Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.081292

ARTICLE

Generative AI for Efficient and Secure Authentication in UAV-Enabled Smart City Transportation Systems

Akmalbek Abdusalomov[1], Kudratjon Zohirov[2], Sojida Ochilova[2], Jakhongir Oramov[3], Zafar Ruziyev[3], Malika Rustamova[4], Gulrukh Sherboboyeva[5], Komil Tashev[6,7] 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 Finance and Banking, Karshi State Technical University, Karshi, Uzbekistan
[4]Department of Optical Communication Systems and Networks, Karshi State Technical University, Karshi, Uzbekistan
[5]Department of Information Systems and Technologies, Karshi State Technical University, Karshi, Uzbekistan
[6]Department of Artificial Intelligence, Tashkent University of Information Technologies Named after Muhammad Al-Khwarizmi, Tashkent, Uzbekistan
[7]Department of Information Processing and Management Systems, Tashkent State Technical University, Tashkent, Uzbekistan

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

Received: 27 February 2026; Accepted: 16 April 2026; Published: 15 June 2026

ABSTRACT: Unmanned aerial vehicles (UAVs) are also increasingly becoming more often in the transportation infrastructure of smart cities, so that they can successfully achieve real-time observation of traffic, emergency coordination, and two-way communication relaying. However, the security and privacy risks arising in open, highly mobile intelligent transportation systems (ITS) enabled by UAVs are critical, as they pose threats of impersonation, replay, Sybil, and tracking attacks. Secondly, standard static authentication mechanisms are unable to support dynamic risk environments and excessive resource consumption on UAV platforms with limited capacity. To address these challenges, this study introduces a Generative-AI-assisted Risk-Adaptive Authentication (GRAA) system that modulates the intensity of the authentication process based on risk levels identified by mobility, contextual awareness, and the environment. The framework contains unlinkable pseudonymous credentials and, unlike the accumulator-based revocation scheme and AI-based trust evaluation, it is impossible to correlate sessions. The coherence with the majority of attacks is demonstrated under the formal analysis model, which is also based on the real-or-random (ROR) session key, alongside the justifications of forward secrecy and unlinkability. The performance analysis shows that GRAA can achieve up to 87.9% reduction in computation cost and 56.7% reduction in communication overhead compared to pairing-and-group signature schemes, while lowering the latency and energy consumption of the UAVs in a congested urban setting. Generally, the suggested architecture provides a scalable, convenient, and privacy-friendly authentication system for next-generation smart transportation systems that use UAVs.

KEYWORDS: Generative AI; UAV-enabled intelligent transportation systems; risk-adaptive authentication; privacy-preserving security; unlinkability; scalable revocation

1 Introduction

Unmanned aerial vehicles (UAVs) have shifted from being utilized in the military to being important tools in the infrastructure of smart cities. UAVs are also used to assist intelligent transportation systems (ITS) in urban settings, enabling real-time traffic surveillance, emergency management, accident notification, and

Copyright © 2026 The Authors. Published by Tech Science Press. This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

data transmission [1,2]. They are well-suited for developing an elastic, three-dimensional communication infrastructure that involves roadside units (RSUs) and vehicles, given their mobility and communication capabilities [3]. Several parties participate in UAV-enabled transportation systems, including vehicles, RSUs, UAV relays, and edge/cloud servers and send safety-critical messages [4,5]. However, this integration introduces security and privacy threats, such as impersonation and replay attacks, and privacy violations, as multiple authentication exchanges might track vehicles and UAVs.

Traditional authentication schemes in UAV or vehicle networks are static and have the same strength irrespective of the surrounding conditions or danger. Such a method does not work well with dynamic networks, such as smart cities, where traffic levels, emergencies, and network quality fluctuate [6,7]. UAV platforms, specifically, are limited in the ability of their resources (onboard) and therefore fixed authentication schemes are unfeasible [8]. Also, smart city systems need to be efficient in managing identities and revocations. UAVs or vehicles need to be easily revoked when they are compromised; however, classic revocation methods involving a disjointed or centralized list or other centralized schemes will incur high latency and overhead [9–11]. The privacy guarantees, such as unlinkability between sessions, are important to avoid tracking of transportation participants.

Contrary to the conventional authentication mechanism that depends on fixed security configurations, the generated GRAA platform uses generative AI to evaluate the contextual threat and revise authentication intensity in real-time. The generative model examines patterns, including mobility behavior, network conditions, and anomaly indicators, to predict potential threats and, therefore, select the relevant authentication mechanisms. This makes it possible to be proactive and intelligent in security, unlike current solutions, which impose consistent authentication methods despite environmental changes, thereby enhancing security resource efficiency and effectiveness.

To overcome these challenges, we introduce a Generative-AI-assisted, risk-adaptive authentication (GRAA) system for a UAV-enabled smart city. Unlike fixed schemes, our scheme dynamically adjusts authentication strength based on real-time risk assessment. The framework includes privacy-preserving unlinkable credentials, and at scale revocation system with artificial intelligence-assisted detection of unruly behaviours, with minimal disruption. The main contributions include:

1. This study develops a dynamic authentication service that assesses the level of security based on an analysis of the risks relevant to the situation. The structure is effective and robust, and there are several levels of identification that can be applied in the smart city scenario to address the limitations of UAVs.
2. This work proposes a privacy-based authentication layer that enables unlinkable sessions, ensuring that there is no possibility of identity recovery when two vehicles send messages to the RSUs.
3. To demonstrate an improved system of trust and revocation based on anomaly detection to locate malicious or compromised participants and allow invalidation of credentials on a large scale and rapidly.
4. The framework explains the proposal within a real-or-random (ROR) session key security model and demonstrates its resistance to standard attacks using automated protocol verification tools. In addition, we compare the cost of communication and the cost of computation at different risk levels and demonstrate the viability of the framework in the example of smart cities with UAVs.

The rest of the article is structured as follows: Section 2 reviews related work, Section 3 presents the system and threat models, Section 4 describes the proposed framework, Section 5 provides security analysis, Section 6 discusses deployment scenarios, Section 7 presents performance evaluations, and Section 8 concludes with future research directions.

2 Related Work

Security and Privacy in ITS that employ UAVs have attracted significant attention because open wireless channels and high mobility expose a large attack surface. The recent studies [12,13] discuss lightweight authentication for vehicle and V2I applications using elliptic curve cryptography (ECC) to reduce latency while maintaining message integrity and privacy. In [14], ECC-based schemes for dense, dynamic environments are also discussed, with a focus on efficiency under frequent handovers. Moreover, the study [15] focused on anonymous authentication with edge/fog assistance to reduce the workload of centralized authorities. Authentication schemes that avoid leaking identity to others are popularly investigated to reduce identity disclosure and stalking risks [16,17]. It is, however, contentious in these settings, since these mechanisms do not support synchronisation and revocation in environments characterised by high mobility. A higher level of anonymity is provided by group-signature-based authentication, as discussed in [18], but it involves high initial computation and communication complexity, which may be impractical for resource-constrained UAVs

Smart cities require efficient revocation because traditional certificate revocation lists (CRLs) can impose significant communication overhead. The shortcomings of CRL-based systems have been identified in recent works [19], and an aggregator-based revocation scheme is also discussed in [20,21] in order to minimize overheads and increase scalability. Most current methods treat revocation and misbehaviour detection as independent entities, rather than integrating them with adaptive security processes. Methods such as misbehaviour detection, as discussed in [22], are essential for detecting malicious behaviour, including Sybil attacks and false message injection. The works on UAV were also devoted to the development of AI-optimized intrusion detection [23], however, the majority of AI/ML systems are detection-based and are not used to make real-time cryptographic decisions. Authentication and key agreement in a multi-server environment have also been taken up in recent studies. For example, reference [24] introduced a more efficient authentication protocol that resists impersonation attacks while preserving user anonymity and offering superior robustness compared to alternative solutions.

Recent studies have suggested new forms of authentication within UAV-based and vehicle networks, such as blockchain-based architecture, lightweight PUF and ECC protocols, artificial intelligence (AI)-based adaptive security schemes, and others [25,26]. Even though these approaches enhance scalability, efficiency, and intelligence, many of them rely on fixed settings, are computationally intensive, or offer little in terms of privacy preservation and effective revocation in dynamically changing environments. However, the proposed GRAA framework eliminates these shortcomings through risk-adaptive authentication, unlinkable pseudonymous credentials, accumulator-based revocation, and AI-assisted trust evaluation, enabling a highly flexible, privacy-preserving, and efficient solution for smart transportation systems.

Adaptive cybersecurity decision support is a developing method of generative AI implementation [27], but its application to the authentication of UAV ITS communication protocols has not been extensively studied. The article proposes an integrated model of generative-AI-assisted risk assessment with cryptographic authentication and accumulator-based revocation, and aims to assess the levels of security and efficiency in UAV-based smart cities.

3 System Model and Threat Model

This section outlines the network architecture, risk-adaptive security model, and adversary assumptions in the proposed framework, and describes interactions among vehicles, UAVs, roadside units (RSUs), edge servers, and the trusted authority (TA) to maintain secure communication in UAV-enabled smart city transportation systems. The framework considers both external and internal threats and dynamically adapts to evolving security threats.

System Model: The system proposed is made up of vehicles having OBUs, UAVs, RSUs, edge servers, and a centralized TA to issue and revoke credentials, as shown in Fig. 1. Cars produce safety-important messages, UAVs can serve as mobile relays, RSUs provide vehicle-to-infrastructure communication, and edge servers perform computational operations over a poor security channel. To balance security strength and system efficiency, a generative-AI-based risk-adaptive model reviews contextual factors that may determine the degree of authentication: Tier 1 (low risk), Tier 2 (moderate risk), and Tier 3 (high risk). Privacy is ensured by the use of unlinkable pseudonyms and temporal credentials, which prevent session linkage and make revocation easier. This architecture provides scalability, reduced overhead, and high security in large-scale smart city deployments.

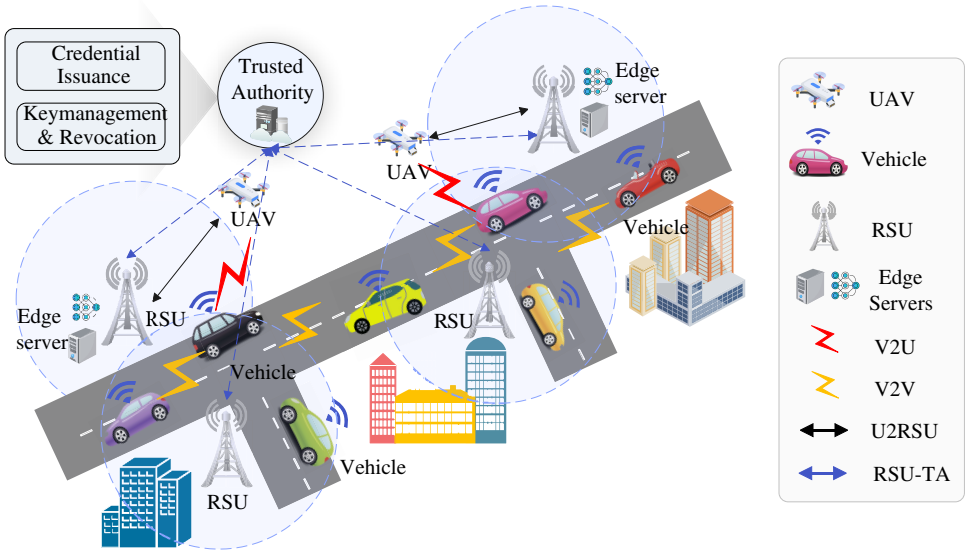

Figure 1: System architecture of the proposed GRAA framework showing interactions between UAVs, vehicles, and RSUs. UAVs assist in data collection and relaying, RSUs provide authentication and coordination, and vehicles communicate securely through adaptive risk-based authentication.

Threat Model: The adversary model takes into account the presence of external and inside attackers, who could use the public medium to eavesdrop, modify messages, replay, and impersonate, and they could also make efforts to compromise the credentials. The proposed scheme provides high security levels by maintaining the confidentiality of session keys, ensuring forward secrecy and mutual authentication, and being unlinkable and resistant to replay, impersonation, Sybil, and credential-cloning attacks. Scalability is further enhanced by efficient revocation mechanisms with minimal overhead. In the example of a smart city, a UAV with vehicles and RSUs will use lightweight authentication in low-risk environments, and more intensive verification in high-risk situations, allowing a balance between security and efficiency in real life.

4 Proposed Generative-AI-Assisted Risk-Adaptive Authentication Framework

This section presents the proposed framework, including system initialization, privacy-preserving credential generation, risk-adaptive authentication, and AI-assisted revocation.

Let $\mathcal{TA}$ be the trusted authority, with V_i, U_j, and R_k representing a vehicle, UAV, and roadside unit (RSU), respectively. $\mathbb{G}$ is a cyclic group of prime order q with generator $P \in \mathbb{G}$. The notation $h(\cdot)$ represents a secure hash function, $\oplus$ denotes XOR, and $\|$ represents concatenation. Security is based on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP) in $\mathbb{G}$. The trusted authority $\mathcal{TA}$ selects a master

private key $s \in \mathbb{Z}_q^*$, computes the public key $P_{\text{pub}} = sP$, and publishes system parameters $\{\mathbb{G}, q, P, P_{\text{pub}}, h(\cdot)\}$. The master secret s is securely maintained by $\mathcal{TA}$. The key notations used throughout the proposed authentication protocol are summarized as follows. ID_i and PID_i denote the real and pseudonymous identities of the i-th entity, respectively. SK represents the session key, while PK and SK_{priv} denote public and private keys. $H(\cdot)$ indicates a secure cryptographic hash function, and r_i denotes a randomly generated nonce. T represents the timestamp used to ensure the freshness of messages. $\oplus$ denotes the bitwise XOR operation, and $\|$ indicates concatenation. These notations are consistently used across all protocol phases for authentication and key agreement. Each entity $E_i \in \{V_i, U_j, R_k\}$ selects a random value $x_i \in \mathbb{Z}_q^*$ and computes $X_i = x_i P$. This is securely sent to $\mathcal{TA}$, which computes $C_i = r_i P$ and $\sigma_i = r_i + s \cdot h(ID_i \| X_i \| C_i) \bmod q$, returning the tuple (C_i, σ_i). The entity then constructs its private key $SK_i = \sigma_i + x_i \cdot h(ID_i \| X_i \| C_i) \bmod q$ and computes the public key $PK_i = SK_i P$. Each entity generates a new pseudonymous credential for each session to ensure unlinkability. For session t, entity E_i selects a random value $\alpha_{i,t} \in \mathbb{Z}_q^*$ and computes $PID_{i,t} = h(ID_i \| \alpha_{i,t})$ and $T_{i,t} = \alpha_{i,t} P$. The pseudonym pair $(PID_{i,t}, T_{i,t})$ is unique to the session, preventing linkability across sessions.

Assume vehicle V_i authenticates with UAV U_j. The generative AI module evaluates contextual features $\mathcal{C}$ (e.g., traffic density, mobility variance) and computes a risk score $R = \mathcal{G}(\mathcal{C})$. Based on thresholds τ_1 and τ_2, authentication mode is selected: M_1 if $R < \tau_1$, M_2 if $\tau_1 \le R < \tau_2$, and M_3 if $R \ge \tau_2$. To start authentication, V_i selects an ephemeral secret e_i, computes $E_i = e_i P$, and generates a session proof $Auth_i = h(PID_{i,t} \| E_i \| Mode \| t_i)$. V_i then transmits $(PID_{i,t}, T_{i,t}, E_i, Auth_i, Mode, t_i)$ to U_j. Upon receiving it, U_j verifies the timestamp and pseudonym, selects e_j, computes $E_j = e_j P$, and derives the shared secret $K = e_j E_i = e_i e_j P$. The session key $SK_{ij} = h(K \| PID_{i,t} \| PID_{j,t} \| Mode)$ is then computed, and $Auth_j = h(SK_{ij} \| E_j \| t_j)$ is returned along with $(PID_{j,t}, T_{j,t}, E_j, t_j)$. Finally, V_i computes $K = e_i E_j$, derives SK_{ij}, and verifies $Auth_j$ to complete authentication. The entire workflow discussed here is summarized in Algorithm 1 and consists of system starting, issuing credentials, risk assessment, adaptive mode choice and intelligent revocation. It shows contextual intelligence to modify the strength of authentication whilst maintaining the forward secrecy, unlinkability, and effective revocation. The step-by-step authentication procedure, which involves system initialisation, system contextual risk assessment via Generative AI, selection of adaptive authentication mode (M1, M2, M3), creation of a pseudonym, mutual authentication, evaluation of trust, and revocation of malicious identities are shown in Fig. 2.

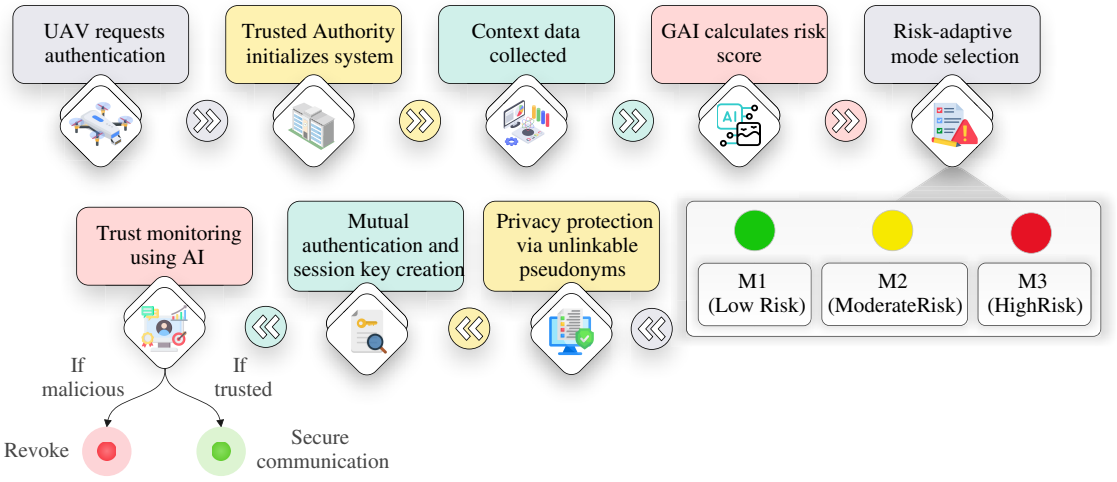

Figure 2: Flow diagram of the generative-AI-assisted risk-adaptive authentication (GRAA) process.

Algorithm 1: Generative-AI-assisted risk-adaptive authentication (GRAA)

Input: Entities E_i, E_j; context $\mathcal{C}$; thresholds τ_1, τ_2, γ; system params $\{\mathbb{G}, q, P, P_{\text{pub}}, h(\cdot)\}$
Output: Mutual authentication decision and session key SK_{ij}

Step *Initialization & Registration*
  TA selects $s \in \mathbb{Z}_q^*$ and computes $P_{\text{pub}} = sP$; For entity E_i: choose x_i, compute $X_i = x_i P$, send (ID_i, X_i) to TA; TA selects r_i, computes $C_i = r_i P$ and $\sigma_i = r_i + s \cdot h(ID_i \parallel X_i \parallel C_i)$; E_i computes $SK_i = \sigma_i + x_i \cdot h(ID_i \parallel X_i \parallel C_i)$ and $PK_i = SK_i P$.
Step *Risk Evaluation & Mode Selection*
  Compute contextual risk $R = \mathcal{G}(\mathcal{C})$;
  if $R < \tau_1$ **then**
    $Mode \leftarrow M_1$;
  else
    if $R < \tau_2$ **then**
      $Mode \leftarrow M_2$;
    else
      $Mode \leftarrow M_3$;
Step *Mutual Authentication*
  Initiator E_i;
  Generate pseudonym $PID_{i,t} = h(ID_i \parallel \alpha_{i,t})$ and $T_{i,t} = \alpha_{i,t} P$; Select e_i, compute $E_i = e_i P$; Compute $Auth_i = h(PID_{i,t} \parallel E_i \parallel Mode \parallel t_i)$; Send $m_1 = \{PID_{i,t}, T_{i,t}, E_i, Auth_i, Mode, t_i\}$.
  Responder E_j;
  Verify freshness and $Auth_i$; Generate $PID_{j,t}$, $T_{j,t}$ and select e_j; Compute $E_j = e_j P$ and shared secret $K = e_j e_i P$; Derive$SK_{ij} = h(K \parallel PID_{i,t} \parallel PID_{j,t} \parallel Mode)$.
  if $Mode = M_3$ **then**
    Compute credential proof $\Delta_j = h(SK_{ij} \parallel C_j \parallel PK_j)$;
  Compute $Auth_j = h(SK_{ij} \parallel E_j \parallel t_j \parallel \Delta_j)$; Send $m_2 = \{PID_{j,t}, T_{j,t}, E_j, \Delta_j, Auth_j, t_j\}$; E_i verifies $Auth_j$ and finalizes SK_{ij}.
Step *Trust Update & Revocation*
  Update trust: $Trust_i(t+1) = \lambda Trust_i(t) + (1-\lambda) f(\mathcal{A}_i)$;
  if $Trust_i < \gamma$ **then**
    Update accumulator $Acc_{\text{new}} = Acc_{\text{old}} \cdot H(ID_i) \bmod N$; Revoke identity and deny further authentication.

In high-risk scenarios (Mode M_3), an additional credential consistency check strengthens security against insider threats. The initiator computes $\Delta_i = h(SK_{ij} \parallel C_i \parallel PK_i)$, which binds the session key to the certificate components. The responder verifies this using (C_i, PK_i) to ensure identity consistency, offering stronger protection against impersonating nodes. Each entity maintains a dynamic trust score, updated as $Trust_i(t+1) = \lambda\, Trust_i(t) + (1-\lambda) f(\mathcal{A}_i)$, where $\mathcal{A}_i$ are anomaly indicators. When the trust score falls below a threshold γ, the entity is flagged as suspicious. The trusted authority updates the revocation accumulator $Acc_{\text{new}} = Acc_{\text{old}} \cdot H(ID_i) \bmod N$, enabling efficient revocation without large CRLs. Compact revocation proofs allow for constant verification complexity, improving scalability. Security properties of the framework are based on complementary schemes: forward secrecy is provided by session keys which are based on the Diffie-Hellman term $e_i e_j P$. Cross-session linkability is disabled through session pseudonym $PID_{i,t}$. Risk-adaptive mode can be considered an efficient and secure mode, and anomaly-driven trust evaluation and accumulator-based revocation offers scalability, proactive defense against malicious parties.

5 Security Analysis

This section analyzes the security of the proposed Generative-AI-assisted risk-adaptive authentication framework, focusing on session key security under the Real-Or-Random (ROR) model, unlinkability, resistance to common attacks, and the feasibility of automated verification. Although the ROR model is grounded in theory, it works only under idealized conditions of adversarial interactions and does not adequately represent the real-life threats like side-channel attacks or implementation-level vulnerabilities, thus calling for the need to validate it on a real-world scale. Under the ROR model, a probabilistic polynomial-time adversary $\mathcal{A}$ interacts with protocol instances through oracle queries such as $Execute$, $Send$, $Reveal$, $Corrupt$, and $Test$ to distinguish between real and random session keys, forming the basis for evaluating semantic security.

$$Adv_{\mathcal{A}}^{ROR} = \left|\Pr[b' = b] - \frac{1}{2}\right|,$$

where $b \in \{0,1\}$ is the challenger's hidden bit.

Theorem 1: *Under the hardness assumption of the Elliptic Curve Computational Diffie–Hellman (ECCDH) problem in the group* $\mathbb{G}$, *the advantage of any polynomial-time adversary in distinguishing the session key from a random value is negligible and bounded by:*

$$Adv_{\mathcal{A}}^{ROR} \leq \frac{q_h^2}{2q} + Adv_{ECCDH},$$

where q_h *denotes the number of hash queries,* q *is the group order, and* Adv_{ECCDH} *represents the advantage of solving the ECCDH problem.*

The proof follows a standard game-based argument. In Game 0, the real protocol execution is considered. In Game 1, the hash function $h(\cdot)$ is replaced with a random oracle, introducing a difference bounded by the collision probability $\frac{q_h^2}{2q}$. In Game 2, the shared Diffie-Hellman secret $K = e_i e_j P$ is replaced with a random group element. If an adversary can distinguish this modification, it can be used to solve the ECCDH problem. Therefore, the difference between Game 0 and Game 2 is bounded by $\frac{q_h^2}{2q} + Adv_{ECCDH}$. Since the session key in Game 2 is uniformly random, the adversary's distinguishing advantage is negligible. Hence, the established session key is secure under the ECCDH assumption. The established session key is computed as $SK_{ij} = h(e_i e_j P \parallel PID_{i,t} \parallel PID_{j,t} \parallel Mode)$, where the shared secret is derived from the ephemeral Diffie-Hellman term $e_i e_j P$. Even if the long-term private keys SK_i and SK_j are compromised at a later stage, previously established session keys remain secure because the ephemeral secrets e_i and e_j cannot be feasibly recovered from their public values $E_i = e_i P$ and $E_j = e_j P$ under the hardness assumption of the Elliptic Curve Discrete Logarithm Problem (ECDLP). Consequently, the proposed scheme achieves perfect forward secrecy. To ensure unlinkability, each authentication session employs a fresh pseudonym computed as $PID_{i,t} = h(ID_i \parallel \alpha_{i,t})$, where $\alpha_{i,t}$ is a randomly selected session-specific value. Due to the randomness of $\alpha_{i,t}$, pseudonyms generated in different sessions satisfy $PID_{i,t_1} \neq PID_{i,t_2}$ with overwhelming probability. Without knowledge of the underlying identity ID_i and the secret parameter $\alpha_{i,t}$, an adversary observing protocol transcripts cannot correlate multiple sessions to the same entity. Formally, the adversary's linking advantage is bounded by $Adv_{link} \leq Adv_{preimage}(h)$, which is negligible under the preimage resistance assumption of the hash function. Therefore, the proposed scheme achieves strong unlinkability across authentication sessions.

The framework suggested offers a solid resistance to the normal attacks within open wireless environment scenarios. The freshness is guaranteed by avoiding replay attacks with the help of timestamp t_i

and another parameter called ephemeral parameters E_i. Man-in-the-middle attacks are prevented because the shared secret $K = e_i e_j P$ is derived from an elliptic-curve Diffie-Hellman exchange, and computing the secret without the ephemeral secrets is impossible. Authentication value $Auth_j$ or $Auth_i$ forging is only possible with valid session keys and legitimate pseudonym parameters, thus preventing impersonation. In high assurance mode M_3, the extra consistency check Δ_i binds authentication to issued credentials, which enhances protection against insider attacks. Mitigations toward sybil attacks are achieved by regulated issuance of credentials and trust worth evaluation with the help of AI, in which entities whose trust value is less than threshold γ are revoked. Furthermore, forward secrecy is provided by using independent ephemeral secrets, which are used in securing previous session keys.

The generative AI module establishes the mode of authentication based on the score of the risk as determined, as $Mode = f(R)$. It is a property of adaptive selection that, even with the different authentication modes built on the identical hardness assumption of the Elliptic Curve Computational Diffie-Hellman (ECCDH) problem, it does not weaken the underlying cryptographic primitives. In every mode, there is a minimum baseline security, so that the adaptive mechanism only influences the level of computational complexity and operational efficiency, not the cryptographic soundness. The competitive nature of authentication strength is thus used to further the optimization of performance without affecting the basic security properties. Revocation is enforced through an accumulator-based mechanism in which the revocation value is updated as $Acc_{\text{new}} = Acc_{\text{old}} \cdot H(ID_i) \bmod N$. To authenticate, entities must provide valid non-membership evidence to prove that their identity is not incorporated into the revocation accumulator. In the event of identity revocation, the compromised entities cannot produce valid proofs and thus cannot gain any further access to system services. Such a design results in a tight revocation representation, high verification efficiency, and high security.

The suggested protocol is formally proved with the help of the automated verification tools such as HLPSL and ProVerif within the framework of the Dolev-Yao adversarial model, having the key security properties of mutual authentication, session key secrecy, freshness, and resistance to replay, impersonation, and man-in-the-middle attacks. Symbolic model checking is used to verify the protocol against an active opponent that can intercept, alter, and introduce messages, and the outputs ensure that no sensitive data is exposed and that the opponent has not been subjected to any logical threat. Along with offering forward secrecy, session unlinkability, and efficient revocation through anomaly-based trust assessment, the framework also has practical deployment considerations. In particular, it includes adaptive re-authentication of failed authentication attempts, temporary isolation, reduced trust in suspicious UAVs, and fallback procedures in the case of a network failure to enable service continuity. All these characteristics lead to increased strength, dependability, and convenience of the offered framework in dynamic, resource-constrained UAV-enhanced environments.

6 Deployment in UAV-Enabled Smart City Transportation Systems

In this section, we describe how the proposed Generative-AI-assisted risk-adaptive authentication framework can be deployed across different communication scenarios in UAV-enabled smart city transportation systems. We demonstrate its applicability in vehicle-RSU, UAV-RSU, UAV-UAV, and vehicle-UAV communication models.

Vehicle-RSU Communication: In urban traffic environments, vehicles periodically communicate with roadside units (RSUs) to obtain traffic updates, infrastructure alerts, signal phase and timing information, and congestion reports. When a vehicle V_i approaches an RSU R_k, the generative AI module deployed at the RSU evaluates contextual features $\mathcal{C}$, including traffic density, historical anomaly records, and trust levels, to compute a risk score $R = \mathcal{G}(\mathcal{C})$. Based on the resulting risk tier, the appropriate authentication mode M_1,

M_2, or M_3 is selected, and mutual authentication is performed using unlinkable pseudonymous credentials. It is an adaptive response that minimizes authentication latency in low-risk, low-density situations with lightweight verification, while supporting high-assurance validation in the event of emergencies or suspicious events. Therefore, the framework reduces unnecessary calculations that vehicle OBUs would otherwise have to perform, while remaining highly secure in critical situations.

UAV-RSU Communication: UAVs can also play the role of overhead relay and observation forces that usually exchange information with RSUs in order to offload and access data, signal control, and emergency coordination. Since UAVs are battery-powered, resource-constrained devices, security overhead ought to be managed. The proposed adaptive model will enable lightweight authentication in normal operating conditions to conserve power and minimize latency, and automatically participate in the enhanced authentication process when anomalous or suspicious mobility behaviour has been detected. In cases where a UAV is suspected of compromise, its trust score is dynamically updated according to $Trust_j(t+1) = \lambda Trust_j(t) + (1-\lambda) f(\mathcal{A}_j)$, and if the resulting value falls below the predefined threshold γ, revocation is triggered to prevent further network participation. This mechanism ensures energy-efficient operation while maintaining strong security and rapid containment of compromised aerial nodes.

UAV-UAV Communication: UAV-UAV communication is a major aspect of cooperation between the use of monitoring in smart cities through the transportation system, emergency aerial coordination, and multi-hop data relaying. Aerial networks are also highly susceptible to impersonation and Sybil attacks due to high mobility and dynamic topological changes. The contextual risk score R can also include more samples under dense aerial deployment conditions than the threshold τ_2, which should trigger the high-assurance authentication mode M_3. In this mode, the step of a further tool of credential consistency is performed with the help of $\Delta_i = h(SK_{ij} \parallel C_i \parallel PK_i)$, with the help of which the session of the issue is cryptographically bound with issue credentials. This improved validation scheme attacks insider impersonation and malicious multi-identity attacks on clusters of UAVs.

Vehicle-UAV Communication: There may also be direct communication between vehicles and UAVs, which can be used in the event of accident reporting, constant hazards detection, and temporary connectivity in infrastructure-damage areas. As the repeated interactions between the vehicles and UAVs might compromise the privacy of vehicles due to their exposure to tracking in the event of utilizing the repeated identifiers, the proposed framework supports privacy by applying a session-based pseudonym generated as $PID_{i,t} = h(ID_i \parallel \alpha_{i,t})$. The protocol ensures privacy in dynamic aerial-ground communication use cases by creating new pseudonyms every time the session lasts, and thus external observers can not correlate different interactions to the underlying identity, ensuring privacy.

The generative AI module can be deployed at MEC servers, RSUs, or in a hybrid architecture to enable efficient and real-time risk assessment, satisfying the latency constraint $T_{AI} + T_{auth} \leq T_{max}$ while ensuring $T_{AI} \ll T_{cloud}$ through edge-based inference. The proposed system supports large-scale smart city environments with numerous vehicles, UAVs, and RSUs by employing adaptive authentication that reduces cryptographic operations under low-risk conditions and minimizes revocation overhead. The communication cost per authentication in mode M_k is defined as $Comm(M_k) = \sum_{i=1}^{n_k} |m_i|$, where $n_1 < n_2 < n_3$, enabling dynamic adjustment of message complexity based on contextual risk. Overall, the framework integrates AI-driven risk evaluation with efficient cryptographic mechanisms to achieve scalable, low-latency, and privacy-preserving authentication in UAV-enabled transportation systems.

7 Performance and Comparative Analysis

In this section, we assess the computational performance, communication overhead, adaptability latency, energy usage, and scalability of the proposed GRAA framework. The framework is compared with

representative authentication schemes commonly used in UAV-enabled ITS and vehicle networks. All the schemes are tested at comparable 128–160 bit security levels so as to ensure fairness.

Comparative Authentication Models: To assess the efficacy of the proposed framework, we consider representative authentication models. Static ECC-Based Mutual Authentication (SEMA) is a standard ECC-based key exchange protocol without adaptive security. Certificateless Public Key Authentication (CL-PKA) is an ECC-based certificateless scheme requiring additional scalar multiplications and exponentiations. Pairing-Based Anonymous Authentication (PBAA) is a stronger authentication that uses bilinear pairing, but is more expensive. Group Signature-Based Authentication (GSBA) has both privacy and unlinkability based on group signatures. CRL-Integrated Static Authentication (CRL-SA) uses certificate revocation list verification, whereas Machine Learning-Assisted Static Authentication (ML-SA) combines machine learning with static authentication. A detailed comparison of these models is provided in Table 1.

Table 1: Operational characteristics of comparative authentication models.

Model Name	Cryptographic Primitive	Adaptive Mechanism	Privacy Level	Revocation Mechanism
Proposed GRAA	ECC + Hash	Risk-Adaptive (AI-Driven)	Unlinkable	Accumulator-Based
SEMA	ECC Scalar Multiplication	No	Limited (Pseudonym)	Static
CL-PKA	ECC + Modular Exponentiation	No	Partial	Static
PBAA	Bilinear Pairing + ECC	No	Moderate	Static
GSBA	Bilinear Pairing	No	Strong	Group Revocation
CRL-SA	ECC + CRL Verification	No	Limited	CRL-Based
ML-SA	ECC + ML Inference	Partial	Limited	CRL-Based

Computational Cost Analysis: Let the benchmark cryptographic operation costs be defined as T_{mul} = 0.97 ms for elliptic curve scalar multiplication, T_{pair} = 4.50 ms for bilinear pairing, T_{exp} = 2.15 ms for modular exponentiation, and T_{hash} = 0.05 ms for hash computation, as summarized in Table 2. Based on these benchmarks, the computational cost of the proposed GRAA framework in low-risk fast mode M_1 is $T_{M1} = 2T_{mul} + 3T_{hash} = 2(0.97) + 3(0.05) = 2.09$ ms. In standard mode M_2, the cost becomes $T_{M2} = 3T_{mul} + 4T_{hash} = 3.11$ ms, while in high-assurance mode M_3, it increases to $T_{M3} = 4T_{mul} + 5T_{hash} = 4.13$ ms (see Table 3 for details).

Table 2: Cryptographic operation time and energy benchmarks.

Operation	Symbol	Time (ms)	Energy (mJ)
ECC Scalar Multiplication	T_{mul}	0.97	3.1
Hash Function	T_{hash}	0.05	0.2
Modular Exponentiation	T_{exp}	2.15	5.4
Bilinear Pairing	T_{pair}	4.50	9.8
CRL Verification Delay	T_{CRL}	1.20	1.9
ML Inference Delay	T_{ML}	1.50	2.8

Table 3: Computational cost per authentication session (per entity).

Model	Computation Formula	Total Time (ms)
Proposed GRAA–Mode M_1	$2T_{mul} + 3T_{hash}$	2.09
Proposed GRAA–Mode M_2	$3T_{mul} + 4T_{hash}$	3.11
Proposed GRAA–Mode M_3	$4T_{mul} + 5T_{hash}$	4.13
SEMA	$5T_{mul} + 4T_{hash}$	5.05
CL-PKA	$4T_{mul} + 2T_{exp}$	8.18
PBAA	$2T_{pair} + 3T_{mul} + 3T_{hash}$	12.06
GSBA	$3T_{pair} + 4T_{mul}$	17.38
CRL-SA	$5T_{mul} + 4T_{hash} + T_{CRL}$	6.25
ML-SA	$5T_{mul} + 4T_{hash} + T_{ML}$	6.55

For comparison, the computational cost of representative schemes is as follows: SEMA requires $5T_{mul} + 4T_{hash} = 5.05$ ms; CL-PKA incurs $4T_{mul} + 2T_{exp} = 8.18$ ms; PBAA requires $2T_{pair} + 3T_{mul} + 3T_{hash} = 12.06$ ms; GSBA incurs $3T_{pair} + 4T_{mul} = 17.38$ ms; CRL-SA requires $5T_{mul} + 4T_{hash} + T_{CRL} = 6.25$ ms with $T_{CRL} = 1.2$ ms; and ML-SA incurs $5T_{mul} + 4T_{hash} + T_{ML} = 6.55$ ms with $T_{ML} = 1.5$ ms.

Comparative evaluation shows that in low-risk mode M_1, the proposed framework achieves an 82.6% computational reduction compared to PBAA and an 87.9% reduction compared to GSBA. Even in high-assurance mode M_3, it maintains a 65.8% reduction relative to PBAA and a 76.2% reduction relative to GSBA. These performance improvements are illustrated in Fig. 3.

Communication Overhead Analysis: The parameter sizes adopted in the evaluation are summarized in Table 4, where an ECC point is 320 bits, a pairing element is 512 bits, a hash output is 256 bits, a timestamp occupies 64 bits, and the mode indicator requires 8 bits. Based on these parameters, the total communication cost of the proposed GRAA framework is 2440 bits in mode M_1, 2688 bits in mode M_2, and 2944 bits in mode M_3 (see Table 5 for detailed breakdown). In comparison, the communication overhead of representative authentication schemes is 3520 bits for SEMA, 4096 bits for CL-PKA, 5120 bits for PBAA, and 5632 bits for GSBA. The CRL-SA approach incurs approximately 1.2 MB of periodic broadcast overhead for 10,000 nodes, while Machine Learning-Assisted Static Authentication (ML-SA) requires 3800 bits per authentication (refer to Table 5 and Fig. 4). In low-risk mode M_1, the proposed framework achieves a 30.7% communication reduction compared to SEMA, a 52.3% reduction compared to PBAA, and a 56.7% reduction compared to GSBA, demonstrating significant bandwidth efficiency in dense smart city environments.

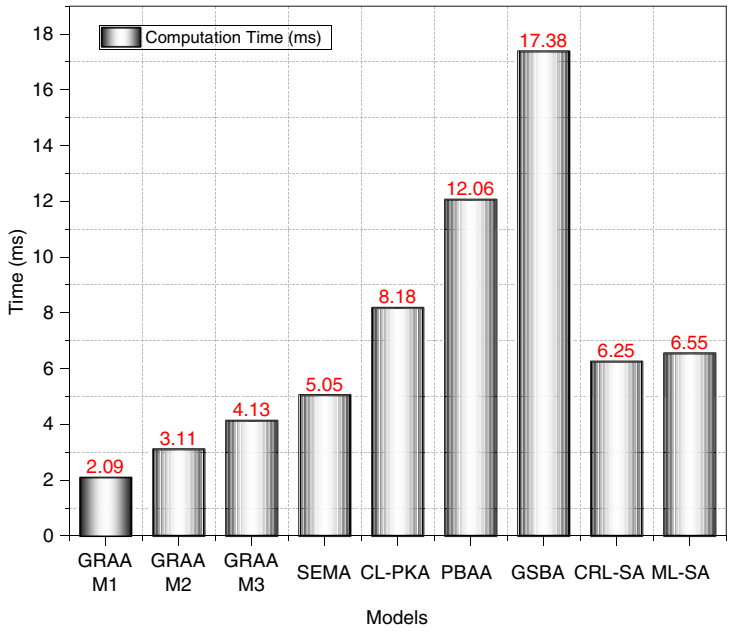

Figure 3: Computational cost comparison of authentication models.

Table 4: Parameter sizes used for communication overhead evaluation.

Parameter	Size (bits)
ECC Point	320
Pairing Element	512
Hash Output	256
Timestamp	64
Mode Indicator	8
Revocation Proof (Accumulator)	256
CRL Entry (Per Node)	120

Table 5: Communication overhead per authentication session.

Model	Total Communication (bits)
Proposed GRAA–Mode M_1	2440
Proposed GRAA–Mode M_2	2688
Proposed GRAA–Mode M_3	2944
SEMA	3520
CL-PKA	4096
PBAA	5120
GSBA	5632
ML-SA	3800
CRL-SA (10,000 nodes broadcast)	9,600,000

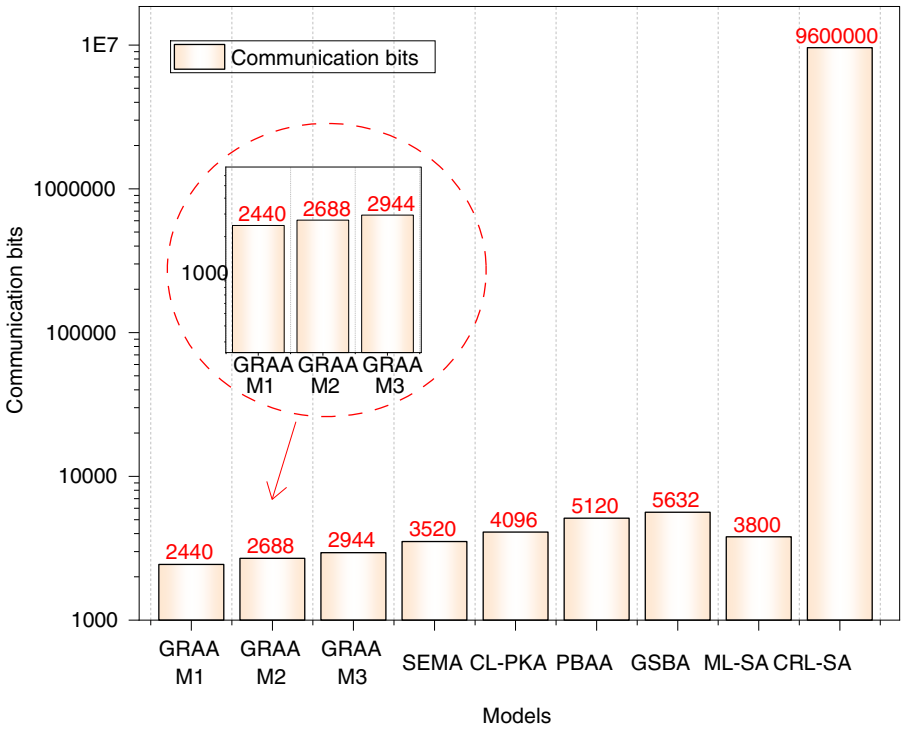

Figure 4: Communication overhead comparison.

Adaptive Latency under Smart City Density: To evaluate latency performance under varying traffic conditions, three urban density scenarios are simulated. In low-density environments (50 vehicles/km^2), where 70% of authentications operate in mode M_1, the average latency is 2.34 ms. In medium-density scenarios (150 vehicles/km^2), with 50% of sessions using mode M_2, the average latency increases moderately to 3.02 ms. Under high-density conditions (300 vehicles/km^2), where 40% of authentications activate high-assurance mode M_3, the average latency reaches 3.89 ms. For comparison, the latency of Static ECC-Based Mutual Authentication is 5.05 ms. These results indicate that the adaptive authentication framework reduces latency by up to 53.7% while maintaining security robustness. The detailed latency comparison is illustrated in Fig. 5.

Energy Consumption Analysis (UAV Perspective): Regarding UAVs, one of the most important performance metrics is energy efficiency due to the limited storage capacity of onboard batteries. The assumed power of elliptic curve scalar multiplication is 3.1 mJ, and a bilinear pairing operation is 9.8 mJ. In the given scheme, the overall energy will be about 6.8 mJ per authentication in the low-risk mode M_1. Pairing-Based Anonymous Authentication, on the other hand, needs $2(9.8) + 3(3.1) = 28.9$ mJ per session. It shows that the suggested solution achieves an energy loss of 76.5% compared with pairing-based schemes. Table 6 shows a detailed comparison of the energy.

Revocation Scalability: The revocation systems are assessed for scalability by comparing traditional CRL-based integrated static authentication with the proposed accumulator-based approach. With 10,000 nodes in a chain, an attempt to revoke all certificates through the CRL-based scheme produces a CRL, which has a size of about 1.2 MB, hence a distribution and synchronization delay of about 180 ms. However, the suggested accumulator-based revocation scheme has only a 256-bit verification-time proof per verification and has a verification complexity constant with time $\mathcal{O}(1)$. This significant reduction in

communication overhead and verification costs greatly enhances scalability in high-density smart city implementations. Fig. 6 represents the results of comparative scalability.

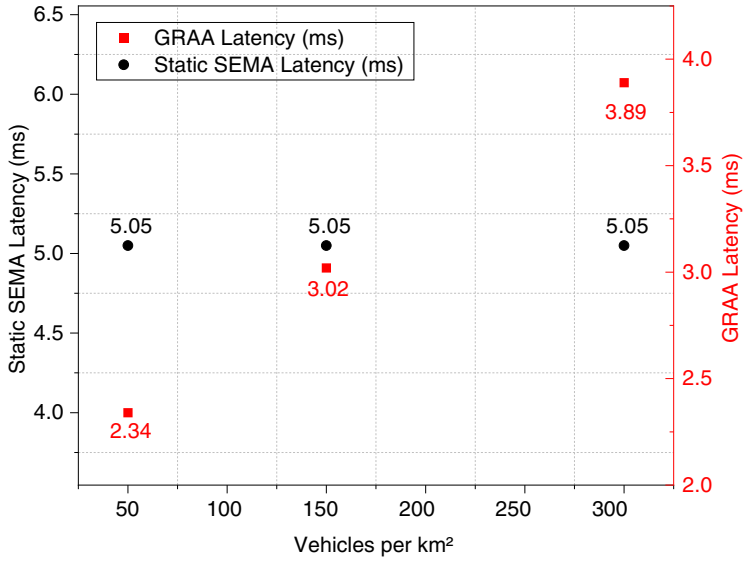

Figure 5: Adaptive authentication latency under varying traffic densities.

Table 6: Energy consumption per authentication session (UAV node).

Model	Energy Formula	Energy (mJ)
Proposed GRAA–Mode M_1	$2E_{mul} + 3E_{hash}$	6.8
Proposed GRAA–Mode M_2	$3E_{mul} + 4E_{hash}$	10.1
Proposed GRAA–Mode M_3	$4E_{mul} + 5E_{hash}$	13.4
SEMA	$5E_{mul} + 4E_{hash}$	16.3
PBAA	$2E_{pair} + 3E_{mul}$	28.9
GSBA	$3E_{pair} + 4E_{mul}$	41.8
CRL-SA	SEMA + CRL Verification	18.2
ML-SA	SEMA + ML Inference	19.1

Altogether, the proposed GRAA framework shows impressive performance gains in comparison with representative fixed authentication solutions with the maximum 87.9% decrease in the computational cost, a 56.7% reduction in the communication overhead, and a 76.5% reduction in the energy consumption, as well as lowering latency with dense traffic and scale-up revocation. The latter are obtained from analytical modeling and controlled simulations, where latency and overhead are calculated with reference to typical benchmarks for cryptographic operations and message size, and the enhancements are compared to the baseline schemes (SEMA, CL-PKA, PBAA, and GSBA) in terms of traditional reduction metrics. Moreover, AI-assisted anomaly detection and adaptive cryptographic methods can be combined to provide an efficient, proactive security scheme, which is why the suggested system is most appropriate for adaptable UAV-enabled intelligent transportation networks.

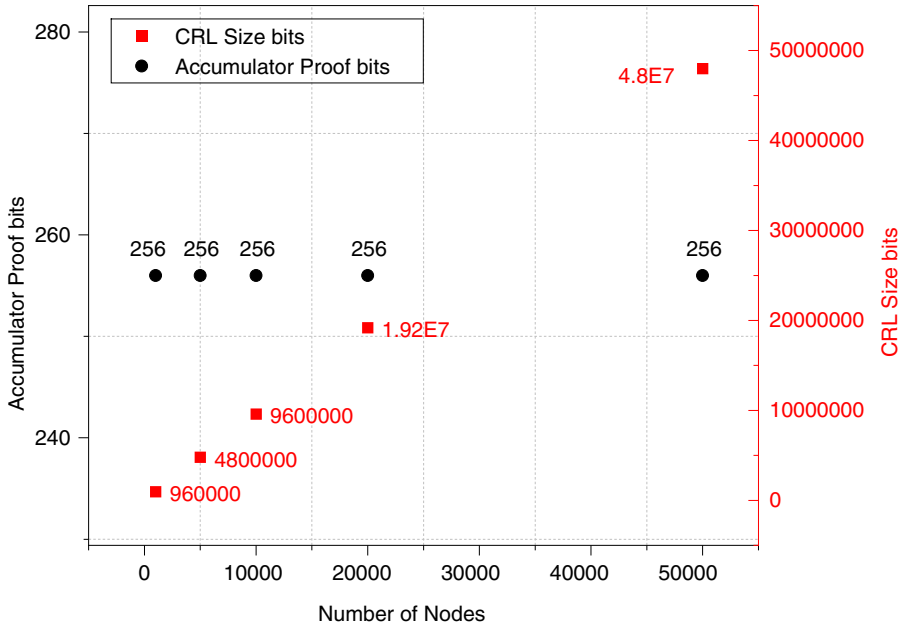

Figure 6: Revocation scalability comparison.

8 Conclusion and Future Work

The present study suggests using a GRAA model to develop UAV-assisted smart transportation systems in cities, which balances computational efficiency with security and strength with risk-affiliated authentication. The model combines AI-powered risk assessment, privacy-preserving credentials that cannot be linked to each other, and accumulator-based revocation to address resource constraints, mobility, and privacy. The ROR model provides strong security properties through formal analysis, and performance evaluation shows that the scheme outperforms other existing schemes in terms of computation, communication, and energy efficiency.

Future study will involve improved work on the framework by applying post-quantum cryptography and better methods of learning so as to enhance flexibility and protection. Also, large-scale verification through extensive simulations and practical implementation at UAV platforms and RSUs will be carried out to determine performance in real-world practice. Other areas that will be researched further include energy optimization, cross-heterogeneity within heterogeneous smart city systems, and scalable cross-domain authentication.

Acknowledgement: Not applicable.

Funding Statement: This research is supported by the Ministry of Trade, Industry and Energy and implemented by the Korea Institute for Advancement of Technology. The project includes (Development of an International Standardization and Sustainability Integration Framework for AI Industry Internalization and Global Competitiveness Enhancement (RS-2025-07372968)).

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Akmalbek Abdusalomov and Kudratjon Zohirov; methodology, Akmalbek Abdusalomov; software, Akmalbek Abdusalomov; validation, Sojida Ochilova, Jakhongir Oramov and Zafar Ruziyev; formal analysis, Malika Rustamova; investigation, Gulrukh Sherboboyeva; resources, Komil Tashev; data curation, Young Im Cho; writing—original draft preparation, Akmalbek Abdusalomov and Kudratjon Zohirov; writing—review and editing, Jakhongir Oramov, Zafar Ruziyev and Komil Tashev; visualization, Malika Rustamova and Gulrukh Sherboboyeva; 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 request from the authors.

Ethics Approval: Not applicable.

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

References

1. Zia MU, Xiang W, Huang T, Ahmad J, Chattha JN, Naqvi IH, et al. Unifying ground and air: a comprehensive review of deep learning-enabled CAVs and UAVs. Artif Intell Rev. 2026;59(1):19. doi:10.1007/s10462-025-11425-1.
2. Yang Z, Zhang Y, Zeng J, Yang Y, Jia Y, Song H, et al. AI-driven safety and security for UAVs: from machine learning to large language models. Drones. 2025;9(6):392.
3. Hashima S, Gendia A, Hatano K, Muta O, Nada MS, Mohamed EH. Next-gen UAV-satellite communications: AI innovations and future prospects. IEEE Open J Veh Technol. 2025;6:1990–2021.
4. Nam VH, Hue CTM, Anh DV. An improved reinforcement learning-based 6G UAV communication for smart cities. Comput Mater Contin. 2026;86(1):1–15. doi:10.32604/cmc.2025.070605.
5. 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.
6. Fu Y, Wang B, Zhao H, Zhou M, Li N, Gao Z. Adaptive safety attitude control of a hybrid VTOL UAV under transition flight subject to multiple faults and uncertainties. Aerosp Sci Technol. 2025;163:110284. doi:10.1016/j.ast.2025.110284.
7. Ahmad T, Morel A, Cheng N, Palaniappan K, Calyam P, Sun K, et al. Future UAV/drone systems for intelligent active surveillance and monitoring. ACM Comput Surv. 2025;58(2):1–37. doi:10.1145/3760389.
8. 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.2024.795448.
9. Zhang C, Sun G, Li J, Wu Q, Wang J, Niyato D, et al. Multi-objective aerial collaborative secure communication optimization via generative diffusion model-enabled deep reinforcement learning. IEEE Trans Mob Comput. 2024;24(4):3041–58. doi:10.1109/tmc.2024.3502685/mm1.
10. Xing X, Ma Y, Lei Y, Li Y, Xiao B. Multi-UAV rendezvous trajectory planning based on improved MADDPG algorithm in complex dynamic obstacle environments. IEEE Trans Veh Technol. 2025;75(4):5580–91. doi:10.1109/tvt.2025.3624052.
11. Xu Z, Wang K, Mu C, Qiu T. Safety-critical path planning for obstacle avoidance based on reinforcement learning and control barrier functions. IEEE Internet Things J. 2025;12(23):51410–21. doi:10.1109/jiot.2025.3614857.
12. Xu H, Wang L, Han W, Yang Y, Li J, Lu Y, et al. A survey on UAV applications in smart city management: challenges, advances, and opportunities. IEEE J Sel Top Appl Earth Obs Remote Sens. 2023;16:8982–9010. doi:10.1109/jstars.2023.3317500.
13. Yao Y, Shu F, Cheng X, Liu H, Miao P, Wu L. Automotive radar optimization design in a spectrally crowded V2I communication environment. IEEE Trans Intell Transp Syst. 2023;24(8):8253–63. doi:10.1109/tits.2023.3264507.
14. Haider ZA, Fayaz M, Zhang Y, Ali A. Advanced hyperelliptic curve-based authentication protocols for secure Internet of drones communication. ICCK Trans Adv Comput Syst. 2025;1(3):138–53. doi:10.62762/tacs.2025.926789.
15. Alshehri M, Xue T, Mujtaba G, AlQahtani Y, Almujally NA, Jalal A, et al. Integrated neural network framework for multi-object detection and recognition using UAV imagery. Front Neurorobot. 2025;19:1643011. doi:10.3389/fnbot.2025.1643011.

16. Yao Y, Xiao W, Miao P, Chen G, Yang H, Chae C, 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.
17. Eskandari M, Savkin A, Deghat M. Visual GANs for end-to-end UAV trajectory generation in RIS-assisted energy-efficient wireless vehicular networks. Green Energy Intell Transp. 2025;52(1):100365. doi:10.1016/j.geits.2025.100365.
18. Ma W, Wu J, Song D, Chen Z, Huang T. HVAE-DC: a hierarchical variational autoencoder-based deep clustering model for multi-level driving behavior. Expert Syst Appl. 2026;305:130882. doi:10.1016/j.eswa.2025.130882.
19. Hou G, Liu A, Zhao T, Wei W, Li B, Liu J, et al. Segment-conditioned latent-intent framework for cooperative multi-UAV search. Comput Mater Contin. 2026;87(1):96. doi:10.32604/cmc.2026.073202.
20. Li D, Li P, Zhao J, Liang J, Liu J, Liu G, et al. Ground-to-UAV sub-terahertz channel measurement and modeling. Opt Express. 2024;32(18):32482–94. doi:10.1364/OE.534369.
21. Li CT, Lee CC, Weng CY, Fan CI. An extended multi-server-based user authentication and key agreement scheme with user anonymity. KSII Trans Internet Inf Syst. 2013;7(1):119–31.
22. Wan P, Li H, Zhang Z, Duan C, Wang J. Motion parameter estimation of near-field drone based on DNSP under sensor position error. IEEE Wirel Commun Lett. 2026;15:1613–7. doi:10.1109/lwc.2026.3660298.
23. Xu GJW, Pan S, Sun PZH, Guo K, Park SH, Yan F, et al. Human-factors-in-aviation-loop: multimodal deep learning for pilot situation awareness analysis using gaze position and flight control data. IEEE Trans Intell Transp Syst. 2025;26(6):8065–77. doi:10.1109/tits.2025.3558085.
24. Hou Q, Yang Y, Liang J, Huo X, Leng J. A deep transfer learning approach for real-time traffic conflict prediction with trajectory data. Accid Anal Prev. 2025;214:107966.
25. Mujtaba G, Liu W, Alshehri M, AlQahtani Y, Almujally NA, Liu H. Aerial images for intelligent vehicle detection and classification via YOLOv11 and deep learner. Comput Mater Contin. 2026;86(1):1–19. doi:10.32604/cmc.2025.067895.
26. Li S, Wang S, Zhang Y, Wang X, Zhang Y, Wu W, et al. Distributed bearing-based fault-tolerant formation control of fixed-wing UAV swarm with prescribed performance. Aerosp Sci Technol. 2025;168(Pt C):110897. doi:10.1016/j.ast.2025.110897.
27. Tang X, Chen Q, Weng W, Jin C, Liu Z, Wang J, et al. Task assignment and exploration optimization for low altitude UAV rescue via generative AI enhanced multi-agent reinforcement learning. IEEE Trans Mob Comput. 2026;25(1):627–43. doi:10.1109/tmc.2025.3594188.