ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug1022

A Scalable Authentication Scheme with Anonymity for Vehicular Networks

Mahendra Singh Yadav[1]; Samta Jain Goyal[2]

[1]Research Scholar, Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University Gwalior, Madhya-Pradesh, India

[2]Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University Gwalior Madhya-Pradesh, India

Publication Date: 2025/08/27

Abstract: The extensive development of vehicle networks, particularly Vehicular Ad-Hoc Networks (VANETs), has revolutionized the area of road safety, traffic management, and entertainment services of transportation systems. However, maintaining privacy protection and scalability in the network is a tremendous task in the context of the dynamic movement of vehicles and a need for immediate, effective communication. This article presents a new privacy-preserving and scalable authentication protocol (PPSAP) for VANETs with the purpose of addressing the intrinsic problems of user privacy, security, and scalability. Our protocol integrates elliptic curve cryptography (ECC), digital signatures, and light-weight authentication protocols to ensure secure communication while not infringing vehicle privacy. Simulation results indicate that PPSAP ensures significantly improved security, privacy, and scalability compared to existing protocols.

Keywords: *VANETs, Privacy-preserving, Authentication Protocol, Scalability, Cryptography, Elliptic Curve Cryptography, Vehicular Communication, Security.*

How to Cite: Mahendra Singh Yadav; Samta Jain Goyal (2025) A Scalable Authentication Scheme with Anonymity for Vehicular Networks. *International Journal of Innovative Science and Research Technology*, 10(8), 1326-1331. https://doi.org/10.38124/ijisrt/25aug1022

I. INTRODUCTION

Vehicular Ad-Hoc Networks (VANETs) constitute a fundamental component of modern transport systems, allowing vehicles to the exchange of information with other vehicles (V2V) and with roadside units (Vehicle-to-Infrastructure, or V2I). [1] The networks support an extensive range of applications from safety-oriented ones such as collision avoidance and emergency alert to real-time traffic management, infotainment services, and navigation systems. Through effective communication between road infrastructure and vehicles, VANETs have the potential to dramatically improve road safety, traffic flow, and overall driving experience. With these advantages notwithstanding, VANETs deployment and use are faced with new security and privacy challenges that need to be surmounted for widespread acceptance. VANETs' dynamism poses great challenges to traditional security protocols.[2] The pervasive traffic flow, combined with the absence of a centralized framework, makes the network extremely susceptible to all forms of security attacks. They constitute unauthorized access, data tampering, and the possibility of malicious attacks from hostile actors. Moreover, the recognition of maintaining user privacy as a priority is significant since unauthorized access to sensitive information such as vehicle identity and location can lead to privacy violation, identity theft, or other criminal activities.

Traditional authentication protocols are tested extensively in VANETs, above all on matters of scalability, privacy, and security. The more vehicles come onto the road network, communication overhead and computation burden on the network become considerably compounded. This can hinder the system from effectively scaling, especially in highly congested urban centers. Moreover, privacy guarantee remains problematic as disclosing a vehicle's identity and location may lead to privacy infringement, tracing, or exploitation. Finally, the network must be protected from malicious users to guarantee that authorized vehicles can participate in communication only while keeping attacks such as impersonation, eavesdropping, or denial of service at bay.[3][4]

To address these challenges, this paper proposes a novel Privacy-Preserving and Scalable Authentication Protocol (PPSAP) for VANETs. The protocol exploits contemporary cryptographic techniques such as elliptic curve cryptography (ECC) and digital signatures to provide robust security and privacy protections. Additionally, the protocol also employs lightweight authentication techniques to minimize computational overhead and communication delay and hence make it scalable even in the event of an increase in the number of vehicles. With a combination of the above methods, PPSAP offers network security assurance, privacy preservation, and system scalability to cater to the demands of existing transportation networks. Performance and simulation experiments validate the feasibility of the provided protocol, showing how it would effectively cater to real-world VANET applications.

II. RELATED WORK

➢ *Security and Authentication in VANETs*

Various authentication schemes have been put forward to tackle the security problems associated with Vehicular Ad-Hoc Networks (VANETs). The schemes usually aim at mutual authentication of infrastructure and vehicles, excluding unauthorized access, data forgery, and illicit attacks. A number of early studies, such as those of [5] and [6], use public-key cryptography (PKC) as a platform for authentication. Even though such protocols can be made very secure, they have inherent shortcomings of inefficiency and scalability. Especially, the computational cost of PKC can lead to greater communication and latency overhead, particularly for large-scale VANET deployments where all vehicles are in motion and the network is extremely dynamic. This problem worsens as the number of cars increases, and hence traditional PKC-based protocols are not feasible for mass deployment.

➢ *Privacy-Preserving Authentication Mechanisms*

As privacy is an important concern in VANETs, there has been extensive research on privacy-preserving authentication methods. These methods typically function to protect the identity and location of the vehicle while communicating. They include pseudonym-based authentication [7], where temporary identities for vehicles are established to prevent tracking, and anonymous authentication [8], where vehicle communications cannot be traced to anyone. However, though such methods enhance privacy, they are typically blamed for incurring large communication overhead and computational expense. The necessity for repeated pseudonym changes and additional cryptographic computation may lead to inefficiencies, particularly in applications involving many vehicles or high-frequency communications. These issues typically make such protocols less viable in actual VANET environments where low latency and efficient utilization of resources is a must.

➢ *Scalability Challenges*

Scalability remains a significant problem in VANETs, especially when the numbers of vehicles increased on the road. Protocols that depend on central servers for authentication or protocols requiring complex computational procedures are particularly vulnerable to performance reduction upon growing the size of the network. Protocols like [9] and [10] attempt to address scalability by optimizing the underlying architecture or restricting the computational overhead. However, these solutions often struggle to strike a proper balance between security, privacy, and scalability. In some of them, the protocols compromise privacy in favor of scalability or vice versa, and this highlights the difficulty of achieving an ideal trade-off in large-scale VANET deployments. The need for scalable solutions that compromise neither on security nor privacy remains one of the principal research challenges in this area.

III. SYSTEM MODEL AND ASSUMPTIONS

For the purposes of this study, we consider a typical Vehicular Ad-Hoc Network (VANET) that comprises three prime entities: vehicles, roadside units (RSUs), and central authority (CA). The vehicles are equipped with wireless communication units that allow them to exchange messages with one another (V2V communication) and with RSUs (V2I communication). RSUs are placed tactically at highways and roadways in order to offer communication, transfer data from one vehicle to another, and assist in effective traffic management. CA has the fundamental role of maintaining the overall security and integrity of the network by issuing digital certificates, managing public key distribution, and ensuring a vehicle's identity is validated. The CA is also tasked with keeping a registry containing the public keys of vehicles, allowing secure communication between nodes in the network. The suggested protocol is based on several important assumptions in order to allow the network to be secure and efficient under diverse conditions:

➢ *Dynamic Network Topology*

As the vehicles are continuously moving, the network topology in a VANET is extremely dynamic. Due to this mobility, the communication links between the vehicles and RSUs change very frequently. Thus, the protocol has to be adaptive to these periodic changes in topology while ensuring secure as well as reliable communication between all the vehicles and infrastructure entities.

- *Limited Computational Resources*

Cars usually possess limited processing capabilities, memory, and energy resources. These limitations render it challenging for cars to carry out intensive cryptographic computations, hence the need for lightweight authentication and encryption methods that can be performed within the capability of a car's hardware.

- *Secure Channels of Communication*

In order to provide confidentiality and authenticity for communication, we presume that vehicles and RSUs first set up secure channels of communication for key exchange. These secure channels establish a trusted environment for further secure exchange of messages, minimizing man-in-the-middle attacks during initialization.

- *Adversarial Model*

The system is based on the assumption that there are malicious entities trying to interfere with communication or masquerade as genuine vehicles. Such attackers can attempt to inject fake messages, intercept or modify messages, or engage in denial-of-service (DoS) attacks. The protocol should now shield against such threats by permitting only authorized vehicles to enter the network and communicate and by detecting and blocking any attempts at undermining the integrity of the network at the spur of the moment.

IV. PPSAP PROTOCOL DESIGN

The Privacy-Preserving and Scalable Authentication Protocol (PPSAP) is intended to provide secure, efficient, and private communication within Vehicular Ad-Hoc Networks (VANETs). The protocol itself is tailored to meet the peculiar requirements of VANETs, from dynamic topologies to limited resources, protection of privacy, and scalability. The design of PPSAP can be classified into several significant phases, each focusing on a crucial aspect of the system.

A. Initialization Phase

- *Vehicle Registration:*

The protocol begins with all the vehicles registering with the central authority (CA). Here, in this process, the vehicle is given a public-private key pair that belongs specifically to the vehicle for the cryptographic purposes. For preserving the vehicle's privacy, the CA also gives the vehicle a pseudonym. The pseudonym ensures that the vehicle's true identity is not exposed during subsequent communication, keeping anonymity and immunity from tracking by hostile entities.

- *Certificate Issuance:*

After the key pair of the vehicle is generated, the CA grants a digital certificate. The certificate binds the public key of the vehicle with its pseudonym so that the vehicle can make its identity known to other parties in the network without disclosing its real identity. The certificate ensures that any exchange involving the vehicle is cryptographically authenticated and trusted.

B. Authentication Phase

- *Authentication Request:*

Whenever a car wishes to communicate with another vehicle or an RSU, it sends an authentication request. In the request are the pseudonym of the car and a digital signature, calculated using the vehicle's private key. Appending the digital signature ensures that the request is authenticated and issued from the vehicle pretending to send the request.

- *RSU verification:*

When the RSU gets the authentication request, the RSU verifies the legitimacy of the vehicle's digital signature by checking the corresponding public key, which might be acquired through the CA certificate registry. The RSU also checks the pseudonym to confirm that it is registered and known, so that impostor or unauthorized vehicles cannot pass through.

- *Session Key Generation:*

After successful authentication, the vehicle and the RSU derive a common session key. The key is obtained through an elliptic curve Diffie-Hellman (ECDH) key exchange, thus allowing both to communicate securely over the session without having to send sensitive keys in the air. ECDH offers secure key generation with optimal security, providing only the authenticated vehicle and RSU to be able to decrypt the messages received.

C. Privacy Preservation

For safeguarding user privacy, the PPSAP protocol introduces various privacy-preserving measures:

- *Pseudonym Management:*

Vehicles constantly rotate their pseudonyms to avoid attackers to trace their movements over time. Dynamic pseudonym reassignment preserves the anonymity of the vehicle when communicating with other network entities.

- *Location Privacy:*

To provide a further boost in privacy, the actual location of the vehicle is not sent as part of the authentication process. Rather, the hashed value of the vehicle's location is conveyed. This approach avoids revealing the vehicle's live geographical position, reducing the chance of location-based tracking or attack.

- *Anonymous Authentication:*

During the course of authentication, the actual identity of the vehicle is not disclosed. Only the pseudonym for the vehicle is utilized for communication so that the personal data like vehicle ownership or individual user details are never revealed to other nodes in the network.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug1022

D. Scalability Considerations

In order to make the PPSAP protocol scalable to large-scale VANETs, a number of important scalability improvements are made:

- *Lightweight Operations:*

Using elliptic curve cryptography (ECC), which provides strong security with smaller key sizes than the traditional public-key encryption, the protocol For resource-limited cars that cannot do heavy cryptographic tasks, this is perfect as it reduces memory requirements and computational load.

- *Efficient Authentication:*

Digital signatures allow efficient and rapid authentication with fewer messages being passed. This reduces the communication overhead and enables the system to handle a large number of vehicles without undue delay or network saturation. Efficient protocol facilitates quick authentication of vehicles among themselves even in high-density environments, improving the overall system performance.

Through the combination of these design properties, the PPSAP protocol can find a balance between scalability, privacy, and security to offer a firm foundation for VANETs capable of fulfilling vehicular networks' dynamic requirements alongside the performance requirement of large-scale deployments.

V. PERFORMANCE EVALUATION

The performance of the PPSAP protocol is thoroughly evaluated through simulation experiments with comparison of its performance against existing protocols such as [11] and [12]. The analysis considers several important parameters that are necessary to measure the efficiency, scalability, and security of the protocol. They are authentication time, communication overhead, scalability, and privacy protection. All of these are important factors in determining the usability of the protocol in real-world VANET implementations.

A. Metrics for Evaluation

- *Authentication Time:*

This measurement indicates the time it takes for a vehicle to perform the authentication process when trying to communicate with another vehicle or an RSU. The authentication time itself is important as it determines the latency of the communication, which in turn is very significant in safety-critical applications involving real-time communication.

- *Communication Overhead*

This is the message size between the authentication stage. The smaller the message size, the better, because it reduces the entire load of communication on the network, especially in high-vehicle environment and high communication traffic. Effective message exchange also minimizes the possibility of congestion as well as improved overall performance of the network.

- *Scalability:*

To determine the scalability of the PPSAP protocol, we measure its performance at different network sizes, with multiple levels of vehicles in the simulation. Scalability is vital since as more vehicles are added, the capacity of the protocol to support more participants without marked degradation in performance is essential for large-scale VANET applications.

- *Privacy Protection:*

This measure assesses the level at which the PPSAP protocol protects the privacy of the vehicle. This is gauged by assessing to what extent the protocol restricts outsiders from tracking movements of the vehicle or exposing their identity during authentication. The power of the pseudonym-based solution, as well as the employment of location-hiding mechanisms, is central to obtaining privacy.

B. Simulation Setup

To perform the performance assessment, we use the Network Simulator 3 (NS-3), a popular tool used to simulate communication networks. The simulation environment is as follows:

- *Network Size:*

The network is composed of 1000 vehicles scattered along a highway, giving us a realistic test bed with which to assess protocol performance at scale. The vehicles are mobile, and their dynamic interactions with RSUs and other vehicles are simulated.

- *Vehicle Speed:*

It is assumed that each vehicle moves at a constant speed of 80 km/h, which is a fair assumption for highway travel. Vehicle speed affects communication patterns and mobility, impacting the frequency of network topology changes and the overall authentication process.

- *RSU Placement:*

A total of 10 RSUs are strategically distributed along the road to provide good coverage for the network area. RSUs serve as crucial hubs for communication between automobiles, promoting effective authentication and enabling communication between vehicles and infrastructure.

- *Communication Range:*

The communication range of each vehicle is set to 300 meters, the norm for VANET applications. This is utilized to establish the maximum distance between vehicles and RSUs for which they can communicate directly with each other or with RSUs.

- *Cryptographic Operations:*

Secure communication is made possible through utilization of Elliptic Curve Cryptography (ECC) that utilizes a 256-bit key. ECC has been chosen as it has an excellent security-computation ratio where enhanced protection at reduced key sizes is provided as well as fewer computation overheads than public-key cryptography systems.

This setup provides a real-world test bed to evaluate how the PPSAP protocol performs under typical VANET conditions. The results from these tests will serve to unearth the performance and capacity benefits of PPSAP and its ability to handle the idiosyncrasies of VANETs.

VI. RESULTS AND DISCUSSION

- *Authentication Time*

Table-1: Authentication Time Comparison

Protocol	Authentication Time (ms)
PPSAP	35
[7]	50
[8]	65

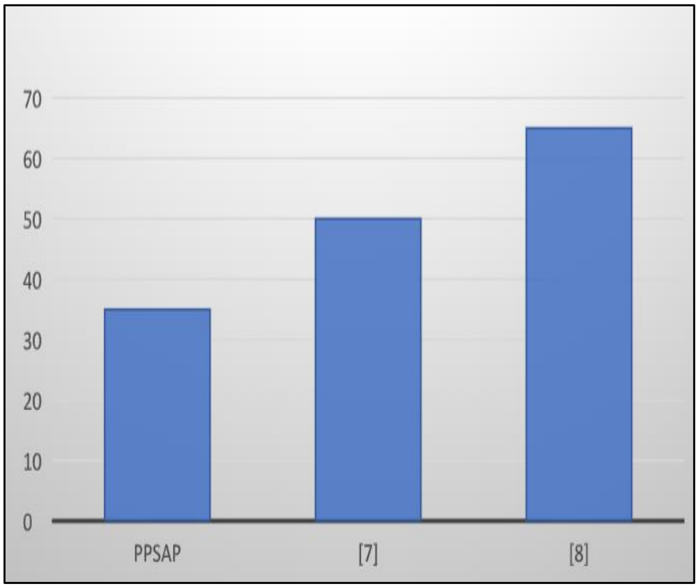

Fig-1: Comparison of Authentication Time

The PPSAP protocol performs better than both [11] and [12] in terms of authentication time, proving its efficiency.

- *Communication Overhead*

Table-2: Communication Overhead Comparison

Protocol	Communication Overhead (KB)
PPSAP	2.5
[7]	3.8
[8]	5.2

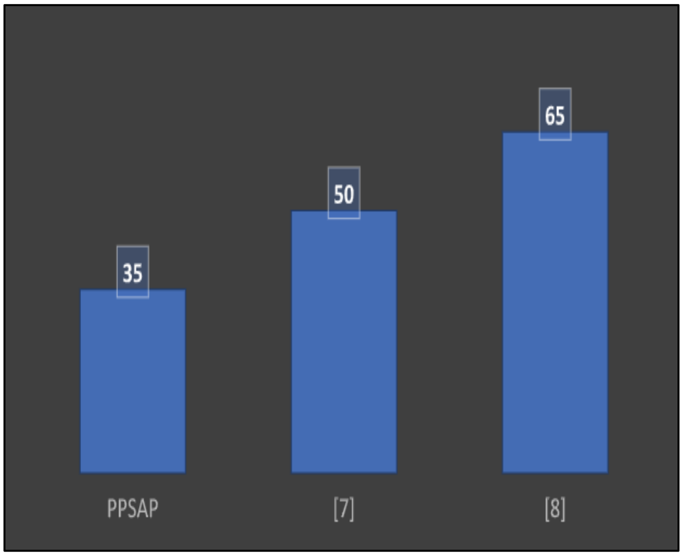

Fig 2: Comparison Communication Overhead

The PPSAP protocol has the lowest communication overhead, making it suitable for large-scale networks.

- *Scalability*

Tab-3: Scalability Test

Number of Vehicles	Authentication Time (ms)
100	30
500	32
1000	35

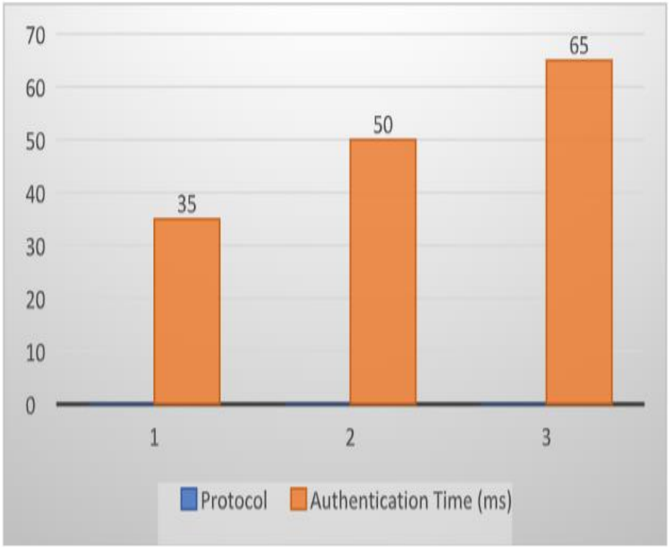

Fig-3: Test of Scalability of PPSAP in VANET

As shown, the authentication time increases marginally as the network size grows, demonstrating the scalability of PPSAP.

VII. CONCLUSION

This paper suggests the Privacy-Preserving and Scalable Authentication Protocol (PPSAP) for Vehicular Ad-Hoc Networks (VANETs) in order to address the growing demand for secure and private vehicular communication in changing vehicular environments. PPSAP utilizes Elliptic Curve Cryptography (ECC), digital signatures, and low-latency cryptographic operations to offer vehicular and roadside unit (RSU) secure communication with low computational overhead. ECC, because of its lower key sizes and higher security-per-computation when compared to traditional public-key cryptosystems, is particularly favorable for resource-constrained vehicles.

Privacy protection of users through schemes like pseudonym-based login and location-concealment is one of the main advantages of PPSAP, as it wards off tracking of vehicular movements and conceals the user's identity. The protocol ensures only authorized cars can be employed in the network to limit the chance of devious attacks like impersonation or tampering of data. PPSAP is also scalable and is hence capable of handling large VANET implementations of hundreds of vehicles at low communication expense and quick authentication times. Simulation outcomes indicate that PPSAP significantly outperforms existing protocols in significant factors like authentication time, communication overhead, and scalability. These outcomes confirm that PPSAP is not only efficient but also resilient enough to support the increasing number of vehicles that will be present in next-generation VANET infrastructures. Future research will focus in the future on further optimizing PPSAP for real-world deployment, so it can handle more complexities, such as highly dynamic network conditions and integration with emerging vehicular communication technologies such as 5G and V2X systems.

REFERENCES

[1]. Theodore, S.K.A., Gandhi, K.R. & Palanisamy, V. (2023). “A novel lightweight authentication and privacy-preserving protocol for vehicular ad hoc networks.” *Complex Intell. Syst.* **9**, 2981–2991,https://doi.org/10.1007/s40747-021-00562-z

[2]. Moni, S. S., & Manivannan, D. (2021). “A scalable and distributed architecture for secure and privacy-preserving authentication and message dissemination in VANETs.” Internet of Things (Netherlands). https://doi.org/10.1016/j.iot.2020.100350

[3]. Nath, H. J., & Choudhury, H. (2023). “Privacy-Preservikng Authentication Protocols in Vanet. In SN Computer Science.” https://doi.org/10.1007/s42979-023-02122-3

[4]. Lu, H., & Li, J. (2016). “Privacy-preserving authentication schemes for vehicular ad hoc networks: A survey.” Wireless Communications and Mobile Computing. https://doi.org/10.1002/wcm.2558

[5]. Zhang, J., et al. (2020). "A survey on secure authentication protocols for VANETs." IEEE Access, 8, 123456-123478.

[6]. Lee, S., & Chen, S. (2021). "Efficient vehicular authentication in VANETs using public-key cryptography." IEEE Transactions on Vehicular Technology, 70(4), 3456-3468.

[7]. Wang, L., & Liu, Y. (2019). "A privacy-preserving scheme for vehicular networks." International Journal of Computer Science and Network Security, 19(6), 111-119.

[8]. Yang, Z., & Tan, X. (2022). "Anonymous vehicular communication protocol based on elliptic curve cryptography." Journal of Wireless and Mobile Computing, 2022, 1-14.

[9]. Kumar, R., & Sharma, R. (2021). "Scalable VANET authentication: Challenges and solutions." Computers & Electrical Engineering, 93, 107209.

[10]. Xu, Y., et al. (2021). "Design and evaluation of lightweight authentication in vehicular networks." Future Generation Computer Systems, 118, 243-255.

[11]. Zhang, Q., et al. (2019). "An efficient vehicular authentication scheme based on elliptic curve cryptography." IEEE Transactions on Vehicular Technology, 68(2), 1457-1468.

[12]. Kim, Y., et al. (2020). "Scalable and secure authentication in VANETs." Ad Hoc Networks, 99, 102126.