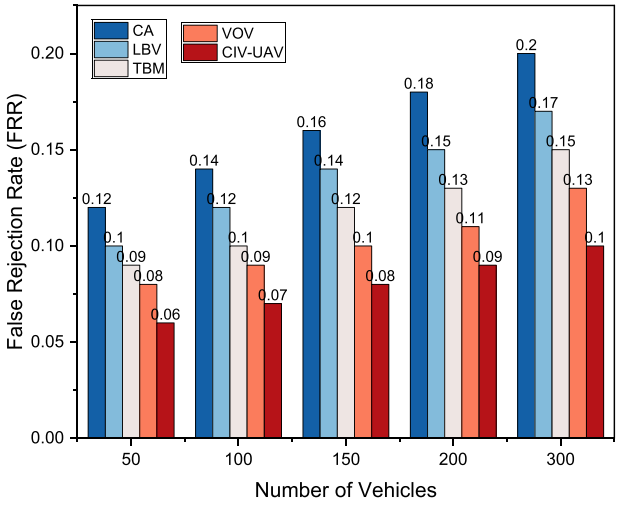

Figure 5: FRR comparison under different schemes.

Detection of Complex Attacks: The detection rates of the various types of attacks can be found in Table 5. The results reveal that CIV-UAV achieves high detection rates across all attack types, with the highest success rates observed for trajectory forgery, mismatched vision communication, and injection of fake events. Unlike the baseline schemes, the integrated scheme is recommended to include multiple dimensions of validation, thereby allowing it to detect sophisticated attacks that would not be detected otherwise.

Table 5: Detection rate (%) under different attack scenarios.

Attack Type	CA (%)	LBV (%)	TBM (%)	VOV (%)	CIV-UAV (%)
Identity Spoofing	45	60	68	72	95
Sybil Attack	40	55	65	70	93
Trajectory Forgery	30	65	70	80	96
Fake Event Injection	35	50	60	75	94
Vision Mismatch	20	40	55	85	97

Impact of Multi-UAV Cooperation: The cooperative validation effect is depicted in Fig. 6. The resulting trust score during UAV validation is more valid because information is fused through consensus among the UAVs. The results prove that multi-UAV cooperation improves validation accuracy on average by 10%–15% and reduces uncertainty significantly in situations when only a portion of the object is seen because of occlusion. This observation highlights the role of distributed, collaborative validation in assessing dense urban landscapes.

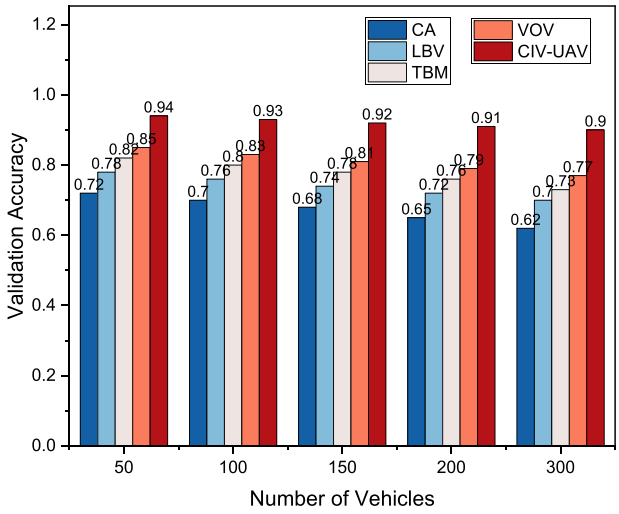

Figure 6: Validation accuracy across various numbers of UAVs.

Validation Latency and Computational Overhead: The results of validation latency and computational overheads are discussed in Fig. 7 and Table 6, respectively. Despite the fact that CIV-UAV requires more computation than the CA and LBV schemes, the proposed risk-adaptive mechanism ensures efficient resource utilization. Specifically, low-risk identities are handled with low overhead, whilst typical high-risk cases are more intensively vetted. As a result, the mean increase in latency remains within a reasonable range of 10%–20%, while the framework achieves high security performance.

The results clearly demonstrate that the proposed CIV-UAV framework provides a significant improvement over traditional validation approaches. Context-aware analysis helps the system recognize malicious identities that would otherwise go undetected due to cryptographic checks. Moreover, cross-modal verification, adaptive decision-making, and multi-UAV cooperation can be integrated to provide a more robust, scalable, and use-case-specific solution for monitoring real-world traffic within the city. Overall, the analysis will demonstrate that CIV-UAV is a vital element for building credibility in UAV-assisted mobility systems, and the novel CIV-UAV framework envisioned in the analysis has the potential to meet this need.

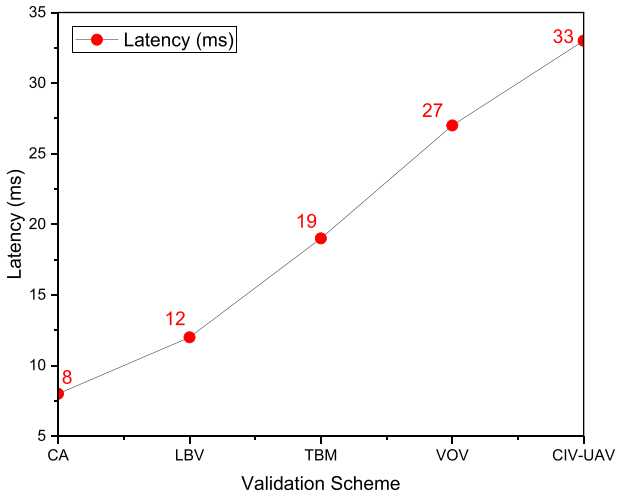

Figure 7: Average validation latency comparison.

Table 6: Average computational overhead and latency comparison.

Scheme	Overhead	Latency (ms)	Complexity
CA	0.18	8	$O(N)$
LBV	0.26	12	$O(N)$
TBM	0.41	19	$O(N \log N)$
VOV	0.57	27	$O(N \cdot U)$
CIV-UAV	0.64	33	$O(N \cdot U)$

6 Conclusion

This study proposes a CIV-UAV framework for UAV-based urban mobility and traffic surveillance applications. Compared with classic methods, where cryptographic authentication is usually the main tool, the framework introduced accounts for a variety of contextual variables, including mobility behavior, visual perception, technological features of the road network, systematic consistency, and cooperation among multiple UAVs. By implementing these points into a single, trust-based, risk-adaptive solution, more reliable identity verification could be achieved in dynamic urban traffic conditions.

The simulation results showed that the CIV-UAV framework is more effective in validation accuracy, reducing false acceptance and false rejection, and improving the detection of more complex attacks, including identity spoofing, Sybil attacks, trajectory forgery, and vision-communication discrepancies. Despite the high effectiveness indicated in the framework, we should examine its performance under harsh sensing uncertainty, in large-scale deployments, and with realistic traffic data in the future. In addition, advanced learning models and decentralized identity management could also be included to further enhance it.

Acknowledgement: Not applicable.

Funding Statement: This research is supported by the Korea Institute of Marine Science and Technology Promotion (KIMST), in 2022 through the Project is Development and Demonstration of Data Platform for AI Based Safe Fishing Vessel Design (Grant Number: RS-2022-KS221571).

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Kuldashbay Avazov, Kudratjon Zohirov, and Alpamis Kutlimuratov; methodology, Charos Khidirova, and Jasur Sevinov; software, Urishev Omadjon; validation, Adilbek Dauletov, and Akmalbek Abdusalomov; formal analysis, Kuldashbay Avazov; investigation, Kudratjon Zohirov; resources, Alpamis Kutlimuratov; data curation, Urishev Omadjon, and Young Im Cho; writing—original draft preparation, Kuldashbay Avazov, and Kudratjon Zohirov; writing—review and editing, Charos Khidirova, Jasur Sevinov, Urishev Omadjon, and Adilbek Dauletov; visualization, Akmalbek Abdusalomov; supervision, Young Im Cho; project administration, Young Im Cho; funding acquisition, Young Im Cho. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Data will be available on reasonable request from the authors.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhang J, Zhang D, Chen X, Zhang T, Wang S. UAV-assisted geo-edge routing protocol for internet of vehicles based on reinforcement learning strategy. IEEE Trans Veh Technol. 2026:1–14. doi:10.1109/tvt.2026.3653679.
2. Bakirci M. Internet of Things-enabled unmanned aerial vehicles for real-time traffic mobility analysis in smart cities. Comput Electr Eng. 2025;123(2):110313. doi:10.1016/j.compeleceng.2025.110313.
3. Ali R, Ali A, Naeem HMY, Asad M, Alsarhan T, Heyat BB. A comprehensive survey of deep learning-based traffic flow prediction models for intelligent transportation systems. ICCK Trans Adv Comput Syst. 2024;1(3):117–37. doi:10.62762/tacs.2025.795448.
4. Miao J, Wang Z, Ning X, Shankar A, Maple C, Rodrigues JJC. A UAV-assisted authentication protocol for internet of vehicles. IEEE Trans Intell Transp Syst. 2024;25(8):10286–97. doi:10.1109/tits.2024.3360251.
5. Ouyang W, Mu J, Jing X, Wang Y. Efficient vehicle recognition and tracking for UAV-enabled intelligent transport systems: a multi-agent reinforcement learning method. IEEE Trans Intell Transp Syst. 2025;26(11):20930–40. doi:10.1109/tits.2025.3601740.
6. Bashir N, Boudjit S, Zeadally S. A closed-loop control architecture of UAV and WSN for traffic surveillance on highways. Comput Commun. 2022;190(7547):78–86. doi:10.1016/j.comcom.2022.04.008.
7. Luo J, Wang G, Li G, Pesce G. Transport infrastructure connectivity and conflict resolution: a machine learning analysis. Neural Comput Appl. 2022;34(9):6585–601. doi:10.1007/s00521-021-06015-5.
8. Wang Q, Chen J, Song Y, Li X, Xu W. Fusing visual quantified features for heterogeneous traffic flow prediction. Promet Traffic Transp. 2024;36(6):1068–77. doi:10.7307/ptt.v36i6.667.
9. Chen J, Zhang S, Xu W. Scalable prediction of heterogeneous traffic flow with enhanced non-periodic feature modeling. Expert Syst Appl. 2025;294(11):128847. doi:10.1016/j.eswa.2025.128847.
10. Fan Y, Chen J, Xu W, Peng W. DADiffNet: delay-aware diffusion networks with adaptive subgraphs for large scale traffic forecasting. Neural Netw. 2026;200:108756.
11. Alshehri M, Wu T, Almujally NA, AlQahtani Y, Hanzla M, Jalal A, et al. UAV-based intelligent traffic surveillance using recurrent neural networks and Swin transformer for dynamic environments. Front Neurorobot. 2025;19:1681341. doi:10.3389/fnbot.2025.1681341.
12. Zhou Z, Wang Y, Zhou G, Nam K, Ji Z, Yin C. A twisted gaussian risk model considering target vehicle longitudinal-lateral motion states for host vehicle trajectory planning. IEEE Trans Intell Transp Syst. 2023;24(12):13685–97. doi:10.1109/tits.2023.3298110.
13. Zhou Z, Wang Y, Liu R, Wei C, Du H, Yin C. Short-term lateral behavior reasoning for target vehicles considering driver preview characteristic. IEEE Trans Intell Transp Syst. 2021;23(8):11801–10. doi:10.1109/tits.2021.3107310.
14. Liu X, Wang Y, Zhou Z, Nam K, Wei C, Yin C. Trajectory prediction of preceding target vehicles based on lane crossing and final points generation model considering driving styles. IEEE Trans Veh Technol. 2021;70(9):8720–30. doi:10.1109/tvt.2021.3098429.

15. Zhao X, Wang T, Li Y, Zhang B, Liu K, Liu D, et al. Target-driven visual navigation by using causal intervention. IEEE Trans Intell Veh. 2024;9(1):1294–304. doi:10.1109/ccdc58219.2023.10327097.
16. Ren Y, Wang L, Li M, Jiang H, Cui Z, Yang M, et al. RM2Occ: re-projection multi-task multi-sensor fusion for autonomous driving 3D object detection and occupancy perception. IEEE Trans Intell Transp Syst. 2025;26(11):20864–81.
17. Li J, Sun R, Wang Y, Ochieng WY. A robust time synchronization algorithm for GNSS/IMU integrated navigation in urban environments. Meas Sci Technol. 2025;36(3):036302. doi:10.1088/1361-6501/ada976.
18. Cheng Q, Chen W, Wang J, Mi X, Yang Y, Sun R. Multi-constellation instantaneous single difference triple-carrier ambiguity resolution in urban environments. GPS Solut. 2025;29(4):186. doi:10.1007/s10291-025-01946-1.
19. Sun R, Sheng Q, Cheng Q, Shang X, Ochieng WY. 3D grid-based resilient pseudorange error prediction for adaptive GNSS/IMU integrated navigation in urban areas. IEEE Internet Things J. 2025;12(12):19264–79. doi:10.1109/jiot.2025.3533077.
20. Wu T, Li M, Qu Y, Wang H, Wei Z, Cao J. Joint UAV deployment and edge association for energy-efficient federated learning. IEEE Trans Cogn Commun Netw. 2025;11(6):4126–40. doi:10.1109/tccn.2025.3543365.
21. Yin R, Peng J, Cai Y, Wu C, Champagne B, Al-Dhahir N. Radar-assisted predictive beamforming for UAV-aided networks: a deep-learning solution. IEEE Trans Veh Technol. 2025;74(10):16079–93. doi:10.1109/icc51166.2024.10622815.
22. Yao Y, Xiao W, Miao P, Chen G, Yang H, Chae CB, et al. UAV-RHS-enabled full-duplex ISAC covert system: robust beamforming and trajectory optimization. IEEE Trans Commun. 2026;74:5637–53. doi:10.1109/tcomm.2026.3668166.
23. Yin R, Peng J, Cai Y, Wu C, Champagne B, Al-Dhahir N. Intelligent 3D trajectory and resource control for multi-UAV 6G networks via GNN and deep unfolding. IEEE Trans Commun. 2026. doi:10.1109/tcomm.2026.3655771.
24. Zhang Z, Ming Y, Song G. A new approach to identifying crash hotspot intersections (CHIs) using spatial weights matrices. Appl Sci. 2020;10(5):1625. doi:10.3390/app10051625.
25. Zhang Z, Ming Y, Song G. Identify road clusters with high-frequency crashes using spatial data mining approach. Appl Sci. 2019;9(24):5282. doi:10.3390/app9245282.