Revolutionising Vehicular Security: Lightweight Handover Authentication in RIS-Aided VANETs

Mahmoud A. Shawky*, Syed T. Shah†, Ahmed Gamal‡, Wali Ullah Khan§, Insaf Ullah†,
Rana Muhammad Sohaib¶, Gagangeet Singh Aujla$^\|$
* James Watt School of Engineering, University of Glasgow, Glasgow, UK
† School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK
‡ Faculty of Engineering, Alexandria University, Alexandria, Egypt
§ Interdisciplinary Centre for Security, Reliability & Trust (SnT), University of Luxembourg, Luxembourg
¶ Department of Computer and Information Science, Northumbria University, UK
$^\|$ Department of Computer Science, Durham University, UK

***Abstract*—Vehicular Ad Hoc Networks (VANETs) form the foundational communication framework of intelligent transportation systems, facilitating low-latency, vehicle-to-everything data exchange for enhanced traffic efficiency and safety. Accordingly, ensuring secure, efficient, and scalable authentication is essential to maintain communication trustworthiness, especially in highly dynamic and dense traffic scenarios. While traditional public key cryptography (PKC)-based solutions offer strong security guarantees, they are computationally intensive and struggle to scale under VANET workloads. To address these challenges, this paper proposes a novel lightweight handover authentication scheme that integrates pairing-based cryptography with symmetric key primitives to ensure message integrity, anonymity, and unlinkability. The proposed solution is deployed within a real-world Reconfigurable Intelligent Surface (RIS)-assisted communication environment, enhancing the robustness and feasibility of the authentication process during handover. Furthermore, a comprehensive evaluation is conducted, comparing the computational and communication overhead of the proposed scheme with existing cryptographic protocols. Results demonstrate the superior scalability and efficiency of the proposed approach, making it well-suited for next-generation VANET applications.**

***Index Terms*—Blockchain-assisted security, Handover authentication, Intelligent transportation systems, Reconfigurable intelligent Surfaces, VANETs**

I. Introduction

Vehicular Ad Hoc Networks (VANETs) have emerged as a critical component of intelligent transportation systems (ITS), enabling high-speed, low-latency communication among vehicles and roadside infrastructure [1]. Through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, VANETs facilitate cooperative awareness, enhance traffic safety, and support a wide range of services, including traffic management, accident avoidance, and autonomous driving. A widely adopted protocol for vehicular communication is the Dedicated Short Range Communication (DSRC) standard, operating in the 5.850–5.925 GHz frequency band, which ensures fast and reliable message dissemination in highly mobile environments [2].

Despite the benefits, VANETs face significant challenges in ensuring secure and efficient handover authentication as vehicles frequently switch connections across road segments. Traditional cryptographic techniques, while secure, often introduce high computational and communication overhead, making them difficult to scale in dense, fast-moving networks. Lightweight authentication methods are, therefore, essential, yet designing scalable solutions that do not compromise security or privacy remains an open research problem [3]. To address these challenges, this paper proposes a lightweight, scalable authentication scheme that combines bilinear pairing, ephemeral keys, and HMAC-based signatures to ensure secure message exchange with minimal computational cost. Our method is validated through real-world experimentation using a Reconfigurable Intelligent Surface (RIS)-assisted vehicular communication setup, demonstrating both security robustness and performance gains. In general, the key contributions are:

1) This paper presents a novel handover authentication scheme that ensures message integrity, anonymity, and unlinkability by leveraging pairing-based cryptography and lightweight symmetric primitives.
2) The proposed scheme is implemented and evaluated within a real-world RIS-assisted communication system to validate its practical feasibility and performance.
3) A comprehensive comparison of computational and communication costs with existing cryptographic protocols is conducted, demonstrating the scalability of the proposed approach for VANET environments.

The rest of this paper is organized as follows. Section II reviews related work in secure VANET authentication. Section III presents the proposed authentication scheme. Section IV provides a detailed performance evaluation, including experimental analysis and computational comparisons. Section V concludes the paper and outlines future research directions.

II. Background and System Modelling

A. Overview of the current state-of-the-art

Authentication is essential to securing VANETs, ensuring that only trusted participants engage in communication [4]. With the increasing vehicular density in such networks, scalable, efficient, and secure authentication mechanisms are vital. Public Key Infrastructure (PKI) is a foundational strategy wherein vehicles are equipped with multiple key pairs and certificates. Techniques such as those proposed by Raya et al. [5] enhance unlinkability by allowing vehicles to randomly select keys from a certificate pool. To bolster privacy, Conditional Privacy-Preserving Authentication (CPPA) schemes employ Elliptic Curve Cryptography (ECC), enabling secure yet lightweight signatures with pseudonyms that protect anonymity while allowing conditional identity recovery [6]. Certificate-less schemes further simplify authentication by eliminating certificate management overhead [7]. To address computational constraints, proxy-based models delegate signature verifications to capable nodes, alleviating the load on infrastructure units like roadside units (RSUs). Meanwhile, schemes based on bilinear pairings provide strong security and batch verification, albeit with increased computational cost, and are being tailored for future 6G environments [8].

Group Signature (GS) mechanisms offer anonymity and traceability by organizing RSUs into hierarchical groups for decentralized key management [9]. Approaches using regional or group-based authorities help mitigate centralized congestion, and mathematical innovations like the Chinese Remainder Theorem optimize group key distribution [10]. However, PKI-based methods face scalability issues in dense traffic conditions due to the immense volume of signature verifications, often exceeding thousands per second per unit, challenging their practicality. Consequently, Symmetric Key Cryptography (SKC) is gaining attention for lightweight authentication, offering significantly reduced computational overhead and faster processing, making it more viable for real-time, high-frequency VANET communications without compromising essential security assurances.

B. System modelling

The roles of each network entity in the proposed scheme are defined as follows.

1) *Trusted authority (TA)*: The TA is responsible for generating and managing identity-based cryptographic keys, setting up the system parameters, and maintaining security. It also creates and controls the blockchain network, ensuring that ephemeral keys are updated periodically and that only authorised entities can participate in the network. Additionally, the TA enforces network membership policies by adding or revoking entities as needed.
2) *Vehicle's on-board unit (OBU) (V_i)*: The vehicle's OBU is responsible for securely communicating with RSUs during authentication and handover. It retrieves the ephemeral public key from the blockchain network, computes its own authentication credentials, and exchanges messages with RSUs to establish secure communication sessions. The OBU also participates in message signing and verification processes to ensure the integrity of transmitted safety messages.
3) *Roadside Unit (RSU) (R_j)*: The RSU verifies the legitimacy of vehicles by handling the authentication process and establishing secure session keys. It collaborates with RIS to enhance signal reception, supports handover authentication, and integrates ML-based models for improved position verification. Additionally, the RSU acts as a bridge between vehicles and the blockchain network.
4) *Reconfigurable intelligent surface (RIS)*: The RIS is deployed in intersection areas to improve localization accuracy and enhance channel characteristics. It dynamically adjusts the phase shifts of its metasurfaces to facilitate optimal signal reception and constructive interference at designated positions. RIS also aids in secure handover authentication by assisting RSUs in position-dependent channel estimation.
5) *Blockchain network*: The blockchain network securely stores and distributes ephemeral public keys, preventing replay attacks between different sessions. Operating as a private blockchain controlled by the TA ensures that only authorised entities participate in authentication while maintaining decentralised security properties.

The system architecture of the proposed scheme is depicted in Fig. 1.

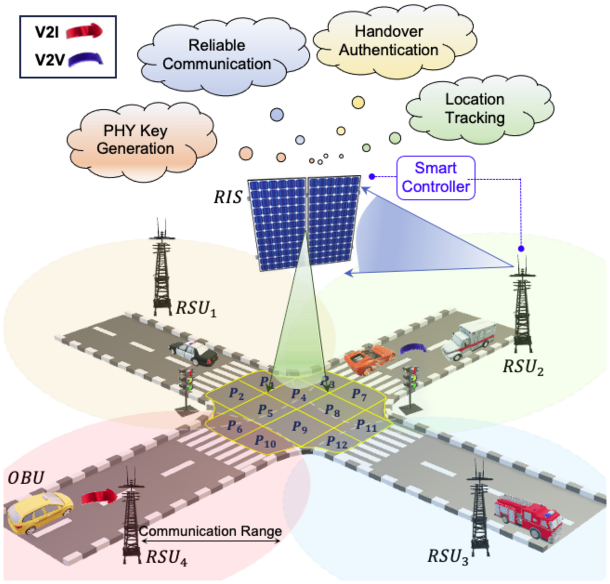

Fig. 1: System architecture of the proposed scheme.

III. The Proposed Method

This method employs an ID-based authentication approach, wherein the RSU R_j verifies the legitimacy of the communicating vehicle V_i by initiating the handshaking process. This stage consists of four distinct phases, outlined as follows.

A. The initialization phase

This phase is executed once during system setup and involves key generation, RIS configuration, and establishment of system public parameters (PPs).

Step 1 (System setup): The TA is responsible for generating and managing identity-based keys. In general, this step comprises the following processes.

1) A finite field $\mathbb{F}_q$ is generated, where q is a prime number, ensuring that addition and multiplication operations are well-defined and satisfy field properties. An elliptic curve $E(\mathbb{F}_q)$ is defined over this finite field and consists of all points (x, y) satisfying the Weierstrass equation $y^2 = x^3 + ax + b \mod p$, where $a, b \in \mathbb{F}_q$ are constants ensuring $4a^3 + 27b^2 \neq 0$ (to prevent singularities), along with a special point at infinity O.

2) Let $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing where: G_1 is an additive cyclic group of prime order q generated by P, G_2 is a multiplicative cyclic group of the same order q, e satisfies bilinearity, non-degeneracy, and efficiency.
3) A cyclic group G of points on $E(\mathbb{F}_q)$ forms an additive group under elliptic curve point addition, generated by a base point P, where each point $Q \in G$ is a multiple of P, i.e., $Q = kP$ for some integer k.
4) The TA computes the master secret key $MSK \in \mathbb{F}_q$ and its public parameter $PK_{TA} = MSK \cdot P$. Furthermore, the TA initiates a hash function $H : \{0,1\}^* \rightarrow E\left(\mathbb{F}_q\right)$ for identity-based key derivation.
5) A random ephemeral key seed generator G_{EK} for dynamic key updates. Finally, the PPs involves $\langle a, b, q, p, P, PK_{TA}, H, e(,) \rangle$.

Step 2 (RIS-assisted authentication zone configuration)**:**

1) RIS elements are strategically deployed at specific regions to cover the intersection area between RSU (RSU_j) and its adjacent RSU (RSU_{j+1}) to improve localization accuracy.
2) The intersection area is partitioned into a grid of L positions ($P_i, \forall i = \{1, \ldots, L\}$) with interspacing x distance per meter. Accordingly, each RIS unit is configured to adjust the phase shifts of its metasurfaces to ensure constructive interference at the designated position P_i.
3) The RIS's smart controller is controlled by the RSU_j and integrated with the ML-based channel mapping to support position P_i verification during handover.

B. The registration phase

This phase involves some processes to be performed by the TA for RSUs and vehicles before joining the network.

- *Step 1*: Each RSU R_j and vehicle V_i obtains a unique identity-based private key from the TA, so that $SK_{R_j} = H\left(ID_{R_j} \| MSK\right)$ and $SK_{V_i} = H\left(ID_{V_i} \| MSK\right)$, respectively.
- *Step 2*: The TA creates a blockchain network. Then, the ephemeral key generator G_{EK} is initialized with a cryptographic pseudo-random function and updated every session period T_s. Accordingly, each V_i and R_j register with a lightweight blockchain ledger to call the current ephemeral public key $G_{EK} \rightarrow PK^{EK}_{TA} \in G$, avoiding replay attacks between different sessions.
- Finally, the TA stores $\langle PPs, SK_{V_i} \rangle$ in V_i, and the same process is performed for each R_j.

It is assumed that the blockchain network operates as a private blockchain, where only the TA has the authority to add or remove entities. This enables the TA to manage network membership and revoke access in response to malicious activities.

C. The authentication phase

When a vehicle V_i enters the coverage zone of RSU RSU_j, the following steps are performed.

Step 1: V_i retrieves the current ephemeral public key PK^{EK}_{TA} from the blockchain network which is used to compute V_i's ephemeral secret key as $SK^{EK}_{V_i} = H(SK_{V_i} \cdot PK^{EK}_{TA})$. Then, V_i computes $PK^{EK}_{V_i} = SK^{EK}_{V_i}.P$

Step 2: At the beginning, V_i sends an initial authentication request to RSU_j in the form of the tuple $\langle PID_{V_i}, PK^{EK}_{V_i}, T_1, \sigma_{V_i} \rangle$, where $\sigma_{V_i} = Sign_{SK^{EK}_{V_i}}(PID_{V_i} \| PK^{EK}_{V_i} \| T_1)$.

Step 3: The RSU_j checks T_1, verifies σ_{V_i} using $PK^{EK}_{V_i}$, and computes $SK_{session} = e(SK^{EK}_{RSU_j}, PK^{EK}_{V_i})$. At last, RSU_j replies by $\langle PID_{RSU_j}, PK^{EK}_{RSU_j}, T_2, \sigma_{RSU_j} \rangle$ to V_i.

Step 4: The V_i checks T_2, verifies σ_{RSU_j} using $PK^{EK}_{RSU_j}$, and computes $SK_{session} = e(SK^{EK}_{V_i}, PK^{EK}_{RSU_j})$.

Proof of key consistency: Using the bilinearity property of e, which states that for all $A, B \in G_1$ and $x, y \in \mathbb{Z}_q$:

$$e(xA, yB) = e(A, B)^{xy}$$

We substitute $A = P, x = SK^{EK}_{V_i}, y = SK^{EK}_{RSU_j}$:

$$e\left(SK^{EK}_{V_i} \cdot P, SK^{EK}_{RSU_j}\right) = e(P, P)^{SK^{EK}_{V_i} \cdot SK^{EK}_{RSU_j}}$$

Similarly, at V_i :

$$e\left(SK^{EK}_{RSU_j} \cdot P, SK^{EK}_{V_i}\right) = e(P, P)^{SK^{EK}_{RSU_j} \cdot SK^{EK}_{V_i}}$$

Since multiplication in exponents is commutative, we conclude:

$$e(P, P)^{SK^{EK}_{V_i} \cdot SK^{EK}_{RSU_j}} = e(P, P)^{SK^{EK}_{RSU_j} \cdot SK^{EK}_{V_i}}$$

Thus, both V_i and RSU_j derive the same session key:

$$SK_{session} = e(P, P)^{SK^{EK}_{V_i} \cdot SK^{EK}_{RSUV_j}}$$

Step 5: (Message signing)**:** In this step, the session key $SK_{session}$ is used to generate a message authentication code for each safety-related message m. Consequently, the tuple $\langle m, PID_{V_i}, T_3, \sigma_{V_i} \rangle$ is transmitted from V_i to RSU_j, where $\sigma_{V_i} = HMAC_{SK_{session}}(m \| PID_{V_i} \| T_3)$.

Step 6: (Message verification)**:** The RSU_j verifies T_3, checks the validity of σ_{V_i}, and accepts m if σ_{V_i} is valid; otherwise, m is rejected.

D. RIS-assisted PHY channel handover authentication phase

This phase consists of offline and online phases, which are detailed below.

Offline stage: During this phase, the intersection region between the coverage zones of RSU_j and RSU_{j+1} is partitioned into L discrete positions, each separated by an inter-position spacing of x meters. This region is referred to as the "mapped area." The following outlines the key stages in this phase.

1) *RIS-assisted channel mapping*: This process involves the structured acquisition of channel characteristics with RIS assistance, involving the following processes.
   Step 1 (Channel probing): For each position P_l (where $l \in \{1, 2, \ldots, L\}$), the transmitter Tx located at P_l transmits pilot signals, while two receivers at RSU_j and RSU_{j+1} measure the received signal characteristics.

Step 2: The RIS units dynamically adjust their phase shifts to enhance signal reception and minimize interference at each designated position.

Step 3 (Channel estimation): This process is repeated M times per position, producing a set of channel estimates $Ch_{R_j}^{T_m}$ and $Ch_{R_{j+1}}^{T_m}, \forall m \in \{1, \ldots, M\}$, where each estimate is timestamped at T_m.

2) *Dataset formation*: The collected estimates are aggregated into a dataset representing the spatio-temporal channel characteristics across the mapped area as $DS = \left\{\left\{Ch_{R_j}^{T_1}, Ch_{R_{j+1}}^{T_1}\right\}, \ldots, \left\{Ch_{R_j}^{T_M}, Ch_{R_{j+1}}^{T_M}\right\}\right\}$. The dataset accounts for RIS configurations at each location, ensuring an optimal mapping of channel variations.

3) *Machine learning-based training*: The dataset DS is utilised to train machine learning (ML) models deployed at RSU_j and RSU_{j+1}. The ML models learn the position-dependent channel signatures to enhance the accuracy of localization and authentication.

Online stage: This phase is executed when a moving vehicle V_i is authenticated by RSU_j and is transitioning towards RSU_{j+1}. The process involves the following.

1) *Handover authentication request*: The moving vehicle V_i, positioned at a specific location P_l, initiates a handover authentication request: $\langle PP, PID_{V_i}, PK_{V_i}^{EK}, T_4, \sigma_{V_i}\rangle$, where PP is the probing packet. In parallel, the RIS controller dynamically adjusts the phase shifts to enhance the channel response at P_l, ensuring optimal reception at both RSU_j and RSU_{j+1}.

2) *Channel estimation and secure transmission*: $\hat{Ch}_{R_j}^{T_1}$ and $\hat{Ch}_{R_{j+1}}^{T_1}$ are computed at RSU_j and RSU_{j+1}, respectively. Accordingly, RSU_j securely transmits the tuple: $\langle PID_{V_i}, \hat{Ch}_{R_j}^{T_1}\rangle$ to RSU_{j+1} over a secure communication link.

3) *ML-Based Position Verification*: Upon receiving $\hat{Ch}_{R_j}^{T_1}$ from RSU_j, RSU_{j+1} utilises the trained machine learning model to process the input $\{\hat{Ch}_{R_j}^{T_1}, \hat{Ch}_{R_{j+1}}^{T_1}\}$ and predicts the estimated position $\hat{P}_l$.

4) *Binary hypothesis testing for trust delegation*: A binary hypothesis test is conducted: $\hat{P}_l \overset{?}{=} P_l$. If $\hat{P}_l = P_l$, trust is delegated, and the vehicle transitions seamlessly to RSU_{j+1}. Otherwise, the system executes crypto-based authentication, ensuring an additional security layer before allowing handover.

IV. Performance Evaluation

This section demonstrates that the proposed scheme effectively meets the security and privacy requirements of VANETs.

A. Security analysis

This subsection proves that the proposed scheme satisfies VANET security and privacy requirements.

1) *Message authentication*: The proposed scheme ensures message authentication by employing the $HMAC_{SK_{Session}}()$ process to generate the signature σ_{V_i} for each message m. Furthermore, the signature is computed based on the Bilinear Diffie-Hellman (BDH) problem, whose computational intractability ensures that an adversary cannot feasibly forge valid signatures.

2) *Unlinkability*: The unlinkability of messages is achieved by updating the ephemeral key PK_{TA}^{EK} every session period T_s. Accordingly, an adversary cannot correlate multiple messages to the same vehicle from different sessions. The infeasibility of solving the ECDLP further strengthens unlinkability by preventing the reconstruction of identity links.

3) *Resistance to active attacks*: This scheme proves to be resistant to the following attacks:

***Resistance to modification*:** The signature σ_{V_i} is generated at timestamps T_1 and T_2 using the elliptic curve digital signature algorithm (ECDSA), ensuring security against forgery due to the computational infeasibility of solving the elliptic curve discrete logarithm problem (ECDLP). Additionally, at T_3, σ_{V_i} is generated using $HMAC_{SK_{Session}}()$, which remains resistant to forgery, as deriving a valid HMAC without knowledge of the secret key $SK_{Session}$ is computationally infeasible.

***Resistance to impersonation*:** The use of bilinear pairing-based key generation ensures that only legitimate vehicles with valid private keys can generate signatures σ_{V_i} on m. An adversary cannot forge a valid tuple $\langle m, PID_{V_i}, T_3, \sigma_{V_i}\rangle$ without solving the BDH problems, which are computationally infeasible. This mitigates impersonation attacks.

***Resistance to replaying*:** Each signed message tuple includes a timestamp T_i to ensure freshness, with replay attempts mitigated by verifying whether T_i falls within a predefined time window. Also, the periodic update of PK_{TA}^{EK} every T_s enhances security by preventing adversaries from replaying messages in different sessions.

B. Experimental analysis

To validate the effectiveness of the proposed methodology, a comprehensive experimental evaluation is conducted in the Creativity Laboratory at the James Watt School of Engineering, University of Glasgow. The experimental setup comprised a reconfigurable intelligent surface with binary state control and two software-defined radio (SDR) platforms, functioning as the transmitter and receiver. The reconfigurable surface, spanning 132×132 cm^2, consisted of $4,096$ unit cells arranged in a 64×64 matrix and divided into 16 subarrays of 33×33 cm^2, each containing 256 semiconductor switching elements. These elements are controlled via 16-bit LED drivers in a serial daisy-chain configuration and are mounted on a 142×142 cm^2 polycarbonate substrate, reinforced with an aluminum frame for structural stability. Dynamic control of the electromagnetic surface is facilitated through five interface lines per subarray, enabling precise voltage regulation and data transmission. The control system is powered by a Raspberry Pi $3B+$, which manages dual SPI connections

(SPI0 and SPI1) operating at 7.8 MHz. A MATLAB-based control algorithm running on a host PC communicated with the RIS via a wireless link, with the Raspberry Pi acting as an access point for command execution. The transmission system utilised a directive antenna with an 80 beamwidth in both the azimuth (E-plane) and elevation (H-plane), while the receiver implemented a single-input multiple-output (SIMO) configuration using two antennas. For precise localisation, broadband log-periodic directional antennas are employed, covering a frequency range of $1.35 - 9.5$ GHz, offering a gain of $5 - 6$ dB and a reflection coefficient below 2.5.

The communication framework is based on orthogonal frequency-division multiplexing (OFDM) with 256 subcarriers, a cyclic prefix length of 64 samples, a carrier frequency of 3.75 GHz, and a sampling rate of 200 kHz. The OFDM frame, designed using LabVIEW, allocated 105 subcarriers for zero-padding, 26 for channel estimation and equalisation, 125 for channel probing, and 64 for cyclic extension. A CBX-120 USRP daughterboard is used to enable high-bandwidth processing, supporting an operational bandwidth of 120 MHz. The experimental campaign involved nine distinct receiver positions ($T = 9$), with inter-position spacings of 1 m. The transmitter is placed 3 m from the RIS midpoint, while the initial receiver (P_1) is positioned 5 m away. The transmitter antenna is aligned perpendicularly to the RIS plane ($\theta_{incident} = 90°$), while the receiver antenna is oriented at $\theta_{reflection} = 135°$. Both antennas are mounted at 126 cm to ensure optimal signal reflection and reception.

TABLE I: Performance evaluation of machine learning models under RIS activation conditions.

Algorithm	**Accuracy (%)**	**Loss**
Directive Antennas, $x = 1$ m Distance, RIS Activated		
Gradient Boosted Trees	81.9 ± 1.6	0.49 ± 0.04
Naïve Bayes	67 ± 0.4	7 ± 0.3
Random Forest	72 ± 0.4	0.7 ± 0.4
Support Vector Machine	81 ± 0.9	0.6 ± 0.06
Logistic Regression	78 ± 1.6	0.7 ± 0.04
Neural Network	27 ± 1.9	13 ± 0.6
Decision Tree	64 ± 2	0.6 ± 0.04
Class Distributions	65 ± 2	1.9 ± 0.06
Nearest Neighbors	62 ± 0.9	1.2 ± 0.01

Table I presents the classification performance of various machine learning algorithms under active RIS conditions with directive antennas and a receiver placed 1 meter away. Among all models tested, Gradient Boosted Trees and Support Vector Machine (SVM) demonstrated the highest accuracy, at 81.9% and 81% respectively, with relatively low loss values (0.49 and 0.6), indicating strong predictive reliability. Logistic Regression also performed well, achieving 78% accuracy, slightly below the top performers. In contrast, Neural Networks showed notably poor performance with only 27% accuracy and the highest loss (13), suggesting possible overfitting or inadequate training under the current experimental setup. Simpler models like Naïve Bayes and Nearest Neighbors also underperformed, achieving accuracies below 70%, with comparatively higher losses. Overall, the results indicate that ensemble methods (like Gradient Boosted Trees and Random Forests) and margin-based classifiers (like SVM) are more effective in capturing the signal behavior influenced by the RIS, while more basic or overly complex models struggle to generalize well in this setting.

Moreover, the performance of Gradient Boosted Trees under different RIS conditions highlights the significant impact of RIS activation on classification accuracy. When the RIS is off, the model achieves an accuracy of 62 ± 2% with a loss of 1 ± 0.04, indicating a limited ability to distinguish between classes in the absence of surface-induced enhancements. In contrast, with the RIS activated, accuracy improves markedly to 81.9 ± 1.6%, and loss drops to 0.49 ± 0.04, demonstrating a substantial gain in model performance. This clear improvement underscores the effectiveness of the RIS in shaping the wireless channel to enhance signal characteristics, making it easier for machine learning models to identify patterns and make accurate predictions.

C. Computation and communication comparisons

For a comprehensive comparison, we used the average execution times for various cryptographic operations measured per milliseconds in [11], using the MIRACL cryptographic library [12] on a quad-core i7 system with 16GB of RAM. The results show that bilinear pairing operations (T^{bp}) in group $\mathbb{G}_1$ are the most computationally intensive, averaging 13.44 ms, which is significantly higher than all other operations. This is followed by scalar multiplication in the same group (T^{sm}_{bp}) at 2.521 ms, and in the elliptic curve group $\mathbb{G}$ (T^{sm}_{ecc}) at 1.489 ms, highlighting the high cost of elliptic curve scalar multiplication operations. Point addition operations are much less demanding, taking $0.018 ms$ in $\mathbb{G}_1$ (T^{pa}_{bp}) and 0.008 ms in $\mathbb{G}$ (T^{pa}_{ecc}). Meanwhile, lightweight operations such as hashing with SHA-256 (T_h) and AES encryption/decryption (T^{enc}_{AES}, T^{dec}_{AES}) exhibit minimal overhead, with execution times of 0.003 ms, 0.002 ms, and 0.001 ms, respectively.

TABLE II: Computation and communication comparisons

Scheme	**Verification cost ($msec$)**	**Transmission cost**
[13]	$(3n+2)T^{sm}_{bp} + (3n)T^{pa}_{bp}$ $+(n)T_h \approx 2.978 + 4.494(n)$	$408(n)\ bytes$
[14]	$(2n+2)T^{sm}_{ecc} + (2n+1)T^{pa}_{ecc}$ $+(3n)T_h \approx 2.986 + 3(n)$	$208(n)\ bytes$
Ours	$(T^{sm}_{ecc} + T^{pa}_{ecc} + T^{bp})$ $+(n)(T_h + T^{dec}_{AES}) \approx 14.9 + 0.004(n)$	$156 + 68(n)\ bytes$

Table II presents a comparative analysis of the computation and communication costs associated with verifying and transmitting n digital signatures across three different cryptographic schemes: those proposed in [13], [14], and the scheme introduced in this work (denoted as "Ours"). In terms of verification cost, the scheme in [13] incurs a high computational burden due to its reliance on pairing-based operations, requiring $(3n + 2)$ scalar multiplications and $(3n)$ point additions in group $\mathbb{G}_1$, plus n hash operations. This translates to a total verification time of approximately 2.978+4.494n milliseconds, which scales steeply with the number of signatures.

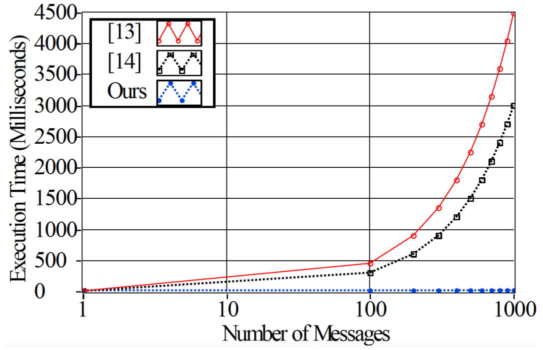

Fig. 2: The computation overhead of verifying n signatures.

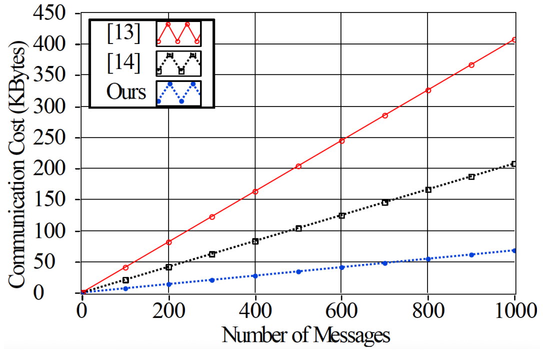

Fig. 3: The communication overhead of sending n safety-related messages.

The scheme in [14], based on elliptic curve operations in group $\mathbb{G}$, offers improved efficiency, requiring $(2n + 2)$ scalar multiplications, $(2n + 1)$ point additions, and $3n$ hash operations, resulting in a verification time of around $2.986{+}3n$ $msec$. While still linear in n, this method avoids the costlier pairing operations. The proposed scheme demonstrates superior computational efficiency, with a constant-time base cost of one elliptic curve scalar multiplication, one point addition, and a single bilinear pairing—independent of n. The only linear component is the combined cost of n hash and AES decryption operations, yielding a total time of approximately $14.9{+}0.004n$ milliseconds, which scales much more favorably for larger n, see Fig. 2. In terms of communication cost, the proposed scheme also shows clear advantages. While the schemes in [13] and [14] incur linear transmission costs of $408n$ and $208n$ bytes respectively, the proposed method requires only $156{+}68n$ bytes, offering substantial bandwidth savings, particularly for small to moderate n, see Fig. 3. Overall, this comparison highlights the efficiency of the proposed scheme in both computation and communication, making it highly suitable for resource-constrained environments or large-scale signature verification scenarios.

V. Conclusions

This paper introduces a secure, privacy-preserving handover authentication scheme for VANETs using bilinear pairing, ephemeral keys, and HMAC-based signatures to achieve message authentication, unlinkability, and resistance to active attacks. Real-world validation using a RIS-assisted communication setup confirms the system's effectiveness, with RIS activation significantly enhancing signal characteristics. Gradient Boosted Trees achieved over 81% classification accuracy, outperforming other models, especially under RIS conditions. Computational and communication cost analysis shows the proposed scheme outperforms existing methods with lower verification time and reduced transmission overhead, making it ideal for real-time, resource-constrained vehicular networks. Future work includes supporting dynamic mobility and multi-hop communication, incorporating adaptive RIS control for real-time beamforming, and employing federated learning for privacy-preserving model training. Further testing in urban settings and adversarial conditions will assess the scheme's robustness and scalability.

Acknowledgment

This work was supported by the Engineering and Physical Sciences Research Council for project CHEDDAR: Communications Hub For Empowering Distributed ClouD Computing Applications And Research [Grant number EP/X040518/1].

References

[1] M.A. Shawky, S. T. Shah, M. Usman, M. Abdrabou, Q.H. Abbasi, D. Flynn, M.A. Imran, S. Ansari, and A. Taha, "How secure are our roads? An in-depth review of authentication in vehicular communications", *Vehicular Communications*, p.100784, 2024.

[2] M.A. Shawky, S.T. Shah, Q.H. Abbasi, M. Hussein, M.A. Imran, S.F. Hasan, S. Ansari, A. Taha, "RIS-Enabled Secret Key Generation for Secured Vehicular Communication in the Presence of Denial-of-Service Attacks", *Sensors*, vol. 23, no. 8, Apr. 2023.

[3] M.A. Shawky, M. Usman, M.A. Imran et al., "Adaptive Chaotic Map-based Key Extraction for Efficient Cross-Layer Authentication in VANETs", *Vehicular Communications*, vol. 39, Feb. 2023.

[4] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A Privacy-Preserving Trust Model Based on Blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, Aug. 2018.

[5] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing Vehicular Communications," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[6] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, and P. Lorenz, "On the Design of Conditional Privacy Preserving Batch Verification-Based Authentication Scheme for Internet of Vehicles Deployment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5535–5548, May 2020.

[7] H. Tan and I. Chung, "Secure Authentication and Key Management With Blockchain in VANETs," *IEEE Access*, vol. 8, pp. 2482–2498, Jan. 2020.

[8] M. R. Asaar, M. Salmasizadeh, W. Susilo, and A. Ajidi, "A Secure and Efficient Authentication Technique for Vehicular Ad-hoc Networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, Apr. 2018.

[9] M. Azees, P. Vijayakumar, and L. J. Deborah, "EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, pp. 2467–2476, Feb. 2017.

[10] Y. Jiang, S. Ge, and X. Shen, "AAAS: An Anonymous Authentication Scheme Based on Group Signature in VANETs," *IEEE Access*, vol. 8, May 2020.

[11] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of Blockchain-Based Lightweight V2I Handover Authentication Protocol for VANET", *IEEE Trans. on Net. Sci. and Eng.*, vol. 9, no. 3, Jun. 2022.

[12] MIRACL Crypto Library: Multiprecision Integer and Rational Arithmetic C/C++ Library. Available: https://github.com/miracl/MIRACL.

[13] J. Li, Y. Ji, K. -K. R. Choo, and D. Hogrefe, "CL-CPPA: Certificate-Less Conditional Privacy-Preserving Authentication Protocol for the Internet of Vehicles", *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10332-10343, Dec. 2019.

[14] Y. Ming, and H. Cheng, "Efficient Certificateless Conditional Privacy-Preserving Authentication Scheme in VANETs", *Mobile Information Systems* (Hindawi), Feb. 2019.