LAIOV-5G: LIGHTWEIGHT AUTHENTICATION SCHEME FOR IOV BASED ON 5G TECHNOLOGY IN SMART-CITY ENVIRONMENT

Murtadha A. Alazzawi[1], Saad Ali Alfadhli[1], Ahmed Al-Shammari[2], Zaid Ameen Abduljabbar[3] and Vincent Omollo Nyangaresi[4]

(Received: 12-Oct.-2024, Revised: 3-Dec.-2024, Accepted: 6-Dec.-2024)

ABSTRACT

The Fifth Generation (5G) networks have enabled the development of smart cities, in which massive amounts of data are collected, stored and disseminated. The ultimate objective of these smart cities is to cut costs and improve security performance. In this environment, Internet of Vehicles (IoV) helps connect vehicles, pedestrians, control rooms and some roadside infrastructure. Owing to the insecure nature of the communication channel utilized in IoV to exchange information, it is important to develop practical techniques to preserve data confidentiality and privacy. To this end, numerous security solutions have been proposed over the recent past. Unfortunately, most of these authentication techniques have security flaws, which endangers the transmitted data, while some of them are highly inefficient. To address these gaps, we present a Lightweight Authentication Scheme for the Internet of Vehicles (IoV) based on 5G technology (LAIOV-5G).The security analysis carried out demonstrates that LAIOV-5G mitigates numerous potential attacks that threaten the IoV communication in a smart-city environment. In addition, the performance analysis of LAIOV-5G verifies its effectiveness and efficiency.

KEYWORDS

Authentication, 5G, Security, VANETs, Smart City.

1. INTRODUCTION

The Internet of Things (IoT) encompasses modern wireless technologies or applications that sense, process, manage and control large volumes of data used for service or application-level enhancements [1]. These advancements are not just theoretical, but they have a direct impact on our daily lives. For instance, the smart-city applications, such as smart homes, IoV, Intelligent Transportation System (ITS) and smart industrial manufacturing, have facilitated scalable and efficient information exchanges that meet various domain requirements [2]-[3]. As explained in [4], a real-time IoV computing environment has been facilitated by the exponential growth of today's automotive technologies, combining numerous approaches, like IoV, VANETs and cloud. This helps address a variety of challenges that may arise on roadways due to congestions and other traffic-related concerns [4]. This practical application of IoT in addressing real-world problems underscores its relevance and importance.

The increasing integration of IoT into smart cities has revealed new possibilities for enhancing efficiency and productivity in various areas, such as intelligent transportation systems, critical infrastructure management and industrial automation [5]-[7]. Among all these technologies, IoT has emerged as a crucial enabler for services, such as real-time traffic control, accident-avoidance mechanisms and vehicle-to-infrastructure (V2I) communication. However, these developments pose significant security hurdles, such as protecting confidential information, ensuring communication integrity and thwarting unauthorized access. This investigation addresses these hurdles by proposing a simplified authentication scheme specifically designed for IoV networks based on 5G technology. By leveraging fast data-transfer speeds, reduced latency and improved reliability of 5G technology, this scheme offers a robust and effective answer for secure and seamless connectivity in smart urban environments [8]-[9].

1. M. A. Alazzawi and S. A. Alfadhli are with Department of Computer Techniques Engineering, Imam Alkadhim University College (IKU), 10001, Baghdad, Iraq. Emails: murtadhaali@alkadhum-col.edu.iq and Saadali@alkadhum-col.edu.iq
2. A. Al-Shammari is with Department of Computer Science, College of Computer Science and Information Technology, University of Al-Qadisiyah, Al Diwaniyah, 58002, Iraq. Email: ahmed.alshammari@qu.edu.iq
3. Z. A. Abduljabbar is with Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq and with Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen, China. Email: zaid.ameen@uobasrah.edu.iq
4. V. O. Nyangaresi is with Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga Uni. of Science & Technology, Bondo, Kenya and with Department of Applied Electronics, Saveetha School of Eng., SIMATS, Chennai, Tami lnadu, India. Email: vnyangaresi@jooust.ac.ke

Recently, the rise in vehicle production has made IoV the longest-lasting technical trend in the world today [10]. With IoV, a self-organized network may be formed and messages can be broadcast to the moving vehicles. It offers several advantages, exampled by integrated warning systems which alert drivers about accidents. Afterwards, drivers may make decisions quickly depending on the information provided. Still, the accuracy and safety of self-driving cars could be increased by sharing more complex information among them [11]. However, if there is no substantial security and privacy protection in place, adversaries can quickly access sensitive and private information belonging to car users [12]. Apart from privacy issues, data authenticity and integrity are other important security topics in IoV. For instance, malicious IoV entities can forward false information to human drivers or self-deriving cars, which can result in wrong judgments and decisions. Ultimately, this can lead to tragic events, such as serious road accidents that result in loss of lives. It is also possible for malicious entities to infiltrate IoV networks in order to carry out terrorist attacks. Moreover, falsified information may lure customers to dangerous zones or rival parking lots where evils, such as kidnapping, can be executed. This potential misuse of IoV underscores the need for robust security measures. As discussed in [13]-[15], significant investments in wireless-communication technologies has led to the development of 5G networks. In these networks, mobile data rates can be increased 1000 folds, resulting in transmission rates of up to 10 Gbps. As such, 5G networks have increased speeds compared to their predecessors, such as the Fourth-Generation (4G) networks. Moreover, 5G networks have reduced latencies and increased efficiency, which improves the battery life of their network elements. This helps in creating a conducive environment for the deployment of many battery-powered devices in the IoT [16].

Motivated by the inefficiency and security vulnerabilities of most existing authentication schemes, we propose a lightweight authentication technique for 5G-based IoV networks in a smart-city environment. The proposed LAIoV-5G scheme solves the security challenges by introducing a lightweight authentication scheme specifically designed for 5G-based IoV. By leveraging high data transfer rates of 5G, reducing latency and improving reliability, the LAIoV-5G scheme provides a robust solution for secure and efficient communications in smart-city environments. The proposed LAIoV-5G scheme aims to improve security, privacy and resilience against potential attacks, through reliable authentication across full assessments. Specifically, the major contributions of our work are as follows:

- The authentication method is developed based on a lightweight and secure cryptographic primitive; namely, ECC, hash function and timestamp to make the source-authentication process secure and efficient. In fact, a two-factor authentication mechanism is presented that is lightweight, efficient, dependable and secure for IoV applications in a smart-city environment.
- We have designed LAIoV-5G scheme to be extremely lightweight, ensuring its high performance in the IoV system. The improved security performance of our proposed LAIoV-5G scheme is crucial for the IoV in which communications take place over insecure communication media.
- We have conducted a comprehensive evaluation of the resistance of our proposed LAIoV-5G scheme to various security intrusions. The results indicate that LAIoV-5G scheme has robust security features.

The rest of this work is structured as follows: Section 2 describes some of related works in this domain while Section 3 presents a background of lightweight authentication schemes, which is followed by the proposed LAIoV-5G scheme in Section 4. Section 5 presents the security analysis. Section 6 discusses the performance analysis. The paper is finally concluded in Section 7.

2. RELATED WORK

This section explores the IoV studies based on 5G technology. IoV, compared to conventional wireless networks, presents a host of technical and security obstacles [17]. For instance, issues such as privacy, key distribution, bootstrap, mobility, incentives and poor error tolerance are yet to be addressed. Therefore, both industry and academia have developed several methods to protect privacy and ensure the authenticity of vehicle users in response to these challenges. For instance, Public Key Infrastructure (PKI) has been developed to facilitate key distribution and mutual authentication across IoV users [18]-[24]. In 2005, authentication schemes have been presented in [18] and [19]. In these two protocols, vehicle location and public-key signatures are utilized to prevent attackers waiting on the side of the road from pretending to be an authorized vehicle user on a highway. However, the deployed PKI makes these schemes inefficient, especially in dense IoV networks. In addition, large storage is required for storage of these public-key signatures. To address some of these concerns, hash chain-based authentication mechanisms are developed in [20]-[22]. However, user anonymity is not provided in these schemes and hence, attackers can obtain sensitive driver information, such as registration plates and driver identities. To address this concern, anonymous authentication techniques have been suggested in [23] and [24]. In these schemes, unique pseudo-identities are deployed to conceal true identities and hence mitigate privacy leakage. Here, only the trusted authority (TA) can recover the true identities from these pseudo-identifications.

When it comes to high density of vehicle populations, the task of gathering and storing traffic-related data becomes complex. To tackle this issue, several strategies have been suggested for integrating cloud computing into automotive networks. Basically, the cloud allows vehicles to share resources, like storage, computation and bandwidth. As seen in [25]-[27], these strategies comprise of center, vehicular and roadside clouds. These three clouds have diverse considerations. For instance, the authors in [25] have incorporated autonomous vehicular clouds to utilize unused resources. On the other hand, the platform as a service cloud platform has been incorporated for interactive, mobile and functional clients in [26]. However, the IoV clouds in [27] have been classified as being hybrid vehicular clouds (HVCs), vehicular clouds (VCs) or vehicle-utilizing clouds (VuCs). The unique nature of these solutions emanate from the fact that vehicles can act as cloud service providers (for VCs), customers (for VuCs) and both customers and cloud service providers (for HVCs).

Recent research works in [28]–[33] have proposed authentication techniques to address vehicle networks' privacy and security aspects. In addition, identity-based methods [28]–[34] have been developed to leverage on Bilinear Pair (BP)-related cryptographic procedures for message signing and signature validation. However, BP procedures are computationally extensive. In addition, signature signing and validation require heavy computations and message exchanges. To address these issues, an Elliptic Curve Cryptography (ECC) and identity-based approach is developed in [35]. Although this technique solves the high-computation problems in BP procedures, it has some performance challenges. For instance, as the number of participating nodes increases, the time consumption of ECC procedures also increases, highlighting the urgency of finding a solution. Similarly, several authentication systems based on ECC have been presented in [35]–[42] to address vehicular communication's privacy and security requirements. However, they face the same challenges as the ones in [35].

The most recent schemes utilize vehicle networks supported by 5G technologies [42]–[46] to eliminate the need for Roadside Units (RSUs). In essence, these schemes utilize a vehicle network provided by 5G technology, bypassing the involvement of RSUs in the authentication process. To establish a 5G-enabled vehicle network for RSUs, it is crucial to meticulously analyze and address several key concerns. The 5G wireless network, renowned for its efficiency, enables immediate and low-latency transmission of data, a vital feature for the Vehicle to Everything (V2X) protocol. Vehicles can seamlessly connect with RSUs and other vehicles using 5G modems, sensors and on-board units (OBUs). Relay stations play a pivotal role as intermediaries, facilitating communication between cars and the network backbone, a feature that enhances the network's capabilities. The core network, equipped with resources, efficiently manages data traffic, performs processing tasks and conducts analytics. These resources can be strategically located, either centrally or at the network's periphery. The access network, comprising 5G base stations, ensures comprehensive coverage to RSUs and cars.

Instead, LAIOV-5G leverages the transceiver circuit and algorithmic innovation to circumvent these limitations. In the field of large-scale IoT networks, LAIOV-5G provides lightweight, scalable and efficient authentication mechanisms by taking full advantage of emerging 5G network capabilities, such as ultra-low latency, high data-transfer rates and increased reliability. It is a fully digital scheme with limited computational cost for the authentication process, enhancing higher security features while reducing computational cost compared to existing schemes. This enables fast and secure authentication in real time, especially in dynamic situations, such as intelligent transportation systems (ITSs) and critical infrastructure management. Moreover, LAIOV-5G is specifically built to address the unique problems of smart-city settings, where millions of devices and vehicles must communicate securely and efficiently. The adoption of 5G technology enables the system to handle massive amounts of data and promotes seamless vehicle-to-infrastructure (V2I) communication, which is critical for applications, such as self-driving cars and intelligent traffic management. This makes LAIOV-5G not only more efficient, but also more versatile, as it can meet the security requirements of future IoV systems in smart cities.

3. BACKGROUND

In this part, we describe the network structure as well as the security goals of our LAIoV-5G scheme. Table 1 gives a brief description of all the notations used in our LAIoV-5G scheme.

Table 1. Symbols of the proposed work.

Notations	Definition
TA	Trusted Authority
V_i	Vehicle
SK_i	a shared session key
ID_v	Identity of vehicle
PW_i	Password
r_v	Random number
$\oplus$	Exclusive OR operation
SC_i	Smart card
K_s, K_p	Public and private keys
$\|$	String concatenation
$h_i()$	Cryptography hash function

3.1 Network Structure

This sub-section explains the three network components that make up the network structure of our proposed LAIoV-5G scheme. This includes the vehicles, 5G base station (5G-BS) and the trusted authority, TA. The components shown in Figure 1 are briefly described in the following steps [47].

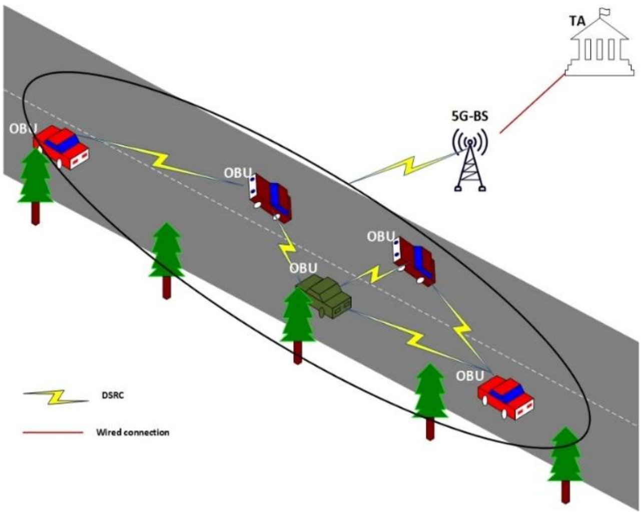

Figure 1. Network structure.

TA: This is a powerful computer system, which is a key player in 5G-enabled vehicular networks. It has a large storage capacity to store data. It also issue private keys for very matching vehicles as well as generating system parameters. To uphold network reliability, prevent single points of failure as well as network bottleneck, a number of redundant TAs are deployed in the IoV network.

5G-BS: This wireless-communication device is positioned at road intersections and other high-traffic areas. The 5G-BS transceiver has breakneck transmission speeds and wide-area coverage. To prevent attacks, this **5G-BS** is properly safeguarded, for instance, by the use of layered security architecture. It basically acts as an intermediary between the network nodes (vehicles) and the trusted authority, TA. Due to the nature of the processing that it carries out, this **5G-BS** is equipped with large storage, which is necessary during its verification procedures.

Vehicle: To facilitate the exchange of traffic-related data in IoV, each vehicle is equipped with an On-Board Unit (OBU). In an effort to prevent unauthorized access, modifications and other attacks, each OBU incorporates a Tamper-Proof Device (TPD). This helps safeguard essential data received from TA and other network elements.

3.2 Threat Model

In this sub-section, we model the attacker to have a range of capabilities that can be used in the process of trying to compromise the proposed scheme. Here, the adversary poses the following risks:

- Can fully take charge of the wireless-communication channels. Afterwards, attackers can intercept, capture, modify, erase and insert bogus messages into the communication channel.
- Can steal a user’s smart card or access a user’s password. Thereafter, these security tokens can be utilized to commit numerous cases of system compromise.
- Using techniques, such as power analysis, attackers in possession of a user’s smart card can retrieve the sensitive security values stored in it.
- It is possible for attackers to determine the identities of every server and all users.

3.3 Security Goals

To counter the capabilities of the attacker advocated above and ensure robust security for IoV communication using 5G technology, our proposed LAIoV-5G scheme must fulfill the following requirements.

1. ***Mutual Authentication and Integrity:*** These are not just crucial elements, but also the backbone of our proposed LAIoV-5 G scheme. They are the pillars on which our communication security stands, ensuring that only approved entities engage in the interaction process and that the transmitted or stored data remains unaltered and unchanged.
2. ***Unlinkability:*** Adversaries should be incapable of associating any session or messages to any particular network element.
3. ***TA Impersonation Attack:*** This is not just a type of cybercrime, but also a serious threat to our LAIoV-5 G scheme. In this attack, an attacker pretends to be a trusted authority, potentially causing significant damage to our system. Therefore, adversaries should be unable to launch this attack against our LAIoV-5 G scheme.
4. ***Social Engineering Attacks*:** Here, the attacker pretends to be a familiar person to the target, such as a known user or a trusted entity, in order to gain trust and exploit access privileges.
5. ***Maintaining Privacy for Users*:** Maintaining user anonymity involves keeping a user's identity concealed or undisclosed to safeguard his/her privacy through encryption methods.
6. ***Replay Attack*:** A legitimate transmission is required in our LAIoV-5 G scheme. Therefore, previously transmitted messages should not be sent again to a target system to trigger unauthorized actions or data breaches.
7. ***Smart-card Threats*:** These are dangerous attacks in which a physical smart card containing sensitive data or cryptographic keys is used to obtain unauthorized access to systems or resources.
8. ***Stolen Verifier and Privileged Insider Attacks*:** This type of attack involves an insider with privileged access to a system that steals a verifier device, such as a token or hardware-security module (HSM). These stolen verifiers can then bypass authentication mechanisms and gain unauthorized access.

3.4 Hash Functions

In this sub-section, the one-way hashing function h (.) takes o (string of arbitrary length) as the input.

Thereafter, it produces an output of fixed length, referred to as the hash code. Therefore, hash code = $h(o)$ and any small alteration in the value of the input string can have profound effects on this hash code. According to [43], the hash h (.) has the characteristics below:

- For a given input string, it is simple to find hash code $= h(o)$.

- Given the hash code $h(o)$, its is mathematically difficult to determine o.
- For any two inputs of o_1 and o_2, it is cumbersome to find $h(o_1) = h(o_2)$. This hash function with this property is said to be collision resistant.

4. THE LAIOV-5G SCHEME

Our proposed scheme consists of four main phases, including initialization, registration, login and password change, each of which plays a critical role in securing IoV communications. The initialization phase is the foundation, where the TA generates the cryptographic parameters required for the scheme. Using ECC, the TA generates and shares common and public parameters, such as curve points and hash functions, with all participating entities. These parameters allow for lightweight and secure cryptographic computations while maintaining efficient resource utilization. In the second phase, each vehicle is securely registered with the TA. Upon successful completion, the TA assigns a unique vehicle ID and securely embeds the registration details on a smart card provided to the vehicle. This phase is crucial in ensuring that only authorized and verified vehicles are granted access to the IoV network, effectively mitigating the risk of unauthorized entities infiltrating the system.

The login phase is responsible for establishing secure communication channels. The vehicle initiates a session; it sends an encrypted request containing its identity and a timestamp to the TA. The TA verifies the request, ensuring the vehicle's legitimacy. Mutual authentication is then performed between the vehicle and the TA, after which a session key is generated. This session key is generated using lightweight cryptographic exchange, ensuring that all subsequent communications remain confidential and tamper-resistant. Finally, the password-update phase allows the vehicle to securely change its credentials. To do this, the vehicle must confirm its current credentials with the TA. Once verified, the TA simplifies the secure update of both the password and the secret key, ensuring that the process is protected from unauthorized changes.

These four phases work together to form a comprehensive security framework for IoV environments. The interactions and computations between entities are illustrated in Figures 2 and 3 of the manuscript, providing a clear overview of the protocol's operation. This structured approach balances strong security with lightweight requirements for IoV systems, making them efficient and practical for deployment in real-world scenarios. Specific descriptions of f these stages are detailed in the following sub-sections.

4.1 Initialization Phase

This phase is responsible for creating and distributing system parameters *via* TA as the following steps:

- Choosing two prime numbers p and q.
- Generating random numbers a and $\in F_p$.
- Choosing an elliptic curve EC, such that $4a^3 + 27b^2 \neq 0$
- Select the private key K_s, where $K_s \in [1, a * b]$.
- Selecting G as a base point on the EC.
- Calculating the public key $K_p = GK_s$.
- Determining the cryptography hash function $h(.)$.
- At the end, trusted authority TA publishes parameters $\{q, K_p, G, h(.)\}$.

4.2 Registration Phase

Every vehicle that aspires to be part of the IoV network plays a crucial role and must first register. If a vehicle V_i decides to register with the TA, the following steps should be followed.

- A user of V_i chooses the identityID_v, PasswordPW_i and an arbitrary number$r_v \in Z_p^*$ and sends $\{ID_v, h(ID_v \parallel PW_i \parallel r_v) \oplus r_v\}$ as request for registration to the TA, *via* a highly secure channel, ensuring the safety of the data.
- On receiving the message $\{ID_v, h(ID_v \parallel PW_i \parallel r_v) \oplus r_v\}$, the TA computes $= h(ID_v \parallel K_s) \oplus h(ID_v \parallel PW_i \parallel r_v) \oplus r_v$. Thereafter, it is sent back to them *via* a secure communication medium.
- After getting A, the V_i computes the following:

- $B = A \oplus r_v$
- $B = h(ID_v \parallel K_s) \oplus h(ID_v \parallel PW_i \parallel r_v)$
- $C = h(ID_v \parallel PW_i \parallel r_v)$
- Then, the values $\{B, C, r_v, h(\,)\}$ (which include the vehicle's unique identifier and registration details) are uploaded on the smart card SC_i for future verification.

4.3 Log-in Phase

The goal of this phase is to have the user of vehicle V_i sign-in into a system with the given SC_i credentials. Thereafter, a secure communication channel is created with a TA server by following the steps outlined below:

Step 1. The user V_i inserts the SC_i and inputs his/her credentials ID_v, PW_i, the OBU, then computes $C^* = h(ID_v \parallel PW_i \parallel r_v)$ and confirms it against stored data on the SC_i. The session will be terminated if the values C and C^* do not match. Otherwise, V_i will start a secure communication with TA by generating an arbitrary number $a \in Z_p^*$ and achieving the following equations:

- $X = aP$
- $Y = ID_v \oplus (aK_p)$
- $\sigma = h(ID_v \parallel X \parallel h(ID_v \parallel PW_i \parallel r_v) \parallel T_1)$

Then, it sends the encrypted message $\{X, Y, \sigma, B, T_1\}$ to the TA.

Step 2. On receiving the message $\{X, Y, \sigma, B, T_1\}$, TA achieves the following equations:

- $ID_v = Y \oplus (K_s X)$
- $U_{TA} = B \oplus h(ID_v \parallel K_s)$
- $\sigma^* = h(ID_v \parallel X \parallel U_{TA} \parallel T_1)$.
- It hecks $? = \sigma^*$; the session will be terminated if the check is not verified. Otherwise, the TA will compute the session secret key SK_i as follows:

$$SK_i = h((K_s X) \parallel ID_v \parallel h(ID_v \parallel K_s))$$
$$Auth_{TA} = h(SK_i \parallel (K_s X), T_2)$$

- Finally, TA sends back the $\{Auth_{TA}, T_2\}$ to V_i.

Step 3. On receiving the message $\{Auth_{TA}, T_2\}$, the V_i achieves the following equations:

- $U_v = A \oplus h(ID_v \parallel PW_i \parallel r_v)$
- $SK_i = h\big((aK_p) \parallel ID_v \parallel U_v\big)$
- $Auth_{TA}^* = h(SK_i \parallel \big(aK_p\big), T_2)$.
- It checks $Auth_{TA} ?= Auth_{TA}^*$; the session will be terminated if the check is not verified. Otherwise, the V_i will send $\{Auth_v, T_3\}$ to the TA as a response message confirming that the vehicle received the session key correctly, where $Auth_v = h(ID_v \parallel \big(aK_p\big) \parallel U_v \parallel SK_i \parallel T_3)$.

Step 4. On receiving the message $\{Auth_v, T_3\}$, the TA computes $Auth_v^* = h(ID_v \parallel (K_s X) \parallel U_{TA} \parallel SK_i \parallel T_3)$ and checks $Auth_v ?= Auth_v^*$. If the check is not verified, the log-in process will be terminated. If not, both TA and V_i consent on using SK_i as a shared session key.

4.4 Password-change Phase

The procedures carried out in this sub-section are crucial, since they give the user of vehicle V_i the ability to update his/her password at their discretion. Both TA and V_i parties are involved in the following steps:

Step 1. The user of V_i logs in to the vehicle, as explained in the previous phase.

Step 2. The user of V_i enters a new password PW_{i-new}.

Step 3. The smart card SC_i, a key player in this process, selects a new arbitrary number r_{v-new} and performs the following equations:

- $B_{new} = B \oplus h(ID_v \parallel PW_i \parallel r_v) \oplus h(ID_v \parallel PW_{i-new} \parallel r_{v-new})$
- $C_{new} = h(ID_v \parallel PW_{i-new} \parallel r_{v-new})$

Step 4. The SC_i stores both B_{new} and C_{new} instead of B and C respectively.

Step 5. The V_i send both new values of B_{new} and C_{new} to the TA after encrypting them by the session key SK_i, ensuring the highest level of security.

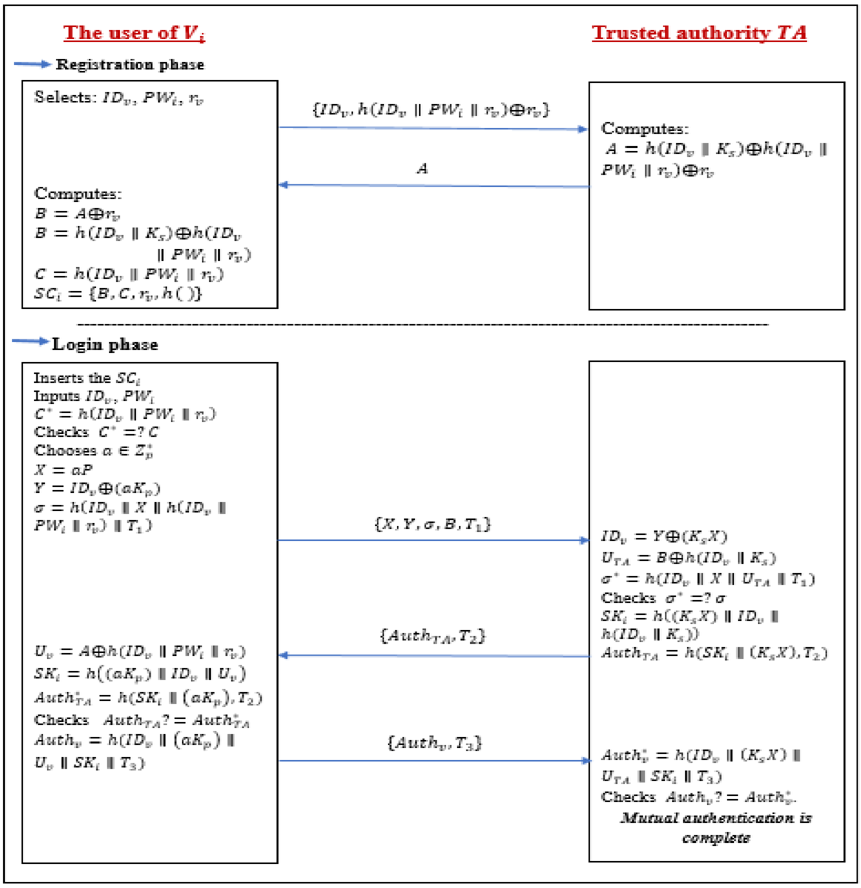

Figure 2. Registration and log-in phases.

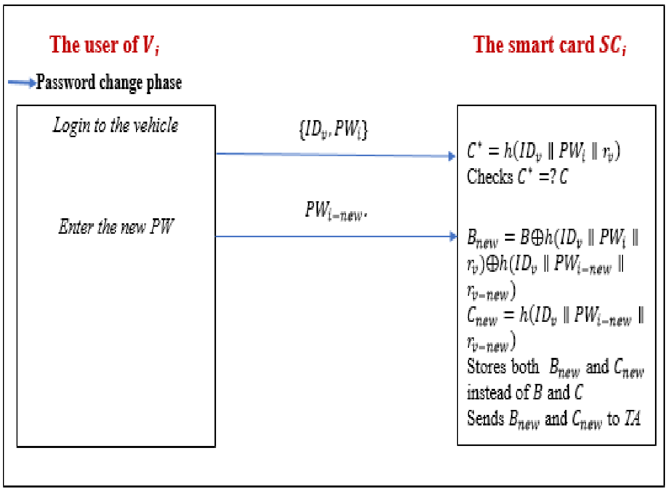

Figure 3. Password-change phase.

5. Security Analysis

The essence of this section is to present security analysis of our LAIoV-5G scheme. This analysis confirm the proposed LAIoV-5G scheme's robustness and highlights its resistance to various attacks. We further demonstrate that the LAIoV-5G scheme's security is unaffected by various potential circumstances. As shown in Table 2, our LAIoV-5G scheme meets key security requirements, as compared to several related schemes. This should reassure you of its effectiveness.

Table 2. Security comparison.

Security requirements	**Wu, T. Y. et al. [49]**	**Karim, S. et al. [50]**	**Salami, Y, et al. [51]**	**Xie et al. [52]**	**LAIoV-5G**
Mutual authentication and integrity	Yes	Yes	Yes	Yes	Yes
Unlinkability	Yes	No	Yes	No	Yes
TA impersonation attack	No	Yes	Yes	Yes	Yes
User of V_i impersonation attack	Yes	Yes	Yes	Yes	Yes
User anonymity	Yes	Yes	No	Yes	Yes
Replay attack	No	Yes	Yes	No	Yes
Stolen smart card threat	Yes	No	No	Yes	Yes
Stolen verifier and privileged insider threats	Yes	No	Yes	Yes	Yes

1. *Mutual Authentication and Integrity*

The authentication and integrity of our LAIoV-5G scheme is provided as follows:

First message $\{X, Y, \sigma, B, T_1\}$: The TA authenticates the received message $\{X, Y, \sigma, B, T_1\}$. Accordingly, it computes the ID_v and U_{TA} by the deployment of private key K_s, then it checks $\sigma ?= \sigma^*$.

Second message $\{Auth_{TA}, T_2\}$: The vehicle user V_i authenticates the received message $\{Auth_{TA}, T_2\}$ according to the equation $Auth_{TA} ?= Auth^*_{TA}$. Only a genuine TA can compute $Auth_{TA}$ since it owns the system's secret key K_s. In the same way, at the V_i part, $Auth^*_{TA}$ contains the session key SK_i, which includes ID_v concatenated with U_v. Moreover, U_v is computed by using the ID_v and PW_i. Thus, only a genuine V_i can compute $Auth^*_{TA}$.

Third message $\{Auth_v, T_3\}$: The TA authenticates the received message $\{Auth_v, T_3\}$ according to the equation $Auth_v ?= Auth^*_v$. As $Auth^*_v = h(ID_v \parallel (K_s X) \parallel U_{TA} \parallel SK_i \parallel T_3)$ includes the system's secret key K_s and one-way hash function $h()$ is used, it is impossible for the attacker to compute it.

Hence, the proposed LAIoV-5G scheme offers mutual verification and integrity protection.

2. *Unlinkability*

The design of the messages sent in our LAIoV-5 G scheme, such as $\{X, Y, \sigma, B, T_1\}$, is a testament to its technical complexity. It has no static value according to an arbitrary number $a \in Z^*_p$., ensuring that all messages for the exact vehicle are different. This level of complexity makes it impossible for attackers to establish whether any two beacons are being generated by the same vehicle. Hence, the proposed LAIoV-5G scheme offers the unlinkability, a feat of technical ingenuity.

3. *TA Impersonation Attack*

In our LAIoV-5G scheme, to pretend to be a legitimate TA, an adversary must be in possession of the system's private key $K_s$so as to facilitate the computation of $U_{TA} = A \oplus h(ID_v \parallel K_s)$. Additionally, the session key $SK_i = h((K_s X) \parallel ID_v \parallel h(ID_v \parallel K_s))$ will calculate if having the K_s. Likewise, the TA's signature $Auth_{TA} = h(SK_i \parallel (K_s X), T_2)$ contains both K_s and SK_i. Thus, only the genuine TA can compute all these security parameters. For this reason, our LAIoV-5G scheme can resist the TA masquerade threats.

4. *Vehicle V_i User Impersonation Attack*

In our LAIoV-5G scheme, let's assume that an attacker captures the log-in message $\{X, Y, \sigma, A, T_1\}$, he/she cannot modify this message due to changing the Y for each session. Furthermore, $\sigma = h(ID_v \parallel X \parallel h(ID_v \parallel PW_i \parallel r_v) \parallel T_1)$ contains ID_v, PW_i and hash function. Hence, our LAIoV-5G scheme can mitigate vehicle V_i user impersonations.

5. *Anonymous Communication*

In our LAIoV-5G scheme, the user of V_i sends a message $\{X, Y, \sigma, A, T_1\}$ through the open-access

environment that ID_v is not in the plain text, during the log-in phase. If any challenger intercepts the message, whose role is to test the user's authenticity, he/she cannot obtain the ID_v, because in $Y = ID_v \oplus (aK_p)$, the arbitrary nonce a is exposed to a multiplication operation with the public key K_p.

Besides, XOR is applied between ID_v and the aK_p. Additionally, in $\sigma = h(ID_v \parallel X \parallel h(ID_v \parallel PW_i \parallel r_v) \parallel T_1)$, ID_v is concatenated with X, $C^*$and then encrypted with hashing function $h()$. Hence, the proposed LAIoV-5G scheme offers anonymous communication.

6. *Message Replay Attacks*

For the proposed LAIoV-5G scheme, timestamp T_i is applied to all sending messages $\{X, Y, \sigma, A, T_1\}$; $\{Auth_{TA}, T_2\}$; $\{Auth_v, T_3\}$,, the receiver avoids the replay attack by refusing the message if the timestamp expires. Hence, our LAIoV-5G scheme can prevent replay attacks.

7. *Stolen Smart Card Attack*

Our LAIoV-5G scheme is built with a strong focus on security. The smart card securely stores data $B = h(ID_v \parallel K_s) \oplus h(ID_v \parallel PW_i \parallel r_v)$ and $C = h(ID_v \parallel PW_i \parallel r_v)$., making it impossible for an attacker to obtain any parameter used to guess the ID_v and PW_i or the secret data. Even if the attacker manages to get the user's information SC, he/she cannot utilize the stored data for his/her own benefit. This robust security design of our LAIoV-5G scheme effectively prevents smart card-loss attacks.

8. *Privileged Insider and Stolen Verifier Threats*

In our LAIoV-5G scheme, we do not preserve any database and TA authenticates the message received from the V_i using the private keyK_s. Also, the ID_v and $PW_i$are not sent to the TA in plaintext. So, our LAIoV-5G scheme can resist the privileged-insider and stolen-verifier threats.

6. PERFORMANCE EVALUATION

The security features supported by the proposed LAIoV-5 G scheme with those offered by its peers [49]–[52] are presented in Table 2. It is clear that our scheme mitigates numerous threats, including privileged insider, user impersonation, stolen verifiers, server impersonation and stolen smart-card threats. The added benefit of user anonymity further enhances the appeal of the suggested protocol. Based on the information shown in Table 2, it is clear that the related protocols contain a few security issues, whereas our LAIoV-5 G scheme is fully secure against such threats.

In this section, an examination of the effectiveness of our scheme, including computational and communication costs, is presented. We demonstrate the performance of our scheme by comparing it with the schemes of Wu, T. Y. et al. [49], Karim, S. et al. [50], Salami, Y. et al. [51] and Xie et al. [52]. Our evaluation of the computational complexities of our LAIoV-5G scheme and its peers yielded impressive results. We adopted the time of cryptographic operations as managed by Xie et al. [52] which are executed on a 64-bit laptop with Windows 10 Pro environment installed and 16 GB of RAM, running on an Intel i5 6300 GHz CPU. Table 3 shows the time taken to run different cryptographic operations.

Table 3. Execution time.

Operation	Notation	Time cost (ms)
Hash function	T_h	0.019
Multiplication of point on ECC	T_m	2.610
Symmetric encryption/decryption	$T_{enc-dec}$	0.511

In the scheme of Wu, T. Y. et al. [49], the following operations are executed: (12 scalar multiplications) and (22 secure hash functions). Thus, the total computation time is $22T_h$+ $12T_m = 31.738$. In the scheme of Karim, S. et al. [50], the following operations are executed: (6 scalar multiplications) and (10 secure hash functions). Thus, the total computation time is $10T_h$+ $6T_m = 15.85$. In the scheme of Salami, Y, et al. [51], the following operations are executed: (8 scalar multiplications) and (30 secure hash functions). Thus, the total computation time is $30T_h$+ $8T_m = 21.45$. In the scheme of Xie et al. [52], the following operations are executed: (6 scalar multiplications) and (18 secure hash functions) and (1 Symmetric Encryption/Decryption). Thus, the total computation time is $18T_h$ + $6T_m$ + $1T_{enc-dec} = 16.513$. On the other hand, our LAIoV-5G scheme needs only (3 scalar multiplications) and (13 secure hash functions). Thus, the total computation time of our LAIoV-5G scheme is $13T_h$+ $3T_m = 8.077$. Table 4 gives the comparative analysis of the obtained computation complexities.

Table 4. Computation-cost comparison.

Schemes	T_h	T_m	$T_{enc-dec}$	Total	Computation cost (ms)
Wu, T. Y. et al. [49]	22	12	0	$22T_h$+ $12T_m$	31.738
Karim, S. et al. [50]	10	6	0	$10T_h$+ $6T_m$	15.85
Salami, Y, et al. [51]	30	8	0	$30T_h$+ $8T_m$	21.45
Xie et al. [52]	18	6	1	$18T_h$+ $6T_m$+$1T_{enc-dec}$	16.513
LAIoV-5G	13	3	0	$13T_h$+ $3T_m$	8.077

In terms of communication cost, Table 5 shows the sizes of different cryptographic operations, while Table 6 provides a comparative analysis of the communication complexity of our scheme *versus* its counterparts. In Karim, S. et al. [50], four messages are transmitted; namely (Mssg1 = RIDVn, CertifVn, AVn, DsignVn, TS1), (Mssg2 = RIDRSU, CertifRSU, BRSU, SKey-VerRSU−V, TS2) and (Mssg3 = ACKVn−RSU, TS3), which include (3 ECC points), (2 physical identities), (4 hash function outputs) and (3 timestamps). Thus, a total of 2400 bits are transmitted. In the same way, the communication cost is calculated for Wu, T. Y. et al. [49], Salami, Y, et al. [51], Xie et al. [52] and our LAIoV-5G schemes.

Table 5. Cryptographic-operation output sizes.

Operations	Cost (bits)
Elliptic Curve Point	256 bits
Actual identity	256 bits
One-way hash function	256 bits
Timestamps	32 bits
Arbitrary nonce	256 bits
Symmetric encryption/decryption	AES-128 bits

Table 6. Communication-cost comparison

Schemes	No. of messages	Communication cost (bit)
Wu, T. Y. et al. [49]	5	3744
Karim, S. et al. [50]	3	2400
Salami, Y, et al. [51]	5	3520
Xie et al. [52]	4	2976
LAIoV-5G	3	1632

As shown in Table 4 and Table 6, the computation time of our LAIoV-5G scheme is 8.077 ms, which is 74.6%, 49%, 62.3% and 51% lower than those of Wu, T. Y. et al. [49], Karim, S. et al. [50], Salami, Y. et al. [51] and Xie et al. [52], respectively. The communication cost of our LAIoV-5G scheme is 1632 bits, which is 56.4%, 32%, 53.6% and 45.1% lower than those of Wu, T. Y. et al. [49], Karim, S. et al. [50], Salami, Y. et al. [51] and Xie et al. [52], respectively.

Table 7. Improvement of our LAIoV-5G scheme over other schemes.

Schemes	Computation improvement	Communication improvement
Wu, T. Y. et al. [49]	74.6%	56.4%
Karim, S. et al. [50]	49%	32%
Salami, Y, et al. [51]	62.3%	53.6%
Xie et al. [52]	51%	45.1%

Table 7 shows the improvement of our LAIoV-5G scheme compared with other schemes in terms of computation and communication costs. The results unequivocally demonstrate the superiority of computational and communication efficiency of our scheme over other related schemes. Moreover, our scheme achieves a robust security posture at lower-bandwidth requirements, further solidifying its effectiveness and impressiveness.

7. CONCLUSION

This paper presents a highly effective LAIOV-5G protocol to secure message exchanges in IoV enabled smart cities. The proposed scheme enables a unique authentication method and demonstrates cost-effectiveness in terms of computation and communication complexities. The comparative evaluation results show that it incurs the lowest costs when contrasted against its peer authentication protocols. Specifically, security evaluations show that LAIOV-5G protocol withstands significant known security attacks. Some of these attacks include stolen smart card, privileged insider, impersonation and message-replay attacks. Hence, the suggested methodology has been demonstrated to be effective, dependable and secure. In future work, we plan to conduct a detailed evaluation of the performance of the proposed scheme in large-scale smart-vehicle networks and address the challenges related to real-world applications, which were beyond the scope of this study.

REFERENCES

[1] S. Chen, H. Xu, D. Liu, B. Hu and H. Wang, "A Vision of IoT: Applications, Challenges and Opportunities with China Perspective," IEEE Internet of Things J., vol. 1, no. 4, pp. 349-359, 2014.

[2] C.-M. Chen, Z. Li, A. K. Das, S. A. Chaudhry and P. Lorenz, "Provably Secure Authentication Scheme for Fog Computing-enabled Intelligent Social Internet of Vehicles," IEEE Transactions on Vehicular Technology, vol. 73, no. 9, pp. 13600-13610, DOI: 10.1109/TVT.2024.3382971, Sept. 2024

[3] S. Mumtaz, A. Bo, A. Al-Dulaimi and K.-F. Tsang, "Guest Editorial 5G and Beyond Mobile Technologies and Applications for Industrial IoT (IIoT)," IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 25882591, Jun. 2018.

[4] S. Garg et al., "MobQoS: Mobility-aware and QoS-driven SDN Framework for Autonomous Vehicles," IEEE Wireless Communications, vol. 26, no. 4, pp. 1220, Aug. 2019.

[5] M. A. Al Sibahee et al., "Blockchain-based Authentication Schemes in Smart Environments: A Systematic Literature Review," IEEE Internet of Things J., vol. 11, no. 21, pp. 34774-34796, 2024.

[6] V.O. Nyangaresi et al., "Energy Efficient Dynamic Symmetric Key Based Protocol for Secure Traffic Exchanges in Smart Homes," Applied Sciences, vol. 12, no. 24, p. 12688, 2022.

[7] V.O. Nyangaresi et al., "Smart City Energy Efficient Data Privacy Preservation Protocol Based on Biometrics and Fuzzy Commitment Scheme," Scientific Reports, vol. 14, Article no. 16223, 2024.

[8] V. O. Nyangaresi et al., "Authentication and Key Agreement Protocol for Secure Traffic Signaling in 5G Networks," Proc. of the 2021 IEEE 2nd Int. Conf. on Signal, Control and Communication (SCC), pp. 188-193, DOI: 10.1109/SCC53769.2021.9768338, Tunis, Tunisia, 2021.

[9] V. O. Nyangaresi et al., "Towards Security and Privacy Preservation in 5G Networks," Proc. of the 2021 29th Telecommuni. Forum (TELFOR), pp. 1-4, DOI: 10.1109/TELFOR52709.2021.9653385, Belgrade, Serbia, 2021.

[10] G. Rathee et al., "Trusted Orchestration for Smart Decision-making in Internet of Vehicles," IEEE Access, vol. 8, pp. 157427-157436, 2020.

[11] C.-M. Chen, Q. Miao, S. Kumari, M. K. Khan and J. J. P. C. Rodrigues, "A Privacy-preserving Authentication Protocol for Electric Vehicle Battery Swapping Based on Intelligent Blockchain," IEEE Internet of Things J., vol. 11, no. 10, pp. 17538-17551, 15 May15, 2024.

[12] C.-M. Chen et al., "A Secure Authentication Protocol for Internet of Vehicles," IEEE Access, vol. 7, pp. 12047-12057, 2019.

[13] J. G. Andrews et al., "What Will 5G Be?" IEEE Journal on Selected Areas in Communications, vol. 32, pp. 1065–1082, 2014.

[14] X. Huang, R. Yu, J. Kang, Y. He and Y. Zhang, "Exploring Mobile Edge Computing for 5G-enabled Software Defined Vehicular Networks," IEEE Wireless Communications, vol. 24, pp. 55–63, 2017.

[15] S. A. A. Shah, E. Ahmed, M. Imran and S. Zeadally, "5G for Vehicular Communications," IEEE Communications Magazine, vol. 56, pp. 111–117, 2018.

[16] M. A. Al-Shareeda et al., "Password-guessing Attack-aware Authentication Scheme Based on Chinese Remainder Theorem for 5G-enabled Vehicular Networks," Applied Sciences, vol. 12, no. 3, p. 383, 2022.

[17] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," Proc. of Workshop Hot Topics Network (HotNets-IV), pp. 1_6, Annapolis, MD, USA, 2005.

[18] S. Capkun and J.-P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," Proc. of the IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1917-1928, Miami, USA, Mar. 2005.

[19] L. Lazos, R. Poovendran and S. Apkun, "ROPE: Robust Position Estimation in Wireless Sensor Networks," Proc. of the IEEE 4th Int. Symposium on Information Processing in Sensor Networks (IPSN 2005), Boise, USA, p. 43, 2005.

[20] A. Studer, F. Bai, B. Bellur and A. Perrig, "Flexible, Extensible and Efficient VANET Authentication,"

Journal of Communications and Networks, vol. 11, no. 6, pp. 574-588, Dec. 2009.

[21] X. Lin et al., "TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving," IEEE Transactions on Wireless Communications, vol. 7, no. 12, pp. 4987-4998, Dec. 2008.

[22] B. Ying, D. Makrakis and H. T. Mouftah, "Privacy Preserving Broadcast Message Authentication Protocol for VANETs," J. of Network and Computer Applications, vol. 36, no. 5, pp. 1352-1364, 2013.

[23] C. Zhang, R. Lu, X. Lin, P.-H. Ho and X. Shen, "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks," Proc. of the 27th IEE Conf. on Computer Communications (IEEE INFOCOM 2008), pp. 246-250, Phoenix, USA, Apr. 2008.

[24] C. Zhang, P.-H. Ho and J. Tapolcai, "On Batch Verification with Group Testing for Vehicular Communications," Wireless Networks, vol. 17, no. 8, p. 1851, 2011.

[25] M. Eltoweissy, S. Olariu and M. Younis, "Towards Autonomous Vehicular Clouds," Proc. of the Int. Conf. on *Ad Hoc* Networks, Part of the Book Series: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Eng., vol. 49 pp. 1-16, Berlin, Germany, 2010.

[26] D. Bernstein, N. Vidovic and S. Modi, "A Cloud PAAS for High Scale, Function and Velocity Mobile Applications - With Reference Application As the Fully Connected Car," Proc. of the 2010 IEEE 5th Int. Conf. on Systems and Networks Communications (ICSNC), pp. 117-123, Nice, France, Aug. 2010.

[27] R. Hussain, J. Son, H. Eun, S. Kim and H. Oh, "Rethinking Vehicular Communications: Merging VANET with Cloud Computing," Proc. of the IEEE 4th Int. Conf. on Cloud Computing Technology and Science Proceedings (CloudCom), pp. 606-609, Taipei, Taiwan, Dec. 2012.

[28] H. Zhong, S. Han, J. Cui, J. Zhang and Y. Xu, "Privacy-preserving Authentication Scheme with Full Aggregation," Information Sciences, vol. 476, pp. 211–221, 2019.

[29] M. Azees, P. Vijayakumar and L. J. Deboarh, "EAAP: Efficient Anonymous Authentication with Conditional Privacy-preserving Scheme for Vehicular *Ad Hoc* Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 18, pp. 2467–2476, 2017.

[30] L. Zhang et al., "Distributed Aggregate Privacy-preserving Authentication in VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 18, pp. 516–526, 2016.

[31] M. Bayat et al., "A New and Efficient Authentication Scheme for Vehicular *Ad Hoc* Networks," Journal of Intelligent Transportation Systems, vol. 24, pp. 171–183, 2020.

[32] M. Bayat, M. Pournaghi, M. Rahimi and M. Barmshoory, "NERA: A New and Efficient RSU-based Authentication Scheme for VANETs," Wireless Networks, vol. 26, pp. 3083–3098, 2020.

[33] S. M. Pournaghi et al., "NECPPA: A Novel and Efficient Conditional Privacy-preserving Authentication Scheme for VANET," Computer Networks, vol. 134, pp. 78–92, 2018.

[34] M. A. Al-Shareeda et al., "SE-CPPA: A Secure and Efficient Conditional Privacy-preserving Authentication Scheme in Vehicular *Ad Hoc* Networks," Sensors, vol. 21, p. 8206, 2021.

[35] D. He, S. Zeadally, B. Xu and X. Huang, "An Efficient Identity-based Conditional Privacy-preserving Authentication Scheme for Vehicular *Ad Hoc* Networks," IEEE Transactions on Information Forensics and Security, vol. 10, pp. 2681–2691, 2015.

[36] M. R. Asaar, M. Salmasizadeh, W. Susilo and A. Majidi, "A Secure and Efficient Authentication Technique for Vehicular Ad-hoc Networks," IEEE Transactions on Vehicular Technology, vol. 67, no. 6, pp. 5409–5423, 2018.

[37] M. A. Al-Shareeda, M. Anbar, S. Manickam and I. H. Hasbullah, "Towards Identity-based Conditional Privacy-preserving Authentication Scheme for Vehicular Ad Hoc Networks," IEEE Access, vol. 9, pp. 113226–113238, 2021.

[38] M. A. Al-Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam and A. S. Al-Hiti, "LSWBVM: A Lightweight Security without Using Batch Verification Method Scheme for a Vehicle Ad Hoc Network," IEEE Access, vol. 8, pp. 170507-170518, DOI: 10.1109/ACCESS.2020.3024587, 2020,.

[39] J. S. Alshudukhi, B. A. Mohammed and Z. G. Al-Mekhlafi, "Conditional Privacy-preserving Authentication Scheme without Using Point Multiplication Operations Based on Elliptic Curve Cryptography (ECC)," IEEE Access, vol. 8, pp. 222032–222040, 2020.

[40] M. Alazzawi, H. Lu, A. Yassin and K. Chen, "Efficient Conditional Anonymity with Message Integrity and Authentication in a Vehicular Ad hoc Network," IEEE Access, vol. 7, pp. 71424–71435, 2019.

[41] M. A. Alazzawi et al., "ID-PPA: Robust Identity-based Privacy-preserving Authentication Scheme for a Vehicular Ad-Hoc Network," Proc. of Advances in Cyber Security (ACeS 2020), Part of Book Series: Communications in Computer and Information Science, vol. 1347, DOI: 10.1007/978-981-33-6835-4_6, Springer, Singapore, 2021.

[42] J. S. Alshudukhi, Z. G. Al-Mekhlafi and B. A. Mohammed, "A Lightweight Authentication with Privacy-preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography," IEEE Access, vol. 9, pp. 15633–15642, 2021.

[43] J. Cui, J. Chen, H. Zhong, J. Zhang and L. Liu, "Reliable and Efficient Content Sharing for 5G-enabled Vehicular Networks," IEEE Trans. on Intelligent Transportation Syst., vol. 23, no. 2, pp. 1–13, 2020.

[44] J. Cui, X. Zhang, H. Zhong, Z. Ying and L. Liu, "RSMA: Reputation System-based Lightweight Message Authentication Framework and Protocol for 5G-enabled Vehicular Networks," IEEE Internet of Things

J., vol. 6, no. 4, pp. 6417–6428, 2019.

[45] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu and L. Liu, "Edge Computing-based Privacy-preserving Authentication Framework and Protocol for 5G-enabled Vehicular Networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 7, pp. 7940–7954, 2020.

[46] M. A. Al-Shareeda et al., "CM-CPPA: Chaotic Map-based Conditional Privacy-preserving Authentication Scheme in 5G-enabled Vehicular Networks," Sensors, vol. 22, no. 13, p. 5026, 2022.

[47] M. A. Al-Shareeda et al., "Efficient Conditional Privacy Preservation with Mutual Authentication in Vehicular Ad Hoc Networks," IEEE Access, vol. 8, pp. 144957–144968, 2020.

[48] M. A. Alazzawi, H. Lu, A. A.Yassin and K. Chen, "Robust Conditional Privacy-preserving Authentication based on Pseudonym Root with Cuckoo Filter in Vehicular Ad Hoc Networks," KSII Trans. on Internet and Information Systems, vol. 13, no. 12, DOI: 10.3837/tiis.2019.12.018, 2019.

[49] T.-Y. Wu, Z. Lee, L. Yang and C.-M. Chen, "A Provably Secure Authentication and Key Exchange Protocol in Vehicular Ad Hoc Networks," Security and Communication Networks, vol. 2021, no. 1, p. 9944460, 2021.

[50] S. M. Karim et al., "BSDCE-IoV: Blockchain-based Secure Data Collection and Exchange Scheme for IoV in 5G Environment," IEEE Access, vol. 11, pp. 36158-36175, 2023.

[51] Y. Salami, V. Khajehvand and E. Zeinali, "SAIFC: A Secure Authentication Scheme for IOV Based on Fog-cloud Federation," Security and Communication Networks, vol. 2023, no. 1, p. 9143563, DOI: 10.1155/2023/9143563, 2023.

[52] Q. Xie and J. Huang, "Improvement of a Conditional Privacy-preserving and Desynchronization-Resistant Authentication Protocol for IoV," Applied Sciences, vol. 14, no. 6, p. 2451, 2024.

ملخص البحث:

لقد مكّنت شبكات الجيل الخامس من تطوير مُدنٍ ذكية يتمّ فيها جمْع كمّياتٍ هائلةٍ من البيانات وتخزينها ونشرها. ويتمثّل الهدف النّهائي لتلك المدن الذّكية في تقليل التّكلفة ورفع مستوى أمان الأداء. وفي هذه البيئة، تساعد إنترنت المركبات في ربْط المركبات والمشاة وغُرف التّحكُّم وبعض البِنى التّحتية للطرق. ونظراً للطّبيعة غير الآمنة لقنوات الاتّصال في إنترنت المركبات لتبادل المعلومات، فإنّ من المهمّ تطوير تقنياتٍ عمليةٍ للحفاظ على سرّية المعلومات وعلى الخصوصية.

وقد تمّ اقتراح العديد من الحُلول المرتبطة بالأمان في الماضي القريب. ولسوء الحظّ، فإنّ غالبية تقنيات المصادقة لها عيوب فيما يتعلّق بالأمان، الأمر الّذي يهدّد البيانات المنقولة، كما أنّ بعضها يتّصف بقدرٍ عالٍ من عدم الفاعلية.

ولِجَسْر تلك الفجوات، نقدّم في هذه الورقة البحثية مخطّط مصادقةٍ "خفيف الوزْن" لإنترنت المركبات، مبنياً على تقنية الجيل الخامس. وقد جرى تحليل المخطّط المقترح من حيث الأمان، وبيّنت نتائج التّحليل أنّ المخطّط المقترح تمكَّن من كبْح العديد من الهجمات الّتي تهدّد اتّصالات إنترنت المركبات في بيئة المدينة الذّكية. ومن ناحيةٍ أخرى، أثبت مخطّط المصادقة المقترح مستوىً عالياً من الفاعلية في تجارب تحليل الأداء.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).