НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
июль–август 2025 Том 25 № 4 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
Jule–August 2025 Vol. 25 No 4 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
сентябрь–октябрь 2023 Том 23 Номер 5

doi: 10.17586/2226-1494-2025-25-4-755-761

An improved authentication protocol for self-driving vehicles based on Diffie–Hellman algorithm

Muhammad Salman Saeed[1], Sergey V. Bezzateev[2]✉

[1] ITMO University, Saint Petersburg, 197101, Russian Federation
[2] Saint Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, 190000, Russian Federation

[1] salman.saeed@itmo.ru, https://orcid.org/0009-0006-1425-4863
[2] bsv@guap.ru✉, https://orcid.org/0000-0002-0924-6221

Abstract
Authentication is a critical challenge in autonomous vehicles, particularly within Controller Area Networks which are prone to various cyber threats. Existing protocols often fall short in balancing strong security guarantees with computational efficiency and privacy preservation. In this paper, we propose a lightweight authentication protocol based on the Decisional Diffie–Hellman problem, specifically designed for Controller Area Network environments. The protocol employs lightweight cryptographic operations to verify vehicle authenticity and validate data messages, while also maintaining anonymity by regularly updating login identities. It also supports password changes without requiring a trusted third party. The protocol security is formally verified using Burrows-Abadi-Needham logic. Performance evaluation shows that our approach significantly reduces computational overhead, achieving an execution time of 0.90908 ms, outperforming existing solutions in the literature. By combining formal verification with practical efficiency, the proposed protocol offers a robust solution for secure and efficient authentication in resource-constrained vehicular networks. Its lightweight design and anonymity-preserving mechanisms make it particularly suitable for real-time autonomous vehicle applications.

Keywords
autonomous vehicles, controller area networks, authentication protocol, efficient authentication, anonymity-preserving mechanisms

Acknowledgments
The work was carried out within the framework of the State Assignment (project No. FSER-2025-0003).

For citation: Saeed M.S., Bezzateev S.V. An improved authentication protocol for self-driving vehicles based on Diffie–Hellman algorithm. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2025, vol. 25, no. 4, pp. 755–761. doi: 10.17586/2226-1494-2025-25-4-755-761

УДК 004.056

Улучшенный протокол аутентификации беспилотных транспортных средств, использующий алгоритм Диффи–Хэллмана

Мухаммад Салман Саид[1], Сергей Валентинович Беззатеев[2]✉

[1] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[2] Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация

[1] salman.saeed@itmo.ru, https://orcid.org/0009-0006-1425-4863
[2] bsv@guap.ru✉, https://orcid.org/0000-0002-0924-6221

Аннотация
Аутентификация является критически важной задачей в автономных транспортных средствах, особенно в сетях контроллеров, которые подвержены различным киберугрозам. Существующие протоколы часто не обеспечивают надлежащий баланс между высокими гарантиями безопасности, вычислительной эффективностью

и защитой конфиденциальности. В работе предлагается облегченный протокол аутентификации, основанный на предположении о сложности решения задачи Диффи–Хеллмана, специально разработанный для сети контроллеров. Протокол использует простые криптографические операции для проверки подлинности транспортного средства и подтверждения достоверности передаваемых данных, при этом поддерживая анонимность за счет регулярного обновления идентификаторов входа. Также поддерживается смена пароля без необходимости в доверенном третьем лице. Безопасность протокола формально подтверждена с использованием логики Берроуза–Абади–Нидхема. Оценка производительности показывает, что предложенный подход значительно снижает вычислительные затраты, достигая времени выполнения 0,90908 мс, что превосходит существующие решения, представленные в подобных научных работах. Благодаря сочетанию формальной верификации и практической эффективности, предлагаемый протокол представляет собой надежное решение для безопасной и эффективной аутентификации в условиях ограниченных ресурсов транспортных сетей. Простая структура и механизмы сохранения анонимности делают предлагаемый протокол особенно подходящим для приложений в реальном времени в автономных транспортных системах.

Ключевые слова
автономные транспортные средства, сети контроллеров, протокол аутентификации, эффективная аутентификация, механизмы сохранения анонимности

Благодарности
Работа выполнена в рамках государственного задания (проект № FSER-2025-0003).

Ссылка для цитирования: Саид М.С., Беззатеев С.В. Улучшенный протокол аутентификации беспилотных транспортных средств, использующий алгоритм Диффи–Хэллмана // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 4. С. 755–761 (на англ. яз.). doi: 10.17586/2226-1494-2025-25-4-755-761

Introduction

With the rapid growth of vehicle communication technologies, like cellular networks, Autonomous Vehicles (AVs) are reality now. These networks allow vehicles to interact with each other, enabling applications, such as cooperative safety driving, location-based services, and media sharing [1]. However, as these services become more common, they raise serious security issues, particularly around user and message authentication [2]. Without proper safeguards, attackers could exploit vulnerabilities to carry out attacks like replay, identity theft, or impersonation, threatening the security of vehicle networks.

Vehicle Controller Area Networks (CANs) are especially vulnerable because they require fast, reliable communication to ensure the safety of drivers and passengers. For instance, in safety-critical applications, even a slight delay in message delivery (more than 0.5 s) can lead to accidents [3]. Besides efficiency, it’s also crucial to protect user privacy by keeping vehicle identities and travel routes anonymous, shielding them from potential attackers. For an AV, early authentication before joining a network is critical. A Central Authority (CA) should be responsible for this process. The vehicle sends a join request to the CA when it connects to a nearby Base Station Transceiver (BTS). The CA then verifies the authenticity of both the vehicle and the BTS before allowing the vehicle to connect. In Figure below, we explained the authentication architecture for AV in detail.

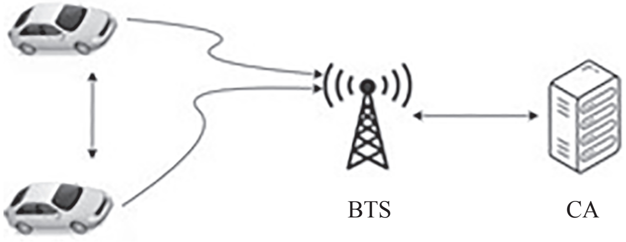

Figure. Authentication architecture for AV

While many existing privacy-preserving authentication systems focus on verifying message validity, they often fall short in verifying user legitimacy, leaving them open to active attacks [4–6]. Additionally, the high computational demands of these methods, which frequently rely on bilinear pairings and scalar multiplications, make them impractical for resource-limited vehicle environments. To tackle these issues, we introduce a new, lightweight, and anonymous authentication protocol tailored for CAN environments. Our approach uses the Decisional Diffie-Hellman (DDH) assumption to enhance both security and computational efficiency. Unlike prior methods, our protocol ensures that vehicles are authenticated before joining the network, while also verifying the integrity of transmitted data. By using dynamically generated login identities, it preserves anonymity and prevents attackers from linking real identities to vehicles. Moreover, our protocol features a password change mechanism that doesn’t depend on a CA or third-party servers, making it resistant to offline password guessing attacks. We also provide a formal security analysis using Burrows-Abadi-Needham (BAN) logic, demonstrating that our protocol is secure under the DDH assumption.

Our performance evaluation shows that this protocol significantly reduces computational costs compared to existing approaches. In this paper, we define efficiency through measurable metrics, such as the number of cryptographic operations (e.g., exponentiation, hash, exclusive OR), total protocol execution time (in milliseconds), and reduced communication overhead. This definition provides a clear and quantifiable basis for evaluating the effectiveness of our proposed solution.

Related Work

Authentication in AV is a key area of research due to the security and privacy risks in vehicle communication [7]. In recent years, various protocols have been developed to improve user security and privacy while maintaining the efficiency required for real-time vehicle operations. Several privacy-preserving authentication schemes for Vehicular Ad Hoc Networks (VANETs) have been designed to protect user identities and secure communications.

Ying et al. [8] introduced a lightweight protocol called Anonymous and lightweight authentication scheme Smart Card (ASC) for securing vehicular networks. While it offers efficient authentication and privacy, later research [9] exposed its vulnerability to offline impersonation and location spoofing attacks. This underscores the need for protocols that not only offer basic security but also resist a wider range of attacks. Lee et al. [10] developed a honey list-based authentication protocol that strengthens VANET security by using deception techniques to counter brute-force password guessing and impersonation attempts. It uses mock credentials alongside real ones, and if an attacker uses false credentials, the system triggers an alert to detect malicious activity quickly.

Li et al. [11] presented a privacy-preserving authentication scheme focused on explainability, ensuring legitimate users aren't falsely accused of wrongdoing. Using elliptic curve cryptography and group signatures, it balances computational efficiency with privacy, protecting vehicle identities and messages while maintaining performance. Parmar et al. [12] introduced a privacy-preserving authentication scheme using blockchain technology, shifting from traditional centralized models to a decentralized approach. Blockchain immutable ledger improves security and privacy, preventing attacks like message tampering and replay attacks, while eliminating the risk of single-point failures.

Vasudev et al. [13] proposed a lightweight mutual authentication protocol for Vehicle-to-Vehicle communication in the Internet of Vehicles, aiming to reduce computational overhead. Their protocol focuses on efficient mutual authentication without relying heavily on resource-intensive cryptography, making it suitable for real-time environments like smart cities. For CAN, there is increasing concern about the lack of secure and simple authentication methods. CAN systems are sensitive to message delays, and many existing protocols are not suitable for such environments. Some proposed solutions use lightweight cryptographic operations, such as hash functions and symmetric encryption, to reduce computation costs, but they often compromise anonymity or fail to handle dynamic identities effectively [14].

To address these limitations, we are exploring advanced cryptographic methods, such as the DDH assumption, to improve the efficiency and security of CAN authentication protocols. Formal security analysis using BAN logic [15] is also important for proving robustness against attacks like replay, impersonation, and man-in-the-middle. Despite these advancements, there is still a need for a straightforward authentication protocol that addresses security and privacy concerns while minimizing computational costs and ensuring anonymity in CAN environments. Our protocol aims to fill this gap by leveraging DDH for improved security and using dynamically generated login identities to ensure anonymity, without relying on a trusted third party.

Proposed Model and Assumptions

Let G be a finite cyclic group of prime number p that is created by the function g. The elements of G are represented as $g^n \bmod p$, where $n \in [1, p - 1]$, and the operation within the group is multiplication modulo p. Rather than relying on computations within cyclic groups for the Computational Diffie–Hellman (CDH) or Discrete Logarithm assumptions, we employed the DDH assumption. The DDH problem is concerned with distinguishing between two types of tuples in group G. Given three elements $g^a \bmod p$, $g^b \bmod p$, and $g^c \bmod p$, (where $a, b, c \in [1, p - 1]$), the task is to decide whether $c = a \cdot b$ (i.e., whether the third element is equal to $g^{ab} \bmod p$) or whether c is a random value in G.

In other words, the DDH assumption asserts that given the tuple (g, g^a, g^b, g^c), it is computationally hard to distinguish whether g^c is the result of g^{ab} whether c is a random value in the group. This makes DDH a decision problem, as opposed to the CDH problem previously used technique for proposing the authentication protocol which focuses on calculating $g^{ab} \bmod p$ directly. In terms of securing the AV, the three important components are: first is the Vehicle (V_i) itself, second is the BTS, and the third one is the CA which have authenticated the legitimate user. Table 1 below describes the key notations used within this paper.

Proposed Protocol

The five phases of our proposed authentication system are: user registration, user login, user authentication, password change, and data authentication. Before a user can access the network, their smart cards are assigned to them in the user registration step. While the password update phase ensures resilience to offline password guessing attacks, the user login and authentication phases serve to verify the legitimacy of users. In the data authentication phase, messages between vehicles are verified. The following subsections contain the details of the protocol. Please note that timestamps are used in the attached messages to reduce

Table 1. List of Used Notations

Notation	Description
G	Finite cyclic group under multiplicative operation
x	Private key of the CA
H_0, H_1, H_2, H_3	Cryptographic hash functions
n_i	Random number generated by the user V_i
ID_{V_i}	Identity of vehicle
PW_i	Password of the user
N_i	Hash value derived from PW_i and n_i
r_{CA}	Random value generated by the CA
C_{CA}	Challenge generated by the CA
C_{V_i}	Response from the user V_i
T_{update}	Timestamp for password update
T_{msg}	Timestamp for message freshness
M	Message exchanged between vehicles

replay attacks and check the relevance of the semantic content.

User Registration Phase

Assume that $G = \langle g \rangle$ is a finite cyclic group with order p under multiplicative operations, where g is the group generator and p is a prime number. We use hash functions H_i ($i = 0, 1, 2, 3$) that map from $\{0, 1\}^*$ to $\{0, 1\}^{l_i}$, where l_i is the length of the outputs of the hash functions.

Let (x, $y = g^x \bmod p$) be the private key and public key pair of the CA, where x is the CA private key, and $y = g^x \bmod p$ is the public key. A vehicular user V_i must register before accessing the network for the first time. The vehicle V_i must pass through the below steps:

— Firstly, after generating a random number n_i, the user V_i submits their identity ID_{V_i} and $H_0(PW_i \| n_i)$ to the CA via a secure channel;

— Secondly, the user's identity and timestamp T_{reg} are stored by the CA when it receives the registration request at T_{reg}, and computes the following:

$$PV_{ID_{V_i}} = H_0(ID_{V_i}),\ A_i = H_0(H_0(PW_i \| n_i) \| PV_{ID_{V_i}}),$$

$$N_i = H_0(PW_i \| n_i) \oplus H_0(x \| PV_{ID_{V_i}} \| T_{reg}).$$

After passing through these steps, the CA then assigns the smart card to V_i which contains the necessary parameters for future authentication. An attacker cannot readily guess the right password since it is protected by the random integer n_i and the one-way hash function $H_0(\cdot)$, which mitigates insider attacks.

User Login Phase

In the user login phase, a user V_i who holds a smart card needs to authenticate their credentials with the CA before accessing the network. Let g be the generator of a cyclic group G of prime order p, with $y = g^x \bmod p$ as the public key of CA (where x is the private key).

— The user inserts their smart card and inputs their password PW_i. The smart card calculates, $N_i =$ $= H_0(PW_i \| n_i)$, where n_i is a random number stored in the smart card.

— The smart card generates a fresh random number $r_i \in [1, p - 1]$ and computes g^{r_i}. This is sent along with ID_{V_i} to the CA.

— Upon receiving this, the CA checks the validity of ID_{V_i}. It then generates its own random value $r_{CA} \in [1, p - 1]$ and computes $g^{r_{CA}} \bmod p$.

— The CA computes $H_0(x \| PV_{ID_{V_i}})$, retrieves the stored values for V_i, and sends a challenge C_{CA} and $g^{r_{CA}} \bmod p$ to the user.

User Authentication Phase

In this phase, the user V_i must prove their legitimacy based on the challenge received from CA.

Step 1. Upon receiving $g^{r_{CA}} \bmod p$ and the challenge C_{CA}, the smart card computes $g^{r_{CA} r_i} \bmod p$. Under the DDH assumption, an adversary cannot distinguish between this Diffie–Hellman shared key and a random element, ensuring security.

Step 2. The smart card generates a response $C_{V_i} =$ $= H_1(g^{r_{CA} r_i} \| N_i \| T_{login})$, where T_{login} is the timestamp of the login request. The response C_{V_i} and timestamp T_{login} are sent back to the CA.

Step 3. The CA computes the same value $g^{r_{CA} r_i} \bmod p$ and verifies the response C_{V_i} against its own calculation of $H_1(g^{r_{CA} r_i} \| N_i \| T_{login})$. If they match, V_i is authenticated.

Password Change Phase

The password change phase is intended to allow users to update their password without directly involving the certification authority. This phase ensures that password guessing attacks are prevented and is secured using the DDH assumption.

Step 1. The user V_i, after authenticating themselves, decides to change the password PW_i. The user generates a new random number n'_i and calculates the new password hash $H_0(PW_i \| n'_i)$.

Step 2. The smart card stores this new value and updates the associated parameters $N'_i = H_0(PW'_i \| n'_i) \oplus$ $\oplus H_0(x \| PV_{ID_{V_i}} \| T_{update})$, where T_{update} is the current timestamp.

Step 3. The new password is now used for future login attempts, with the security of the DDH assumption ensuring that an attacker cannot calculate the new password even if they observe the password change process.

Data Authentication Phase

The data authentication phase ensures that messages exchanged between vehicles are authentic and have not been tampered with. This phase is crucial to prevent replay attacks, message forgery and ensure data integrity.

Step 1. Vehicle V_i generates a new message M to send to vehicle V_j. The message includes a fresh timestamp T_{msg} and a hash $H_2(M \| T_{msg} \| N_i)$ for integrity protection.

Step 2. The message M, the hash, and the timestamp are sent to V_j. Once received, V_j checks the timestamp to ensure the freshness of the message and calculates the hash using N_i, known to it from previous authentication phases.

Step 3. If the calculated hash matches the received hash, the message is accepted as authentic. The DDH assumption secures this phase by ensuring that, even if adversaries observe the values exchanged, they cannot infer sensitive information or forge messages.

Formal Security Proof

BAN logic is a well-known modal logic framework used to verify the correctness of cryptographic protocols by analyzing their security properties. It serves as a formal method for assessing whether the goals of authentication protocols are achieved. The process of BAN logic involves four key steps: idealizing the protocol, specifying the assumptions, identifying the security objectives, and finally deriving conclusions based on the logic inference rules. In our work, we apply BAN logic to evaluate the security of our proposed protocol.

1. Notations of BAN Logic. The main notations used in BAN logic that defines beliefs and assertions [15] are listed in our Notation Table 2.

In the Table 2 presented, in accordance with [15], P and Q denote entities and X denotes information.

2. Initial Assumptions. Before the analysis begins, we make the following assumptions:

$V_i \equiv (\mathrm{CA} \leftrightarrow V_i)$,

$\mathrm{CA} \equiv (V_i \leftrightarrow \mathrm{CA})$.

Table 2. BAN Logic Notations

Notation	Description
P believes X: $P \equiv X$	Statement X is believed by entity P
P sees X: $P \lhd X$	Statement X has been received by Entity P
P once said X: $P \sim X$	At some point, entity P sent a message that included X
P controls X: $P \Rightarrow X$	Entity P can verify the legitimacy of X and has jurisdiction over it
Fresh(X): $\#(X)$	The message X is fresh
$P \leftrightarrow Q$	Entities P and Q share a secure key for communication

In the user Registration phase, the user V_i and the CA share a common secret key established during the registration.

$V_i \equiv (V_i \leftrightarrow \text{CA})$,

$V_i \lhd M$.

In user Login phase, the user V_i believes that the message M received from the CA is fresh.

$\text{CA} \equiv \#(T_{login})$.

In user Authentication phase, the CA believes the timestamp T_{login} is fresh and the user is authenticated.

3. Protocol Proof using BAN Logic. We demonstrate that the suggested approach can accomplish mutual authentication securely by using BAN logic rules, considering the aforementioned assumptions and security goals. The concrete steps are listed as follows:

User Registration Phase

The BAN logic assumption is that the user V_i receives a smart card with credentials, and the user believes that the CA has authenticated them.

$V_i \equiv (\text{CA} \equiv V_i)$,

$V_i \equiv (\text{CA} \leftrightarrow V_i)$.

This indicates that the user perceives that the CA has verified their legitimacy and has shared a key for communication.

User Login Phase

In this phase, the user sends a message to the CA. The assumptions we can make are:

$\text{CA} \equiv \#(T_{login})$,

$\text{CA} \equiv V_i \leftrightarrow \text{CA}$.

The CA believes the login message with T_{login} is fresh, meaning it hasn't been replayed. After receiving the response from the CA, the user believes the CA authenticated them.

$V_i \equiv \#(T_{login})$,

$V_i \equiv (\text{CA} \leftrightarrow V_i)$.

The user believes the CA is fresh and trusts communication.

User Authentication Phase

After receiving the challenge from the CA, the user V_i replies with C_{V_i}. Here, both the user and CA believe the session is secure.

$\text{CA} \equiv \#(T_{login})$.

The CA believes the timestamp T_{login} is fresh, validating the session.

$V_i \equiv (\text{CA} \leftrightarrow V_i)$.

The user trusts that the CA is secure.

Password Change Phase

This step makes sure the user may modify their password independently of the CA.

$V_i \equiv (V_i \leftrightarrow \text{CA})$.

The user believes that the password change is valid.

Data Authentication Phase

In this phase, vehicles authenticate messages among themselves. The assumption is:

$V_i \equiv (V_j \leftrightarrow V_i)$.

Vehicle V_i believes that V_j (another vehicle) is sending authenticated data.

$V_i \equiv \#(T_{msg})$.

V_i believes the message timestamp T_{msg} is fresh and that the message has not been replayed.

At the end of the analysis, all the protocol goals are met, the user V_i believes they are authenticated by the CA, also the messages sent between vehicles are authenticated and trusted and the timestamps ensure that replay attacks are mitigated.

Performance Analysis

In this section, we analyze the computational cost of the proposed authentication protocol, comparing it with previous protocols from the literature, specifically those outlined in Ying et al. [8] and other relevant works. The computational efficiency of cryptographic operations is critical in AV environments. For this reason, we define efficiency by assessing

— the execution time of cryptographic primitives,

— the number of operations per protocol phase, and

— the total latency incurred by authentication and data exchange.

These metrics allow for a concrete comparison of the computational burden across different schemes.

Compared to the work of Ying et al. [8], which employed the CDH assumption and had a higher computational cost due to the number of hash function operations (t_h) and modular exponential operations (t_e), our protocol, based on the DDH assumption, reduces the total number of costly operations. In our implementation[1], hash function operation requires 0.00074 ms, modular exponential operation requires 0.45 ms, and XOR operation (t_x) requires 0.0002 ms. Ying et al. [8] had a total computational cost of 1.608 ms, largely due to the increased number of exponentiations. While our protocol reduces this by minimizing the number of modular exponentiations and focusing on lighter hash and XOR operations, achieving a computational cost of 0.90908 ms, a reduction from all previously available protocols.

For a better comparison we used the same parameters taken by Mun et al. [16], Zhao et al. [17], Ying et al. [8], and Cui et al. [18] in their articles. For a better understanding of the computational cost for all the previously available studies with our study, we illustrated all the results in Table 3 below.

[1] Crypto++ 5.6.0 Benchmarks. Available at: http://www.cryptopp.com/benchmarks.html (accessed: 20.03.2025).

Table 3. Comparison for the computational cost for different protocols

Protocol	Computational Cost	Time, ms
Mun et al. [16]	$2t_{asm} + 12t_h$	3.088
Zhao et al. [17]	$8t_{mu} + 11t_h + 2t_{e/d} + 2t_s$	9.308
Ying et al. [8]	$2t_e + 11t_h + t_{e/d}$	1.608
Cui et al. [18]	$35t_h + 4t_{mu} + 1t_{fe}$	1.047
Our Protocol	$2t_e + 12t_h + 2t_x$	0.909

Conclusion

In this paper, we presented a lightweight and efficient authentication protocol for vehicular networks, designed to balance security and performance under the Decisional Diffie–Hellman assumption. Our main goal was to reduce computational effort while maintaining strong security against common vehicular network attacks, such as replay, identity theft, and offline password guessing.

The proposed protocol significantly lowers computational costs compared to earlier schemes based on the Computational Diffie–Hellman assumption. Our performance analysis shows that the total computational time for our protocol is approximately 0.90908 ms, making it highly suitable for real-time applications in Autonomous Vehicles (AVs), where both low latency and high security are critical. Additionally, we used Burrows-Abadi-Needham logic to formally verify that the protocol achieves key security properties, including mutual authentication and message integrity. By reducing computational complexity without sacrificing security, this protocol offers an ideal solution for real-world deployment in AV environments.

In future work, we plan to extend the protocol with advanced features such as blockchain integration. While our current approach uses centralized architecture via a trusted Central Authority, which ensures fast and efficient authentication in well-connected environments, we recognize the limitations of such models. Centralized systems can be susceptible to availability or integrity attacks due to single points of failure. In contrast, decentralized (e.g., blockchain-based or multi-agent) models offer improved resilience and may be better suited for distributed, infrastructure-independent vehicle networks. Future extensions of this work will explore hybrid authentication models that combine the efficiency of centralization with the robustness of decentralized approaches.

References

1. Miller J. Vehicle-to-vehicle-to-infrastructure (V2V2I) intelligent transportation system architecture. *Proc. of the IEEE Intelligent Vehicles Symposium*, 2008, pp. 715–720. https://doi.org/10.1109/ivs.2008.4621301
2. Bagga P., Das A.K., Wazid M., Rodrigues J.J.P.C., Park Y. Authentication protocols in Internet of Vehicles: taxonomy, analysis, and challenges. *IEEE Access*, 2020, vol. 8, pp. 54314–54344. https://doi.org/10.1109/ACCESS.2020.2981397
3. Cheng X., Yang L., Shen X. D2D for intelligent transportation systems: a feasibility study. *IEEE Transactions on Intelligent Transportation Systems*, 2015, vol. 16, no. 4, pp. 1784–1793. https://doi.org/10.1109/TITS.2014.2377074
4. Lo N.-W., Tsai J.-L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. *IEEE Transactions on Intelligent Transportation Systems*, 2016, vol. 17, no. 5. pp. 1319–1328. https://doi.org/10.1109/TITS.2015.2502322
5. Nandy T., Idris M.Y.I., Noor R.M., Wahab A.W.A., Bhattacharyya S., Kolandaisamy R., Yahuza M. A secure, privacy-preserving, and lightweight authentication scheme for VANETs. *IEEE Sensors Journal*, 2021, vol. 21, no. 18, pp. 20998–21011. https://doi.org/10.1109/JSEN.2021.3097172
6. Manivannan D., Moni S.S., Zeadally S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). *Vehicular Communications*, 2020, vol. 25, pp. 100247. https://doi.org/10.1016/j.vehcom.2020.100247
7. Jan S.A., Amin N.U., Othman M., Ali M., Umar A.I., Basir A. A survey on privacy-preserving authentication schemes in VANETs: attacks, challenges and open issues. *IEEE Access*, 2021, vol. 9, pp. 153701–153726. https://doi.org/10.1109/ACCESS.2021.3125521
8. Ying B., Nayak A. Anonymous and lightweight authentication for secure vehicular networks. *IEEE Transactions on Vehicular Technology*, 2017, vol. 66, no. 12, pp. 10626–10636. https://doi.org/10.1109/TVT.2017.2744182
9. Saxena N., Choi B.J., Cho S. Lightweight privacy-preserving authentication scheme for V2G networks in the smart grid. *Proc. of the IEEE Trustcom/BigDataSE/ISPA*, 2015, pp. 604–611. https://doi.org/10.1109/Trustcom.2015.425
10. Lee J., Kim G., Das A.K., Park Y. Secure and efficient honey list-based authentication protocol for Vehicular Ad Hoc Networks. *IEEE Transactions on Network Science and Engineering*, 2021,

Литература

1. Miller J. Vehicle-to-vehicle-to-infrastructure (V2V2I) intelligent transportation system architecture // Proc. of the IEEE Intelligent Vehicles Symposium. 2008. P. 715–720. https://doi.org/10.1109/ivs.2008.4621301
2. Bagga P., Das A.K., Wazid M., Rodrigues J.J.P.C., Park Y. Authentication protocols in Internet of Vehicles: taxonomy, analysis, and challenges // IEEE Access. 2020. V. 8. P. 54314–54344. https://doi.org/10.1109/ACCESS.2020.2981397
3. Cheng X., Yang L., Shen X. D2D for intelligent transportation systems: a feasibility study // IEEE Transactions on Intelligent Transportation Systems. 2015. V. 16. N 4. P. 1784–1793. https://doi.org/10.1109/TITS.2014.2377074
4. Lo N.-W., Tsai J.-L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings // IEEE Transactions on Intelligent Transportation Systems. 2016. V. 17. N 5. P. 1319–1328. https://doi.org/10.1109/TITS.2015.2502322
5. Nandy T., Idris M.Y.I., Noor R.M., Wahab A.W.A., Bhattacharyya S., Kolandaisamy R., Yahuza M. A secure, privacy-preserving, and lightweight authentication scheme for VANETs // IEEE Sensors Journal. 2021. V. 21. N 18. P. 20998–21011. https://doi.org/10.1109/JSEN.2021.3097172
6. Manivannan D., Moni S.S., Zeadally S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs) // Vehicular Communications. 2020. V. 25. P. 100247. https://doi.org/10.1016/j.vehcom.2020.100247
7. Jan S.A., Amin N.U., Othman M., Ali M., Umar A.I., Basir A. A survey on privacy-preserving authentication schemes in VANETs: attacks, challenges and open issues // IEEE Access. 2021. V. 9. P. 153701–153726. https://doi.org/10.1109/ACCESS.2021.3125521
8. Ying B., Nayak A. Anonymous and lightweight authentication for secure vehicular networks // IEEE Transactions on Vehicular Technology. 2017. V. 66. N 12. P. 10626–10636. https://doi.org/10.1109/TVT.2017.2744182
9. Saxena N., Choi B.J., Cho S. Lightweight privacy-preserving authentication scheme for V2G networks in the smart grid // Proc. of the IEEE Trustcom/BigDataSE/ISPA. 2015. P. 604–611. https://doi.org/10.1109/Trustcom.2015.425
10. Lee J., Kim G., Das A.K., Park Y. Secure and efficient honey list-based authentication protocol for Vehicular Ad Hoc Networks // IEEE Transactions on Network Science and Engineering. 2021. V. 8. N 3. P. 2412–2425. https://doi.org/10.1109/TNSE.2021.3093435

vol. 8, no. 3, pp. 2412–2425. https://doi.org/10.1109/TNSE.2021.3093435

11. Li S., Yang R., Chen J. A privacy-preserving authentication scheme for VANETs with exculpability. *Security and Communication Networks*, 2023, vol. 2023, no. 1, pp. 8676929. https://doi.org/10.1155/2023/8676929
12. Parmar K., Patil S., Patel D., Patel V., Parikh B., Padaria P. Privacy-preserving authentication scheme for VANETs using blockchain technology. *Procedia Computer Science*, 2023, vol. 220, pp. 40–47. https://doi.org/10.1016/j.procs.2023.03.008
13. Vasudev H., Deshpande V., Das D., Das S.K. A lightweight mutual authentication protocol for V2V communication in internet of vehicles. *IEEE Transactions on Vehicular Technology*, 2020, vol. 69, no. 6, pp. 6709–6717. https://doi.org/10.1109/TVT.2020.2986585
14. Zhou L., Chao H.C. Multimedia traffic security architecture for the internet of things. *IEEE Network*, 2011, vol. 25, no. 3, pp. 35–40. https://doi.org/10.1109/MNET.2011.5772059
15. Burrows M., Abadi M., Needham R. A logic of authentication. *ACM Transactions on Computer Systems*, 1990, vol. 8, no. 1, pp. 18–36. https://doi.org/10.1145/77648.77649
16. Mun H., Han K., Lee Y.S., Yeun C.Y., Choi H.H. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Mathematical and Computer Modelling*, 2012, vol. 55, no. 1–2, pp. 214–222. https://doi.org/10.1016/j.mcm.2011.04.036
17. Zhao D., Peng H., Li L., Yang Y. A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications*, 2014, vol. 78, no. 1, pp. 247–269. https://doi.org/10.1007/s11277-014-1750-y
18. Cui J., Yu J., Zhong H., Wei L., Liu L. Chaotic map-based authentication scheme using physical unclonable function for internet of autonomous vehicle. *IEEE Transactions on Intelligent Transportation Systems*, 2023, vol. 24, no. 3, pp. 3167–3181. https://doi.org/10.1109/TITS.2022.3227949

11. Li S., Yang R., Chen J. A privacy-preserving authentication scheme for VANETs with exculpability // Security and Communication Networks. 2023. V. 2023. N 1. P. 8676929. https://doi.org/10.1155/2023/8676929
12. Parmar K., Patil S., Patel D., Patel V., Parikh B., Padaria P. Privacy-preserving authentication scheme for VANETs using blockchain technology // Procedia Computer Science. 2023. V. 220. P. 40–47. https://doi.org/10.1016/j.procs.2023.03.008
13. Vasudev H., Deshpande V., Das D., Das S.K. A lightweight mutual authentication protocol for V2V communication in internet of vehicles // IEEE Transactions on Vehicular Technology. 2020. V. 69. N 6. P. 6709–6717. https://doi.org/10.1109/TVT.2020.2986585
14. Zhou L., Chao H.C. Multimedia traffic security architecture for the internet of things // IEEE Network. 2011. V. 25. N 3. P. 35–40. https://doi.org/10.1109/MNET.2011.5772059
15. Burrows M., Abadi M., Needham R. A logic of authentication // ACM Transactions on Computer Systems. 1990. V. 8. N 1. P. 18–36. https://doi.org/10.1145/77648.77649
16. Mun H., Han K., Lee Y.S., Yeun C.Y., Choi H.H. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks // Mathematical and Computer Modelling. 2012. V. 55. N 1–2. P. 214–222. https://doi.org/10.1016/j.mcm.2011.04.036
17. Zhao D., Peng H., Li L., Yang Y. A secure and effective anonymous authentication scheme for roaming service in global mobility networks // Wireless Personal Communications. 2014. V. 78. N 1. P. 247–269. https://doi.org/10.1007/s11277-014-1750-y
18. Cui J., Yu J., Zhong H., Wei L., Liu L. Chaotic map-based authentication scheme using physical unclonable function for internet of autonomous vehicle // IEEE Transactions on Intelligent Transportation Systems. 2023. V. 24. N 3. P. 3167–3181. https://doi.org/10.1109/TITS.2022.3227949

Authors

Muhammad Salman Saeed — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation, sc 57886147100, https://orcid.org/0009-0006-1425-4863, salman.saeed@itmo.ru

Sergey V. Bezzateev — D.Sc., Associate Professor, Head of Department, Saint Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, 190000, Russian Federation; Director of Laboratory, ITMO University, Saint Petersburg, 197101, Russian Federation, sc 6602425996, https://orcid.org/0000-0002-0924-6221, bsv@guap.ru

Авторы

Саид Мухаммад Салман — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sc 57886147100, https://orcid.org/0009-0006-1425-4863, salman.saeed@itmo.ru

Беззатеев Сергей Валентинович — доктор технических наук, доцент, заведующий кафедрой, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация; директор лаборатории, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sc 6602425996, https://orcid.org/0000-0002-0924-6221, bsv@guap.ru

Received 13.04.2025
Approved after reviewing 01.07.2025
Accepted 22.07.2025

Статья поступила в редакцию 13.04.2025
Одобрена после рецензирования 01.07.2025
Принята к печати 22.07.2025