



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

The Secure Authenticated Key Agreement Protocol for VANETs Based On ECC

Neha Sharma^{1,*}, Nilesh Jain², Pratik Gupta³

¹Department of Mathematics, Mandsaur University, Mandsaur, India. E-mail: vats1993neha@gmail.com;

²Department of Computer Science and Applications, Mandsaur University, Mandsaur, India. E-mail: Nileshjainmca@gmail.com

³Department of Mathematics, D.A.V. Degree College, Lucknow, India. E-mail: Pratikgupta1810@gmail.com

ABSTRACT

Vehicle-ad-hoc networks (VANETs) have emerged as a prominent area of study within the intelligent transportation system (ITS) domain. This network has grown to be the most well-liked and pertinent for ITS during the past few years. High-end cars are now anticipated to improve storage capacity and onboard performance. To improve ITS, several VANET architectures have been suggested. But after the transportation system and cloud computing were combined, VANET technology underwent a new revolution. However, all ITS communication over the public network faces numerous security challenges. To handle latency with high traffic load across a public channel, vehicle, and onboard unit security. For VANET, we have created an intelligent transportation authentication solution that is both efficient and privacy-focused. With the random oracle model, security and accuracy are shown. A performance comparison reveals that it satisfies the need for reduced computation and communication overhead.

Keywords: Vehicular ad hoc networks, Authentication, Security, Privacy, NS3 Simulator

1. Introduction

Vehicle Ad-Hoc Networks (VANETs) are a particular kind of Mobile Ad-Hoc Network (MANET) that are intended to facilitate communication between automobiles and roadside infrastructure. VANETs are an essential part of Intelligent Transportation Systems (ITS), which use real-time communication to enhance driving experience, efficiency, and traffic safety. An ad hoc network that facilitates communication with mobile entities is called a VANET. No stable infrastructure is in place for the concerned entity. When developing intelligent transportation (IT) systems, mobility, entertainment, privacy, security, and safety are important priorities due to fundamental user needs for the switch service. Intelligent Transportation Systems (ITS) combine modern technology into transportation infrastructure and vehicles to improve traffic management, enhance safety, reduce congestion, and provide more efficient and dependable transportation services. Applications that gather, process, and distribute data to improve the effectiveness and efficiency of transportation systems are included in the broad category of Intelligent Transportation Systems (ITS). Here, select the appropriate financing source. Remove this if there are none. Vehicular Adhoc Networks are the most important IT system direction (VANETs). VANETs are used to provide consumers with a wide range of comfortable and adaptable services. Vehicles with wireless communication capabilities operate VANETs. Through range-restricted communications via Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) open message transmission, all participating vehicles communicate with one another and work together. Intelligent Transportation Systems (ITS) rely on Vehicle-to-Infrastructure (V2I) connectivity to allow vehicles to interface with roadside infrastructure and centralized management systems. Real-time data and information transmission is made possible by this communication, improving safety, efficiency of transportation overall, and traffic management. Typically, inductive loops such as cameras and roadside sensors collect all of the data on traffic on the roads. The new phase of real-time information acquisition from vehicle onboard equipment is made possible by VANETs. It is possible to incorporate all of the data that VANETs have enabled in individual vehicles to simulate a real-time road environment. Vehicle-to-Vehicle (V2V) open message transmission is the name of the communication protocol and system that allows cars to communicate openly and interoperability with one another directly. Intelligent Transportation Systems (ITS) and connected vehicle technology depend on this connectivity to share data in real-time for a variety of applications, including cooperative driving, traffic management, and safety. In recent years, several new applications have embraced VANET technology to improve safety and efficiency in transportation. There are some security risks for VANETs because of open

wireless connection, and they are not insignificant. The notable communication speed of VANET sets it apart from other transdisciplinary networks. As a result, VANET security issues and threats differ greatly from those of other networks. Vehicles in VANET travel at extremely high speeds along predetermined routes, and because of their rapid speed, they only make connections for brief periods. But communication will suffer as a result. Figure 1. A succinct example of a structured model because of its great mobility and quickness. Subsequently, other methods were proposed to address problems with VANET systems. Then vehicular cloud-based strategy is built as the partial solution of the traffic management system. It is a hybrid invention that uses adjustable assets to split traffic onboard units remarkably. There are two distinct partitions designed by the intelligent traffic management system to control the equipment through programming, and there are three types of vehicular networks: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-sensors (V2S). Any two vehicles can communicate with one another in V2V by utilizing every onboard unit (OBU). Roadside units (RSUs) are in communication with vehicles to gather information on congestion. Using sensor devices, this system gathers and disseminates vehicle information. Cloud-centric infrastructure for vehicles operates on a portable hub concept that enables interaction with an external environment. For transportation management, ad hoc network inclusion and vehicular cloud are therefore linked to an intelligent transport system.

2. Related Work

We have reviewed earlier works in the field of intelligent transport and the environment of VANETs. To improve security and latency, we have seen that a lot of articles from the past several years have focused on improving the architecture of intelligent transportation systems in other domains. An overview of the vehicular ad-hoc network for specialized short-distance vehicles was provided by Yin et al. [19]. They created a VANET application for automotive crash resistance. Applications of technology and systems intended to improve vehicle safety and lower the chance of crashes are referred to as vehicle collision resistance applications. These apps use a variety of sensors, communication tools, and clever algorithms to identify possible collisions, alert drivers, and sometimes even take independent action to prevent or lessen the effects of incidents. There are two ways that communication occurs in VANETs to prevent collisions [5]. In this way, a car can connect with the roadside equipment and communicate directly with other vehicles. Jiang et al. [10] are concerned about vehicle communication safety. They enforced a new requirement of wireless communication networks for a vehicle environment. However, it suffers from a weak wireless network's lengthy setup of connectivity and time delays. Robinson et al. [18] proposed a new information-sharing phase that would include both safety and non-safety information. The most important information to provide to the driver of a vehicle is safety information, such as speed warnings, pedestrian crossings, road damage warnings, accident warnings, etc., so they can be informed of potential dangers and prevent accidents. Future transportation systems face obstacles, as noted by Jakubiak et al. [9]. They examined the non-safety information technology, which ensures the efficiency, security, and comfort of the user and service provider by recommending the nearest hospital, nearest fire station, closest gas station, etc. But the user's safety has to come first when it comes to no-safety vehicle systems. The first authentication key management plan for VANETs was introduced by Hao et al. [8]. They assert to be able to stop a variety of known attacks against the VANET system. Regretfully, to ensure security, they had to jeopardize system functions including traceability, availability, confidentiality, and the integrity of car service users. An enhanced dynamic location-based key agreement system for VANETs was presented by Lu et al. [15]. They established secure sessions while maintaining the privacy of the location-based car services. Lu's suggested protocol was under threat from a passive adversary. The issue of consistent VANET service access over the web environment was brought up by Lin et al. [12]. They advised employing a gateway as a service (GaaS) that is hosted in the cloud. To improve internet use for experiencing vehicular systems and to offer efficient door availability, the suggested architecture consists of an emergency response vehicle, a cloud server, and a customer car. The car that is mobile must obtain information via the internet and send requests to the GaaS. However, a multi-authority-based strategy for appropriate storage was not possible. Jianhong [11] improved and introduced a group testing user verification mechanism for VANET. It made a formal security analysis-based security claim. During session verification, impersonation attacks could be launched against this method. Lo and Tsai [14], who asserted to have created a safe identity-based authentication system for vehicles, designed an effective transportation system. However, it was unable to endure insider threats and unlikability. A VANET authentication system proposed by Bayat et al. [4] showed batch verification of each registered car but was unable to withstand revocation of user verification. Another model for an intelligent transportation system was presented by Olariu et al. [17]. It converts vehicular networks into vehicular cloud networks, which can use vehicular assets to frame a cloud by gathering vehicular information. Because this technique's suggested framework avoided taking advantage of the usual cloud, it was much more vital for a vehicle system. A system known as the CROWN framework was presented by Cui et al.

[6] in 2018. It is dependent on certain infrastructures, such as RSUs, that function as cloud registries and between countenances. This plan would require support rights, but occasionally infrastructure failure would prevent users from interacting with the cloud server. RSUs made their gathered data available in 2018 [13], enabling cars to locate their vehicular cloud and utilize its advantages within the RSU-secured area. The installed PC was not seen by the CROWN framework as a vehicle cloud computing component that users could access, aside from the RSU infrastructure. Ahmed et al. [1] suggested the appropriate use of vehicle cloud computing administration by way of RSUs in their 2019 paper on providing security and protection of administrations in vehicular computing. A plan has been proposed by engineers to allow cars to benefit from open vehicular cloud services in roadside scenarios within the vehicular cloud. The previous methods can be categorized as supporting frameworks for cars to access the standard vehicular cloud utilizing certain RSUs using an appropriate entrance to locate a specified server administration without the need for any mobile registration assets. However, this approach has very good computational efficiency. In the current context, the security of Ahmed et al.'s approach is weak. For data sharing in automotive networks, Qin et al. [20] described an ECC-based access control mechanism with conditional authentication and lightweight decryption. For vehicle-to-vehicle communication in VANETs, Ali et al. [21] described an effective and demonstrably safe conditional privacy-preserving authentication based on ECC. For industrial control systems, Chen et al. [22] described an authenticated key agreement mechanism based on ECC. For automotive ad hoc networks, Dwivedi et al. [23] designed a strong and effective batch authentication mechanism based on blockchain and ECC. A Novel Cloud-Assisted Authentication Key Agreement Protocol for VANET was described by Zhou et al. [24].

3. MOTIVATION AND CONTRIBUTION

For improved road safety and management in vehicular networks, latency, scalability, efficiency, dependability, and security are critical. This allows all users to utilize the vehicular transportation service with great comfort and confidence. Vehicle ad hoc networks already provide users with sophisticated digital transit options. A proper atmosphere and acceptable cost efficiency are prerequisites for VANET users to get digital transportation services. For the past few years, scientists have been working to create an appropriate VANET design. Regretfully, a general VANET model has not yet been implemented to support the computing and communication needs of the vehicle user. Additionally, there are a few serious security risks with the current VANET models. The suggested VANET content key delivery infrastructure for the transportation context aims to address user-centric challenges. The suggested approach enhances performance and privacy by using ECC operations. On the other hand, some computationally demanding operations are calculated offline. The adoption of a content key establishment process results in increased security and efficiency can improve security while providing dependable communication overhead and extremely efficient computing. Additionally, mutual authentication is supported. The paper's noteworthy contribution can be summed up as follows:

- a. The suggested architecture creates an authentication link for VANET transportation services between a vehicle and the server.
- b. The random oracle model is used to illustrate the security of the suggested protocol.
- c. The NS3 environment is used to simulate the suggested design.
- d. The suggested approach is safe from a variety of security threats, according to a formal security review.
- e. To verify a few of the suggested scheme's flaws, we utilize AVISPA.

4. PRELIMINARIES

A collection of all pairs (x, y) that belong to Z_p and satisfy the equation $y^2 \equiv x^3 + ax + b \pmod{p}$ plus an imaginary point known as infinity (O) constitute an elliptic curve over Z_p where $p > 3$. Z_p has the values a and b and $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ needs to be met. The curve is implied to have no singularities by the term "elliptic curve." Geometrically speaking, this means that the curve's discriminant, $-16(4a^3 + 27b^2)$, cannot equal zero, ensuring that the plot has no vertices or crosses over itself. For cryptography purposes, it is necessary to analyze the curve in a prime field, as defined. Nevertheless, the result does not resemble a curve when we plot the curve over Z_p . That being said, there is no prohibition on charting an elliptic curve equation over real values. For addition and scalar multiplication, the elliptic curve groups, represented by the letter G, work as follows:

$$[x_3, y_3] = \left[\left(\lambda^2 - x_1 - x_2 \pmod{q} \right), \left(\lambda(x_1 - x_2) - y_1 \pmod{q} \right) \right]$$

$$P + Q = (x_3, y_3) \quad (1)$$

$$(x_3, y_3) = (\lambda^2 - x_1 - x_2 \pmod{q}, (\lambda(x_1 - x_2) - y_1) \pmod{q}) \quad (2)$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod{q} \text{ if } P \neq Q \quad (3)$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \pmod{q} \text{ if } P = Q \quad (4)$$

4.1. Discrete Logarithm Problem with Elliptic Curves (ECDLP)

In the Elliptic Curve Diffie-Hellman Problem (ECDHP), it is difficult to compute abg for group G given the generator g , values a , and b . Elliptic Curve Cryptography (ECC) outperforms other cryptographic protocols such as RSA, DSA, and Diffie-Hellman in terms of key sizes, which affects the systems' bandwidth and performance. The ECDLP deals with an elliptic curve E that is supplied. The task is to find an integer d such that $(1 \leq d < \#E)$ is the number of points on the curve and T is another element on the curve. The primitive P added to itself d times equals T .

$$T = dP = P + P + \dots + P + P \text{ (} d \text{ times)} \quad (5)$$

Within the realm of cryptography, the public key T is represented by a point on the curve with coordinates (x_T, y_T) , and the private key d is regarded as an integer. The ECDLP is not the same as the discrete logarithm problem for Z_p^* , where both keys are integers. Point multiplication, or $T = dP$, is not the true multiplication of an integer d and a curve point P ; rather, it is merely a notation for repeatedly applying the group operation $(y^2 \equiv x^3 + ax + b \pmod{p})$. The hardness of the ECDLP is crucial for the security of all elliptic curve systems.

5. PROPOSED SCHEMES

To provide an authentication mechanism for VCC that is relevant to knowledgeable users, we developed a lightweight authentication framework.

5.1. User Registration Phase

To provide an authentication mechanism for VCC that is relevant to knowledgeable users, we developed a lightweight authentication framework. When using the system for the first time or after the registration period has ended, the user must enter ID_u and PW_{U_i} . After U_i inputs ID_u , PW_{U_i} , and biometrics ω , it uses a generation process called $Gen(\omega)$ to extract uniform randomness R and helper string alpha from the scanned biological feature omega, i.e., $Gen(\omega) \rightarrow (R, \alpha)$. Then, via a registration request, U_i sends data to the server.

a. U_i enters his identity ID_{U_i} , password PW_{U_i} and imprints ω , and performs $Gen(\omega) = (R, \alpha)$.

Finally, U_i calculates $G_u = h(ID_{U_i} \oplus PW_{U_i} \oplus R)$ and transmits $\langle ID_u, G_u \rangle$ to LS_j as a registration request through a secure channel.

b. CS_j checks ID_{U_i} , choose a $x \leftarrow Z_q^*$ as master secret key and $\langle P \rangle$ as generator of a group G . Further, computes $X = x \cdot P$, and then select a secret key $s \leftarrow Z_q^*$ with respect to identity ID_{U_i} .

c. After that, computes $Z = h(ID_{U_i} \parallel (x + s)P)$ and $G_w = Z \oplus G_w$. CS_j stores (s, ID_{U_i}) . Finally, CS_j uses the secure channel to communicate $\langle X, G_u, h(\bullet) \rangle$ to U_i .

d. U_i computes $Z = G_u \oplus G_w$, $Q_u = h(Z \parallel PW_{U_i} \parallel R \parallel ID_{U_i})$ upon getting $\langle X, G_u, h(\bullet) \rangle$. After that U_i stores $\langle Q_u, X, G_w \rangle$, in the device.

5.2. Login and Authentication Phases

If U_i wants to connect to a vehicle digitally, U_i will need the session key and U_i must show an authenticated session with CS_j . The CS_j provides the session key $K_{ID_{VC}}$ after the U_i identification is validated. Figure (2) presents an overview of the proposed key distribution and the precise stages are as follows:

- a. U_i enters his identity ID_{U_i} , password PW_{U_i} and imprints ω in smart vehicular. Verify if Q_u and Q_u^* are equal or not, then the device reader computes $G_u = h(PW_{U_i} \parallel ID_{U_i} \parallel R)$, $Z = G_u \oplus G_w$ then check if $Q_u^* = h(PW_{U_i} \parallel Z \parallel ID_{U_i} \parallel R)$, $Q_{U_i}^* = ? Q_{U_i}$ if holds, then the device reader computes further, otherwise terminate the request.
- b. U_i generate a random number $a \leftarrow Z_q^*$ and timestamp T_i after successfully login. Then compute $A_1 = a \cdot P$, $A_2 = a \cdot X$, $A_3 = ID_{U_i} \oplus h(A_2)$, $VID_u = ID_{VC} \oplus h(A_2 \oplus ID_{U_i} \oplus Z \oplus T_i)$, $G_v = h(ID_{U_i} \parallel A_1 \parallel A_2 \parallel A_3 \parallel ID_{VC} \parallel T_i)$ and sends $\langle VID_u, A_1, A_3, G_v, T_i \rangle$ to the CS_j through public channel.
- c. At first CS_j check the timestamp upon getting $\langle VID_u, A_1, A_3, G_v, T_i \rangle$ from U_i by checking whether $|T_j - T_i| < \Delta T$, where ΔT represents the maximum threshold delay. If the condition is satisfied, CS_j computes $A_2 = x \cdot A_1$ then retrieve $ID_{U_i} = A_3 \oplus h(A_2)$ and then select the corresponding secret key s . Computes $Z = h(ID_{U_i} \parallel (x + s))$ and $ID_{VC} = VID_u \oplus h(A_2 \oplus ID_{U_i} \oplus Z \oplus T_i)$. Verify wheatear, $G_v' = h(ID_{U_i} \parallel A_1 \parallel A_2 \parallel A_3 \parallel ID_{VC} \parallel T_i)$. If $G_v' = ? G_v$ then CS_j compute further otherwise terminate the session. LS_j search $K_{ID_{VC}}$ and generates current time stamp T_k . Further, Computes $A_4 = K_{ID_{VC}} \oplus h(A_2 \parallel ID_{VC} \parallel A_1 \parallel T_k)$, $A_5 = h(ID_{U_i} \parallel A_2 \parallel T_i \parallel T_k K_{ID_{VC}})$. Then CS_j sends $\langle T_k, A_4, A_5 \rangle$ to U_i via public channel.
- d. Now, U_i check the time stamp upon receiving $\langle T_k, A_4, A_5 \rangle$ from CS_j by checking whether $|T_j - T_i| < \Delta T$. After that, U_i computes $K_{ID_{VC}} = A_4 \oplus h(A_2 \parallel ID_{VC} \parallel A_1 \parallel T_k)$, $A_5' = h(ID_{U_i} \parallel A_2 \parallel T_i \parallel T_k K_{ID_{VC}})$. For verification check whether $G_2' = ? G_2$. After successful verification, the user saves the key $K_{ID_{VC}}$; otherwise, the session will be terminated.

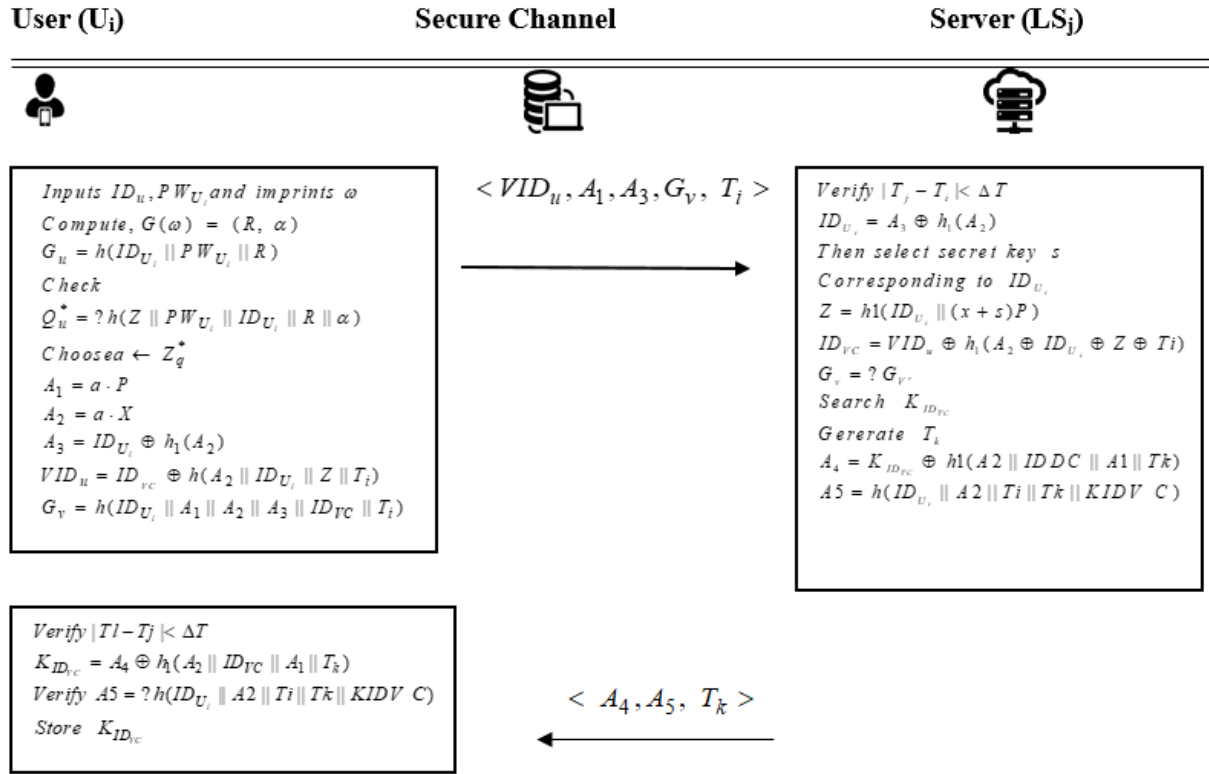


Fig. 2. Authentication and Key Distribution Phase

6. SECURITY PROOF

In this section, the proposed scheme is constructed using a random oracle model, which first introduces the security model and then the proposed scheme.

6.1. Security Model

Let $U_i \in (U, S)$ represents the i th user and a PPT adversary $\mathfrak{S}_{Ad}$ be in control of messaging between U_i and LS_j . The following is the specification of $\mathfrak{S}_{Ad}$:

- Extract:** This query can be used by $ImAd$ to get the secret key associated with the user's unique identity.
- Send (M, U_i) :** $\mathfrak{S}_{Ad}$ transmits a random message to the oracle in this query model. Oracle then transmits our computational output back to $\mathfrak{S}_{Ad}$. **Hash(m):** Initially, $\mathfrak{S}_{Ad}$ transmits message m for hash query to $H(\cdot)$. Oracle then returns $s \in Z_p^*$ as random output and $save(m, s)$ in H_{ij} .
- Reveal U_i :** After invoking queries, $\mathfrak{S}_{Ad}$ to knows the secret credential $K_{ID_{VC}}$. If an oracle receive a reveal query from any $\mathfrak{S}_{Ad}$.
- Corrupt U_i :** If any insider party U_i behave like as $\mathfrak{S}_{Ad}$. It invokes the queries to get the private key of U_i .
- Test U_i :** The oracle picks a bit $c \in \{0, 1\}$ when it gets the test query request from $\mathfrak{S}_{Ad}$. If $c = 0$, Oracle will provide a random integer if $c = 1$, Oracle will return a session key $K_{ID_{VC}}$.

If $\mathfrak{S}_{Ad}$ correctly predicts the proper value of bit c , then $\mathfrak{S}_{Ad}$ wins the game and we denote it as $Succ(\mathfrak{S}_{Ad})$.

The advantage of $\mathfrak{S}_{Ad}$ breaking the protocol is: $ADV_{\mathfrak{S}_{Ad}}^{(A,P)}(k) = |2Pr[Succ(\mathfrak{S}_{Ad})] - 1|$

Theorem-1

Let H_1 and H be two oracles at random. If $\mathfrak{S}_{Ad}$ can break the proposed protocol, then there exist $\mathfrak{S}_{Ad_B}$ which can solve $EcCDH$ problem using $\mathfrak{S}_{Ad}$.

Proof.

$\mathfrak{S}_{Ad_B}$ starts by running an algorithm to produce all public parameters $(h, E_x(), D_x())$. After that, $\mathfrak{S}_{Ad_A}$ and $\mathfrak{S}_{Ad_B}$ interact in the following way:

1. Hash query $\mathfrak{S}_{Ad_A}$ arise hash query on X_u . $\mathfrak{S}_{Ad_B}$ checks to see if $h(G_u) \in H_{lj}$ and after the existence is verified, $\mathfrak{S}_{Ad_B}$ provides the relevant h_2 to $\mathfrak{S}_{Ad_A}$ from the hash list, else $\mathfrak{S}_{Ad_B}$ saves $(h_1 ID_k)$ in H_{lj} and computes $G_v = h(ID_{U_i} \parallel ID_{VC} \parallel A_1 \parallel A_2 \parallel A_3 \parallel T_i)$, $\mathfrak{S}_{Ad_B}$ and verifies whether h_2 is present in H_{lj} . h_2 is returned to $\mathfrak{S}_{Ad_A}$ if existence is confirmed; else, (h_2, G_v^*) is stored in H_{lj} . Then $\mathfrak{S}_{Ad_B}$ returns to $\mathfrak{S}_{Ad_A}$ the corresponding query. While $\mathfrak{S}_{Ad_A}$ performs h query on A_2 , $\mathfrak{S}_{Ad_B}$ verify whether $h(A_2)$ is present in H_{lj} . $\mathfrak{S}_{Ad_B}$ provides the relevant h_3 form H_{lj} if existence is conformed, else $\mathfrak{S}_{Ad_B}$ saves (h_3, A_2) . After that, $\mathfrak{S}_{Ad_B}$ returns the relevant query to $\mathfrak{S}_{Ad_A}$.

2. H_1 Hash query

- While $\mathfrak{S}_{Ad_A}$ performs h query on A_2 , $\mathfrak{S}_{Ad_B}$ verify whether $h_1(A_2) \oplus ID_{U_i}$ is present in H_{lk} . $\mathfrak{S}_{Ad_B}$ provides the relevant h_4 to $\mathfrak{S}_{Ad_A}$ if existence is conformed, else $\mathfrak{S}_{Ad_B}$ saves (h_4, VID_u) . After that, $\mathfrak{S}_{Ad_B}$ returns the relevant query to $\mathfrak{S}_{Ad_A}$.
- While $\mathfrak{S}_{Ad_A}$ performs h query on A_3 . Let $\mathfrak{S}_{Ad_B}$ be aware of the previous information, now $\mathfrak{S}_{Ad_B}$ computes $h_1(A_2) \oplus ID_{U_i} = h_5$, $(X_u = H(ID_u \parallel x))$. $\mathfrak{S}_{Ad_B}$ verify whether h_5 is present in H_{lk} . $\mathfrak{S}_{Ad_B}$ provides the relevant h_5 form H_{lj} if existence is conformed, else $\mathfrak{S}_{Ad_B}$ saves $(h_5, h_1(A_3))$.

3. **Send Query:** We subdivided this phase into three types, after the initial input of U_i .

- Send a request for login to S_j .
- U_i sends $(VID_u, G_v, A_1, A_3, T_i)$ to S_j .
- LS_j returns (A_4, A_5, T_k) to U_i .

4. Send $(VID_u, G_v, A_1, A_3, T_i)$ to S_j : When $\mathfrak{S}_{Ad_A}$ runs query for communication with S_j . $\mathfrak{S}_{Ad_B}$ computes $A_1^* = a \cdot P$, $ID_{U_i} = A_3 \oplus h_1(A_2)$, $Z' = H(ID_{U_i} \parallel (x + s))$ and checks $G_v' = H(ID_{U_i} \parallel ID_{VC} \parallel A_1 \parallel A_2 \parallel A_3 \parallel T_i)$ equal to $G_v' = G_v$. If holds. the $\mathfrak{S}_{Ad_B}$ compute the $A_4 = K_{ID_{VC}} \oplus h(A_2 \parallel ID_{VC} \parallel A_1 \parallel T_k)$, $A_5 = h(ID_{U_i} \parallel A_2 \parallel T_i \parallel T_k \oplus K_{ID_{VC}})$, So $\mathfrak{S}_{Ad_B}$ return c to $\mathfrak{S}_{Ad_A}$, else $\mathfrak{S}_{Ad_B}$ will deny the request.

5. Send (A_4, A_5, T_k) to U_i : While $\mathfrak{S}_{Ad_A}$ performs send query, $\mathfrak{S}_{Ad_B}$ computes A_4 , then compute $K_{ID_{VC}} = A_4 \oplus H(A_2 \parallel ID_{VC} \parallel T_i \parallel A_1 \parallel T_k)$ and verifies $A_5 = h(ID_{U_i} \oplus X_u \oplus T_i \oplus T_k \oplus K_{ID_{VC}})$ if it's holds then $\mathfrak{S}_{Ad_B}$ authenticate $\mathfrak{S}_{Ad_A}$. Otherwise reject the login request request.

6. Analysis In the existing game, let q_i be the total instance of $\Pi_{U_i}^\eta$. The output length of H_1 is s bits and that of the elliptic curve point is l bits. If $\mathfrak{S}_{Ad_A}$ can forge the message (A_4, A_5) in order to replicate the message (G_1, G_2) , then $\mathfrak{S}_{Ad_A}$ can break the proposed scheme.

- a. If $\mathfrak{S}_{Ad_A}$ predicts the value of $(A_4 \text{ or } A_5)$ without knowing IDu or calling the query H . In that instance, $P_r(\mathfrak{S}_{Ad_A})$ to accurately predict the right output of G_2 is smaller than $\frac{1}{2s}$ i.e. $P_r(\mathfrak{S}_{Ad_A}) : \text{to guess } [G_1 / G_2] < \frac{1}{2s}$.
- b. If $\mathfrak{S}_{Ad_A}$ does not require guessing to forge $A_4 \text{ or } A_5$ but instead chooses an authentic message like (u, VID'_u) . The probability of $\mathfrak{S}_{Ad_A}$ making an accurate guess or finding the same value (u, VID'_u) in different sessions is referred as the event e' is less than $q_i / 2^{l^2}$ i.e. $P_r[\mathfrak{S}_{Ad_A}(e')] < q_i / 2^{l^2}$.
- c. Assuming $\mathfrak{S}_{Ad_A}$ want to acquire $K_{ID_{VC}}$ to effectively imitate the communication. Let $r_u P = Z$, and chosen xP such that $xr_u P = xZ$ which is equal to $A_2 = a.xP$ for some a , $x \in Z_q^*$ must get xP in order to solve the $EcCDH$ problem. This δ' is the probability of $\mathfrak{S}_{Ad_A}$ making a correct prediction. If $\mathfrak{S}_{Ad_A}$ has a non-eligible advantage δ , then $\mathfrak{S}_{Ad_B}$ has $\delta - (1/2s) - (q_i/2l2) \leq \delta'$ the advantage in solving the $EcCDH$ problem. Therefore $\mathfrak{S}_{Ad_B}$ has the advantage because if $\mathfrak{S}_{Ad_A}$ breaks the proposed scheme, so can $\mathfrak{S}_{Ad_B}$.

7. PERFORMANCE ANALYSIS AND COMPARISONS

For different related schemes such as Liu et al. [13], Lo and Tsai. [14], Cui et al. [6], Bayat et al. [4], and Maitra et al. [16], a thorough performance analysis is conducted, which covers security properties, and computational and communication costs. The cost of various operations are (see Table (I)) hashing T_h takes 0.000530 seconds, T_{ecm} denotes elliptic curve multiplication takes 0.10300 seconds, T_{eca} denotes elliptic curve addition takes 0.001560 seconds, T_{sym} Tsym denotes encryption or decryption takes 0.15500 seconds, T_{fe} denotes fuzzy extractor takes 0.06300 seconds, and T_b Tb denotes bilinear pairing takes 0.0003 seconds. With a total cost of 0.4580 seconds, Liu et al. [13] use $13.00 T_h + 01.00 T_{fe} + 02.00 T_{sym}$ on the user side and $13.00 T_h + 02.00 T_{sym}$ on the server side. Tsai and Lo. With a total cost of 0.89080 seconds, [14] uses $05.00 T_h + 02.00 T_{sym}$ on the user side and $05.00 T_h + 03.00 T_{ecm} + 01.00 T_{eca}$ on the server side. With a total cost of 0.41460 seconds, Cui et al. [6] use $12.00 T_b + 05.00 T_h$ on the user side and $03.00 T_b + 05.00 T_{ecm}$ on the server side. With a total cost of 02.760 seconds, Bayat et al. [4] use $01.00 T_h + 02.00 T_{ecm} + 04.00 T_b$ on the user side and $01.00 T_h + 01.00 T_{ecm} + 03.00 T_b$ on the server side. $09.00 T_h + 05.00 T_e + 01.00 T_{fe}$ is taken by Maitra et al. [16].

OPERATIONS AND TIME COMPLEXITY

Notations	Meaning	Time (in Sec.)
T_h	Hash Function	0.000530
T_{ecm}	Elliptic Curve Multiplication	0.103000
T_{eca}	Elliptic Curve Addition	0.001560
T_{sym}	Encryption/Decryption	0.155000
T_{fe}	Fuzzy Extractor	0.063000
T_b	Bilinear Pairing	0.000300

TOTAL COMPUTATIONAL COST

Schemes	User	Service provider	Total
---------	------	------------------	-------

Liu et al. ^[13]	$13.00 T_h + 01.00 T_{fe} + 02.00 T_{sym}$	$13.00 T_h + 02.00 T_{sym}$	0.45800
Lo and Tsai. ^[14]	$05.00 T_h + 02.00 T_{ecm}$	$05.00 T_h + 03.00 T_{ecm} + 01.00 T_{eca}$	0.89080
Cui et al. ^[6]	$12.00 T_b + 05.00 T_h$	$03.00 T_b + 05.00 T_{ecm}$	0.41460
Bayat et al. ^[4]	$01.00 T_h + 02.00 T_{ecm} + 04.00 T_b$	$01.00 T_h + 01.00 T_{ecm} + 03.00 T_b$	2.76000
Maitra et al. ^[16]	$09.00 T_h + 05.00 T_e + 01.00 T_{fe}$	$06.00 T_h + 03.00 T_e$	0.21500
Proposed	$06.00 T_h + 02.00 T_{ecm}$	$05.00 T_h + 01.00 T_{ecm} + 01.00 T_{eca}$	0.06020

With a total cost of 0.2150 seconds on the user side and $06.00 T_h + 03.00 T_e$ on the server side. With a total cost of 0.06020 seconds, the suggested takes $06.00 T_h + 02.00 T_{ecm}$ on the user side and $05.00 T_h + 01.00 T_{ecm} + 01.00 T_{eca}$ on the server side.

TOTAL COMPUTATION OVERHEAD IN COMMUNICATION

Schemes	Approx communication cost in bits	No. of communication
Bayat et al. [4]	992.00	02
Lo and Tsai. [14]	1344.0	02
Liu et al. [13]	1344.0	02
Cui et al. [6]	3104.0	02
Maitra et al. [16]	1280.0	02

Additionally, we contrast the suggested scheme's merit analysis and efficiency with those of alternative smart card-based authentication systems. All notations, along with their definitions and execution times (in seconds), are provided in operations and time complexity. If device transmission is $(160 + 160 + 160 + 320 + 32) \text{ bits} = 832 \text{ bits}$ and the server transmits back to user overhead is $(160 + 160 + 32) \text{ bits} = 352 \text{ bits}$, then the overhead in the suggested scheme will be calculated as follows. Additionally, the user transmits a 160-bit verification message. Our suggested plan is effective.

8. Conclusion

To improve traffic safety and management, this paper presented an intelligent transport authentication system for Vanet using ECC. An important advancement in the vehicle communication system is the efficiency-focused vehicular ad-hoc network structure. The suggested approach enables the utilization of distinct biological traits for every user. Communication eavesdropping is protected by the scheme. Security of the formal proof is given in the random oracle model. Following that, we conducted a performance analysis, which demonstrates the low computation and communication costs of the suggested scheme. When compared to other existing schemes, the proposed scheme has an advantage.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

References

1. Zeinab E Ahmed, Rashid A Saeed, and Amitava Mukherjee. Challenges and opportunities in vehicular cloud computing. In *Cloud Security: Concepts, Methodologies, Tools, and Applications*, pages 2168–2185. IGI Global, 2019.
2. Alessandro Armando, David Basin, Yohan Boichut, Yannick Chevalier, Luca Compagna, Jorge Cuéllar, P Hankes Drielsma, Pierre-Cyrille Héam, Olga Kouchnarenko, Jacopo Mantovani, et al. The Avispa tool for the automated validation of internet security protocols and applications. In *International conference on computer aided verification*, pages 281–285. Springer, 2005.
3. Alessandro Armando, David Basin, Jorge Cuéllar, Michael Rusinowitch, and Luca Viganò. Avispa: automated validation of internet security protocols and applications. *ERCIM News*, 64(January), 2006.
4. Majid Bayat, Mostafa Barmshoory, Majid Rahimi, and Mohammad Reza Aref. A secure authentication scheme for vents with batch verification. *Wireless networks*, 21(5):1733–1743, 2015.
5. Jeremy Blum and Azim Eskandarian. The threat of intelligent collisions. *IT professional*, 6(1):24–29, 2004.

6. Jie Cui, Lu Wei, Jing Zhang, Yan Xu, and Hong Zhong. An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, (99):1–12, 2018.
7. Danny Dolev and Andrew Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.
8. Yong Hao, Yu Cheng, Chi Zhou, and Wei Song. A distributed key management framework with cooperative message authentication in vanets. *IEEE Journal on selected areas in communications*, 29(3):616–629, 2011.
9. Jakub Jakubiak and Yevgeni Koucheryavy. State-of-the-art and research challenges for vanets. In 2008 5th IEEE Consumer Communications and Networking Conference, pages 912–916. IEEE, 2008.
10. Daniel Jiang and Luca Delgrossi. Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments. In VTC Spring 2008-IEEE Vehicular Technology Conference, pages 2036–2040. IEEE, 2008.
11. Zhang Jianhong, Xu Min, and Liu Liying. On the security of a secure batch verification with group testing for vanet. *International Journal of Network Security*, 16(5):351–358, 2014.
12. Yen-Wen Lin, Jie-Min Shen, and Hao-Chun Weng. Cloud-supported seamless internet access in intelligent transportation systems. *Wireless personal communications*, 72(4):2081–2106, 2013.
13. Xin Liu and Ruisheng Zhang. A robust authentication scheme with continuously updated information for vehicular sensor networks. *IEEE Access*, 6:70473–70486, 2018.
14. Nai-Wei Lo and Jia-Lun Tsai. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. *IEEE Transactions on Intelligent Transportation Systems*, 17(5):1319–1328, 2015.
15. Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin Shen. A dynamic privacy-preserving key management scheme for location-based services in vanets. *IEEE Transactions on Intelligent Transportation Systems*, 13(1):127–139, 2011.
16. Tanmoy Maitra, Debasis Giri, and Ram N Mohapatra. Sas-sip: A secure authentication scheme based on ECC and a fuzzy extractor for session initiation protocol. *Cryptologia*, pages 1–21, 2019.
17. Stephan Olariu, Tihomir Hristov, and Gongjun Yan. The next paradigm shift: from vehicular networks to vehicular clouds. *Mobile ad hoc networking: cutting edge directions*, 56(6):645–700, 2013.
18. Craig L Robinson, Derek Caveney, Lorenzo Caminiti, Girish Baliga, Ken Laberteaux, and PR Kumar. Efficient message composition and coding for cooperative vehicular safety applications. *IEEE Transactions on Vehicular Technology*, 56(6):3244–3255, 2007.
19. Jijun Yin, Tamer ElBatt, Gavin Yeung, Bo Ryu, Stephen Habermas, Hariharan Krishnan, and Timothy Talty. Performance evaluation of safety applications over dsrc vehicular ad hoc networks. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 1–9. ACM, 2004.
20. Qin, X., Huang, Y., & Li, X. (2020). An ECC-based access control scheme with lightweight decryption and conditional authentication for data sharing in vehicular networks. *Soft Computing*, 24, 18881–18891.
21. Ali, I., Chen, Y., Ullah, N., Kumar, R., & He, W. (2021). An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs. *IEEE Transactions on Vehicular Technology*, 70(2), 1278–1291.
22. Chen, Y., Yin, F., Hu, S., Sun, L., Li, Y., Xing, B., ... & Guo, B. (2022). ECC-based authenticated key agreement protocol for industrial control system. *IEEE Internet of Things Journal*, 10(6), 4688–4697.
23. Dwivedi, S. K., Amin, R., Vollala, S., & Das, A. K. (2023). Design of blockchain and ECC-based robust and efficient batch authentication protocol for vehicular ad-hoc networks. *IEEE Transactions on Intelligent Transportation Systems*.
24. Zhou, Y., Cao, L., Qiao, Z., Xu, R., Han, Y., Xing, J., ... & Zhang, M. (2024). A Novel Cloud-Assisted Authentication Key Agreement Protocol for VANET. *IEEE Transactions on Vehicular Technology*
25. Lee, S., Son, S., Kwon, D., Park, Y., Park, Y. (2025). A secure and efficient authentication scheme for fog-based vehicular ad hoc networks. *Applied Sciences*, 15(3), 1229. <https://doi.org/10.3390/app15031229>
26. Rajkumar, Y., & Santhosh Kumar, S.V.N. (2025). A Dickson polynomial-based group key agreement authentication scheme for ensuring conditional privacy preservation and traceability in VANETs. *Scientific Reports*, 15, 6211. <https://doi.org/10.1038/s41598-025-89208-5>
27. Li, L., Zhang, H., Li, S., Liu, J., Chen, C. (2025). A lightweight batch authenticated key agreement scheme based on fog computing for VANETs. *Symmetry*, 17(8), 1350. <https://doi.org/10.3390/sym17081350>