Journal of Engineering Research

Volume 6 | Issue 3 Article 31

2022

An Efficient Authentication Protocol Based on Chebyshev Chaotic Map for Intelligent Transportation

nermeen Abdalghafour

Vol. 6 – No.3, 2022 Journal of Engineering Research (ERJ)

An Efficient Authentication Protocol Based on Chebyshev Chaotic Map for Intelligent Transportation

Nermeen M. Abdal-ghafour, Mohamed E. Nasr, Roayat I. Abdelfatah
Electronics and Electrical Communications Engineering Department, Faculty of Engineering, Tanta University, Tanta 31527, Egypt
Email: NermeenMohamed@f-eng.tanta.edu.eg

***Abstract*- For meeting the demands of safety, traffic management, and high mobility, vehicular adhoc network (VANET) has become a promising component for smart transportation systems. However, the wireless environment of vehicular network leads to various challenges in the communication security. Hence, several authentication schemes have previously been proposed to address VANET security issues but their procedures disregard the balance between effectiveness and security. Thus, this paper presents a new decentralized authentication protocol that relies on lightweight functions such as the Chebyshev chaotic map and logical shift operator to achieve the high mobility requirement. In order to reduce the number of messages transferred over the network, this protocol attempts to eliminate any redundant authentication steps during its authentication stage. Additionally, the new protocol solves key management problems by applying a little modification to the public key infrastructure to ignore certificates transmission over the network. The proposed design incorporates the self-authentication concept to safeguard the vehicle trip route on the road. Moreover, the performance evaluation is conducted to verify that the proposed protocol outperforms the most related scheme in terms of security and efficiency aspects. Finally, the Scyther simulation validates the security robustness of the new protocol.**

***Keywords*- Management; Network; Mobility; Security; Authentication.**

I. INTRODUCTION

Due to the wide proliferation of the automotive industry, the smart transportation system has emerged as a significant part of the smart city concept to introduce luxury and safety services to a variety of citizens through establishing fast secured connections between mobile nodes on the road and the intelligent city infrastructure [1], [2]. One of the advanced technologies that has emerged with smart cities to improve the effectiveness of transportation networks is the vehicular adhoc network (VANET). To set up the VANET architecture, three network partners are collaborated together as follows: Vehicles can be considered as portable nodes which are equipped with a wireless device called onboard unit (OBU) and it is in order to satisfy wireless connections with other entities along their route. However, roadside units (RSUs), which are fixed nodes placed beside roadways to monitor the network traffic, can be distinguished from the central trusted authority (TA), which is in responsibility of the entity registration and generating public network parameters. Indeed, both RSUs and the TA are the two main components of the VANET infrastructure [3], [4]. Therefore, for optimal interactions with the surrounding environment, vehicles have to communicate with one another and with the infrastructure (V2V and V2I, respectively).

Particularly, the VANET design supports the dedicated short range communication (DSRC) protocol over wireless channels for both V2V and V2I in addition to wired channels between various infrastructure entities [5], [6]. Thus, the network adopts the heterogeneous environment.

According to the wireless characteristics of the VANET environment, the vehicular communications are susceptible to different types of attacks such as eavesdropping, impersonation, repudiation, jamming, and modification attacks [7]. These attacks can track, monitor, and modify the traffic exchanged between network participants. For more illustration, impersonation attacks allow unauthorized entities to gain network access and misuse network resources. In addition, changing the content of warning messages sent from RSUs to vehicles can lead to serious consequences for vehicle drivers' safety on the road, including accidents and death [8]. Attackers can cause a traffic congestion by sending various false messages over the network. That negatively consumes the network bandwidth. Also, jamming attacks can result in preventing vehicles from receiving sensitive information. All the previous attacks have negative effects on the network performance, resulting in the following consequences:

a. The packet drop ratio (PDR) can be specified as the number of dropped packets to the total packet sent. This term PDR is increased.
b. The overall network delay is badly affected.
c. The rate of successful message delivery over a communication channel, defined as network throughput, is reduced.

Consequently, strong authentication techniques are employed to ensure reliable vehicular connections in terms of privacy, security, and efficiency aspects [9]–[15]. Based on these techniques, different entities within the network can transparently exchange traffic messages to control the traffic congestion and reduce road accidents.

This paper’s main contributions are summarized below:

a. An efficient ultralightweight authentication protocol (EUAP) is proposed, supporting the data confidentiality feature and vehicle route plan privacy.
b. The proposed protocol addresses the key management problem and satisfies the high mobility requirements of vehicular networks.
c. A new model for the traditional public key infrastructure is introduced in order to preserve the identity privacy of movable nodes and ignore certificates transmission over wireless channels.

Table 1. Characteristics analysis

Items	[9]	[10]	[11]	[12]	[13]	[14]	[15]
Registration model	Wired	Wired	Wired	N/A	Wired	Wired	Wireless
Efficient authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
High mobility	No	No	No	No	No	No	No
Response to misbehaving action	No	No	No	No	No	No	No
Formal security analysis	No	Yes	No	No	No	No	Yes

d. This model also depends on the self-authentication principle to reduce the number of authentication steps during the entire phases of the protocol in addition to utilizing lightweight techniques such as Chebyshev chaotic maps and logical shift operations.

The structure of this paper is arranged as follows: The related work is illustrated in Section II. The definitions and notations of the proposed protocol are given in Section III. Besides, the proposed model overview is highlighted in Section IV. Moreover, the proposed authentication protocol is introduced in Section V. Throughout Section VI, the performance evaluation for the proposed model is discussed in detail. The security verification is outlined in Section VII. Finally, the conclusion is presented in Section VIII.

II. Related Work

A. *Existing schemes*

The following is a brief illustration for the relevant authentication schemes:

In [9], a self-authentication protocol using pseudonyms and group signatures is introduced to reduce the authentication cost. Although the protocol does not rely on a central trusted TA in its authentication procedures, it still utilizes heavy techniques such as bilinear mapping operations. Additionally, a secured authentication scheme that aims to minimize the message transfer rate during the authentication phase is given in [10]. This scheme fulfills the self-authentication principle, however, it complicates the authentication process by using a fuzzy extractor mechanism to safeguard the biometric template. The use of 32 hash functions throughout the entire scheme has also a negative impact on the computation overhead. To guarantee that emergency vehicles have clear emergency lanes on the road, a novel authentication approach is discussed in [11]. Despite the approach claims that the traffic congestion can be minimized by eliminating the recurring calculations, it is still based on complex fuzzy extractor mechanism in its processes. According to [12], a privacy preserving V2I authentication protocol is proposed to protect the vehicle route privacy along the road using the Moore curve mechanism. However, it is found that the protocol is mainly depended on the advanced encryption standard (AES), which increases the system complexity and limits the ability of VANET to meet its high mobility demands. The proposed protocol in [13] achieves the vehicle anonymity feature without using bilinear pairing processes, but it mainly relies on elliptic curve cryptography (EEC) that has a negative effect on the system implementation.

In [14], an efficient authentication scheme that utilizes the pseudonym-based technique to ensure mutual authentication between vehicles and RSUs is outlined. Besides, using several pseudonyms for each vehicle to sign different messages can result in significant storage overheads. With the help of Chebyshev chaotic maps, the protocol in [15] integrates the symmetric key cryptography with the public key signature to achieve the data confidentiality and the lightweight feature. However, it relies on static public/private key pairs for each network entity. That poses a threat to the vehicle privacy. Furthermore, the continuous exchange of symmetric session keys between vehicles and RSUs in the scheme [15] may result in key management problems. During the authentication session, different network entities require the authentication with the TA before the interaction with each other, leading to heavy communication overheads. According to Table 1, various comparisons between the existing schemes are conducted to illustrate the merits and demerits of each scheme as follows:

a. The wired channel is the common model for the registration of all entities in most schemes. However, the term "N/A" stands for "not available". Also, the term "Yes" indicates satisfying the feature.

b. No existing scheme meets the high mobility requirement for VANETs because most schemes depend on heavy-weight operations that take a long time to process, limiting vehicle mobility. More specifically, it is found that the schemes [9], [12], and [14] rely on complex bilinear operations. Despite a fuzzy extractor technique is used to protect biometric templates in the schemes [10] and [11], the elliptic curve cryptography (EEC) adds a complexity in the implementation of the scheme [13]. Although lightweight operations such as the Chebyshev chaotic maps are used in the scheme [15], excessive authentication procedures are performed to accomplish the authentication between the vehicle and the RSU due to the complete reliance on the central TA.

c. The term $\Delta \boldsymbol{m}$ indicates the maximum number of messages that can be sent from the vehicle to the RSU in a single session. Thus, Misbehaving action can be defined as sending various messages greater than $\Delta \boldsymbol{m}$ from the vehicle to the RSU in a single session. Subsequently, all the schemes ignore the real action of the TA to prevent network entities from dealing with the misbehaving vehicle.

d. Based on a formal verification program, only the schemes [10] and [15] evaluate their security robustness against various attacks. Although the security analysis depends on the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool for the scheme [10], it is relied on the Scyther simulation for the scheme [15].

B. *Problem definition*

The authentication protocols that are previously introduced can be classified as follows: Firstly, centralized schemes use a central trusted authority to accomplish the authentication processes between vehicles and the infrastructure, resulting in a high computational cost due to excessive authentication steps. Secondly, decentralized schemes ignore the dependency of the trusted authority for authenticating various network participants to each other. Besides, they employ sophisticated mechanisms such as fuzzy extractors and bilinear maps that restrict the network mobility. Thirdly, session key-based authentication protocols suffer from key management problems. Fourthly, traditional public key infrastructure-based schemes continuously exchange certificates between multiple entities. Therefore, the usage of static private/public key pairs in the scheme design may threaten the privacy. Subsequently, there is an imbalance between the security of each protocol and its efficiency. In this paper, an authentication protocol is proposed to address the shortcomings of the existing schemes by achieving the following:

a. The proposed protocol does not rely on a central TA to perform vehicle-to-RSU authentication procedures. As a result, the number of authentication messages is reduced to three. This is illustrated briefly in the new protocol's self-authentication stage.
b. The protocol also tries to meet the high mobility requirement by incorporating lightweight operations such as the Chebyshev chaotic map into its processes. Consequently, the computational cost is decreased, as indicated in the section on performance evaluation in this paper.
c. No certificate transmission over the medium is adopted in the new protocol's design. To solve key management problem, the entire procedures of the proposed protocol are based on public keys without the usage of symmetric keys. Moreover, no explicit transmission of the vehicle public key over the wireless network to protect the vehicle trip route and achieve the vehicle privacy.

The proposed protocol strikes an appropriate balance between the security and efficiency. The Scyther simulation confirms that the new protocol is secure against attacks. Additionally, the Wolfram Mathematica proves that the proposed protocol reduces computational, communication, and storage costs.

III. DEFINITIONS AND NOTATIONS

Highlightening on the main cryptographic tool of the proposed protocol procedures, a brief illustration of the Chebyshev chaotic map in its mathematical formulas is discussed throughout this section. Besides, all symbols used within this paper are described.

A. *Principles of Chebyshev chaotic map*

To support the proposed protocol with an efficient security level, the Chebyshev chaotic map is used for both encryption and signatures. According to the stochastic features of this map, a small change in the initial value can have a significant impact on its final outcome. As a result, the crucial traffic information that is exchanged between multiple network participants is preserved. For easy comprehension of the Chebyshev map nature, the following are brief summaries of its key characteristics:

a. Chebyshev map polynomial: Assume η is a random integer from the interval [-1, 1] and P is a big prime number [15]. Suppose m and r are both positive integers. Hence, two main formulas contribute in describing the Chebyshev map polynomial $\mathrm{T_m}(\eta)$ as follows: The trigonometric formula can be outlined using (1)[15]. Also, the recurrence formula is defined according to (2)[15].

$$\mathrm{T_m}(\eta) = \cos(m\,.\cos^{-1}(\eta)) \tag{1}$$

$$\mathrm{T_m}(\eta) = \begin{cases} 1 & \text{if}\, m = 0 \\ \eta & \text{if}\, m = 1 \\ 2\eta\,.\,\mathrm{T_{m-1}}(\eta) - \mathrm{T_{m-2}}(\eta) & \text{if}\, m \geq 2 \end{cases} \tag{2}$$

b. Chebyshev map-based Diffie Hellman problem: Given three known values η, $\mathrm{T_m}(\eta)$, and $\mathrm{T_r}(\eta)$, it is infeasible for the attacker to calculate the value of $\mathrm{T_{mr}}(\eta)$.
c. Commutative property: Given two integers *r* and *m*, the chaotic map can fulfill (3)[16].

$$\mathrm{T_r}(\mathrm{T_m}(\eta)) \equiv \mathrm{T_m}\big(\mathrm{T_r}(\eta)\big) \quad \bmod P \tag{3}$$

d. Semi-group feature: If the two values r and $\mathrm{T_m}(\eta)$ are provided, this characteristic can be satisfied according to (4)[16].

$$\mathrm{T_r}(\mathrm{T_m}(\eta)) \equiv \mathrm{T_{mr}}(\eta) \quad \bmod P \tag{4}$$

More details about various distinct attributes of chaotic maps are given in [16]–[18].

Table 2. Abbreviations used in the EUAP and their definitions.

Abbreviation	Definition
$\boldsymbol{n_1, n_2, n_3}$	Random values generated by the TA
$\boldsymbol{s, S}$	Private/Public key pair of the TA
$\mathbf{SP_1, SP_2, SP_3}$	Security parameters issued by the TA
$\mathbf{RSU_j}$	j th Roadside unit
$\boldsymbol{L_j}$	Unique location of $\mathrm{RSU_j}$
$\mathbf{OID_j}$	Original identity of $\mathrm{RSU_j}$
-	Arithmetic subtraction operator
$\boldsymbol{u_j, U_j}$	Private/public key pair for $\mathrm{RSU_j}$
$\mathbf{Veh_i}$	i th automobile
$\boldsymbol{t_s}$	Timestamps ranging from t_1 to t_3
$\mathbf{RID_i}$	Real identity of $\mathrm{Veh_i}$
$\boldsymbol{v_i}$	Signature key of $\mathrm{Veh_i}$ which is only known to the TA and the automobile itself
$\boldsymbol{V_i}$	Verification key of $\mathrm{Veh_i}$
$\mathbf{AID_i}$	Anonymous identity of $\mathrm{Veh_i}$ which is temporary every communication session
Shift	Logical shift operation
$\boldsymbol{L_i}$	location of $\mathrm{Veh_i}$ based on embedded GPS
$\boldsymbol{\Delta t}$	Allowed network latency
$\boldsymbol{\Delta m}$	The maximum number of messages that a vehicle can send to the RSU in a single session.
+	Arithmetic addition operator
PRq	Private request generated by $\mathrm{Veh_i}$
InverseShift	Right-shift operator which can be considered as the inverse of Shift function
PRp	Private reply created by $\mathrm{RSU_j}$

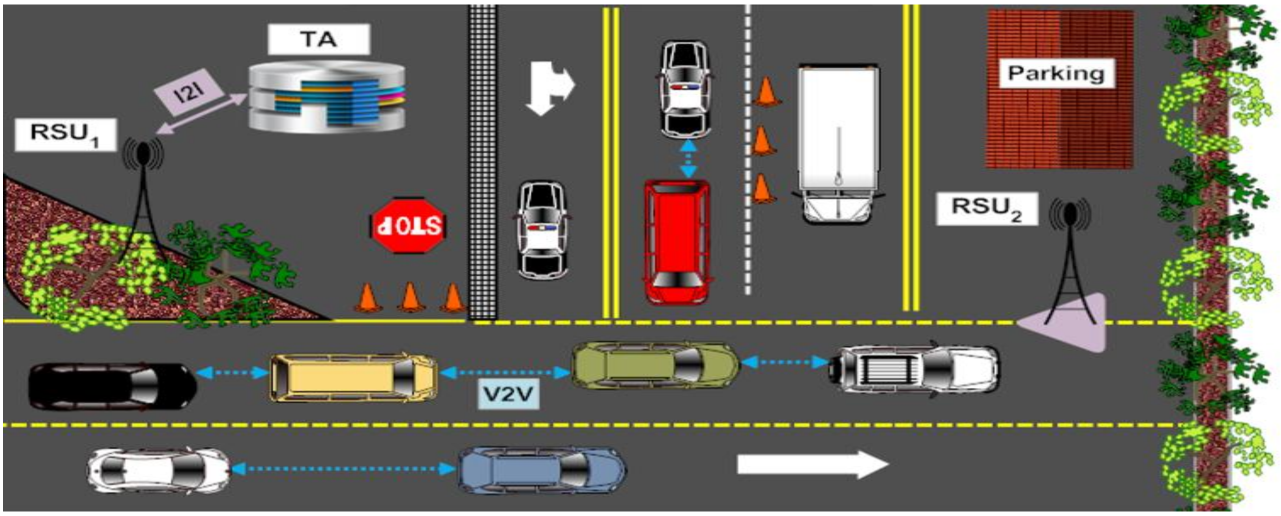


Figure 1. The EUAP network model: Indicating connections among vehicles (V2V) and interactions between different infrastructure partners (I2I).

B. Abbreviations within this paper

In Table 2, all abbreviations included in this paper in addition to their definitions are indicated. Besides, this table provides a description of various arithmetic operations integrated with the cryptographic functions to simplify understanding of the proposed protocol.

IV. PROPOSED MODEL OVERVIEW

In this section, the proposed design for the VANET model is introduced in addition to all the security requirements that have to be satisfied throughout the new protocol procedures as follows:

A. Design model

The network model, indicating its different participants is shown in Fig. 1. This figure is designed using SmartDraw program. This program can be defined as a commercial software that allows quick drawing of different types of diagrams and contains a large database of examples for each type of diagram [19]. The following are short notes about the various network participants and their functionalities:

Trusted authority (TA): It is supposed that the TA is an entity that has powerful functions to manage the entire network and it is also responsible for the registration process for all network participants.

a. To check the validity of license information, the TA is always connected to the motor-vehicle department. This enables the TA to validate the vehicle license and driver license. Additionally, only the TA has the ability to issue the network security parameters.

b. Roadside units (RSUs): Each RSU acts as a fixed node placed on the road to manage traffic information. Moreover, the RSU reduces congestion and warns of possible accidents.

c. Vehicles: Each vehicle has a global positioning system (GPS) to determine its unique location. To protect the vehicle privacy, two approaches are employed as follows: Firstly, no explicit transmission of RID_i over the wireless channels to preserve the vehicle real identity. Consequentially, only the TA and the vehicle itself can know the true value of RID_i. Also, each vehicle has two keys: The first key is the signature key that acts as a private key used to sign the vehicle transmitted messages. Although, using a static public key for the vehicle can be considered as a static identifier that distinguishes the messages of this vehicle, the pseudonyms avoid the vehicle tracking and preserve the vehicle privacy. These pseudonyms result in large storage and communication overheads that restrict the VANET mobility. Therefore, the second key for the vehicle is the verification key that is only known to the sending vehicle and receiving entity to avoid tracking the vehicle using its static public key. Secondly, recognizing the RSUs that a particular vehicle communicates with can aid in estimating the probably route that the vehicle will take based on the locations of the RSUs. Thus, a self-authentication mechanism is applied to achieve the authentication between vehicles and RSUs without the dependence on the TA to accomplish the authentication procedures. Furthermore, the TA cannot predict which RSU should interact with a specific vehicle during each communication session, which can help to secure the vehicle route.

The proposed model classifies the network participants into two main categories as follows. Firstly, a static environment refers to the various fixed nodes used in the network model. It is assumed that all the deployed RSUs along the road and the TA make up together the primary core of the VANET infrastructure. Besides, wired channels can be utilized to connect the various infrastructure partners. Secondly, all mobile nodes, such as vehicles, can represent a dynamic environment.

Two communication modes are adopted as follows: The term "inside-connection" refers to the communication among various mobile nodes, however, the interaction between different vehicles and RSUs is denoted by the term "outside connection". Also, both the previous modes are performed via wireless channels.

B. Security Specifications

The next explanations describe the security demands that are met by the proposed protocol.

a. Authentication: In accordance with this security requirement, each vehicle has to check the legitimacy of the RSU before sending it any confidential information. Additionally, the RSU verifies the vehicle authenticity before granting it access to its resources.

b. Confidentiality: The critical information sent through wireless channels needs to be protected from attackers. The proposed protocol is sufficiently secure against eavesdropping attacks due to this feature.

c. Unlinkability: The unauthorized entities cannot distinguish a specific vehicle according to its transmitted messages over the network. Using a static identifier such as the vehicle real identity may lead to tracking the vehicle by unauthorized entities. To avoid this security breach, a temporary identity is utilized to represent the vehicle and it is changed each session.

d. Traceability: This specification indicates the ability of the TA to extract the real identity of the misbehaving vehicle in order to trace it. As a result, no entity within the network can know the vehicle real identity except the TA and the vehicle itself

e. Identity privacy: Based on this security aspect, no static identifiers, such as the vehicle static verification key and the vehicle real identity, are explicitly transmitted over the wireless channel. Thus, this key is encrypted before being exchanged between the vehicle itself and the receiving RSU to protect the vehicle privacy.

f. Vehicle route privacy: The TA does not have the ability to determine the RSUs with which the vehicle interacts during its journey. In order to secure the vehicle trip route, the authentication procedures between the vehicle and each RSU are not relied on the TA.

g. High mobility: This feature refers to the fast interaction between the vehicle and each RSU along its path. Consequently, the proposed protocol relies on the lightweight operations such as the Chebyshev chaotic map to minimize the processing procedures on the vehicle side. Besides, the proposed protocol seeks to decrease the number of authentication steps, which contributes to a reduction in overall computations.

h. Freshness: All messages exchanged between various entities over wireless channels are checked for freshness. A timestamp is included in each message's formula to ensure that it is current and not out of date.

i. Solution to key management problems: The new protocol tries to solve the key management problem by ignoring the use of symmetric keys in its processes. Moreover, private/public key pairs are assigned to network participants.

j. Response to misbehaving action: When a vehicle misbehaves, both the RSU and the TA take action to avoid interacting with it. Also, a blacklist containing the verification key of this misbehaving vehicle is broadcasted to all deployed RSUs in the network to warn them against communicating with this vehicle.

k. Resistance to various attacks: The proposed protocol has to resist a variety of attacks, including repudiation, modification, and impersonation attacks. To withstand a repudiation attack, digital signatures based on the Chebyshev chaotic map are utilized to validate each message's source. Moreover, any attacker's trial to alter the exchanged traffic over the wireless channel should be detected to resist a modification attack. Furthermore, the proposed protocol's ability to resist any attempt by an attacker to impersonate an authorized entity leads to increasing the security level of the protocol against an impersonation attack.

V. PROPOSED AUTHENTICATION PROTOCOL

According to the existing schemes, each protocol has two main phases as follows: Firstly, the initialization phase, which includes the process of generating system parameters as well as the registration procedures. Secondly, the authentication phase that is accomplished between various network entities. As previously shown in Table 1. The majority of existing schemes use wired connections during the registration phase. The scheme [15] utilizes wireless channels during its processes. However, the proposed protocol depends on wired channels in its registration procedures. Additionally, Table 3 indicates various techniques that are used to issue system parameters and accomplish the authentication process in each scheme. Due to the use of complicated tools, the schemes [9]-[14] suffer from system complexity. The scheme [15] tries to reduce system complexity by relying on lightweight operations such as the Chebyshev Chaotic Map. This scheme does not address vehicle route privacy, which is a critical security issue. On one hand, tracking a specific vehicle using its messages can be considered as a security problem in the scheme [15]. On the other hand, the proposed protocol protects the vehicle route privacy and addresses the problem of vehicle tracking.

Table 3. Tools used to generate system parameters.

Scheme	Tools
[**9**]	Bilinear maps
[10]	One way hash function
[**11**]	Cyclic groups
[**12**]	Moore curves
[**13**]	Elliptic curves
[**14**]	Bilinear pairings
[15]	Chebyshev chaotic map
EUAP	Chebyshev chaotic map

In this section, the proposed protocol is introduced with its two new stages: The establishment phase and the self-authentication phase. A flow diagram for the protocol procedures is depicted in Fig. 2. Besides, a full explanation of each phase is provided as follows:

A. Establishment stage

Before allowing the VANET network to be activated within a country, the establishment stage has to be initiated to set the network parameters and register its all participants. According to this stage, the TA attempts to carry out multiple security procedures in order to generate global parameters and secret keys before starting the registration processes for all RSUs and vehicles. Subsequently, each procedure is illustrated below:

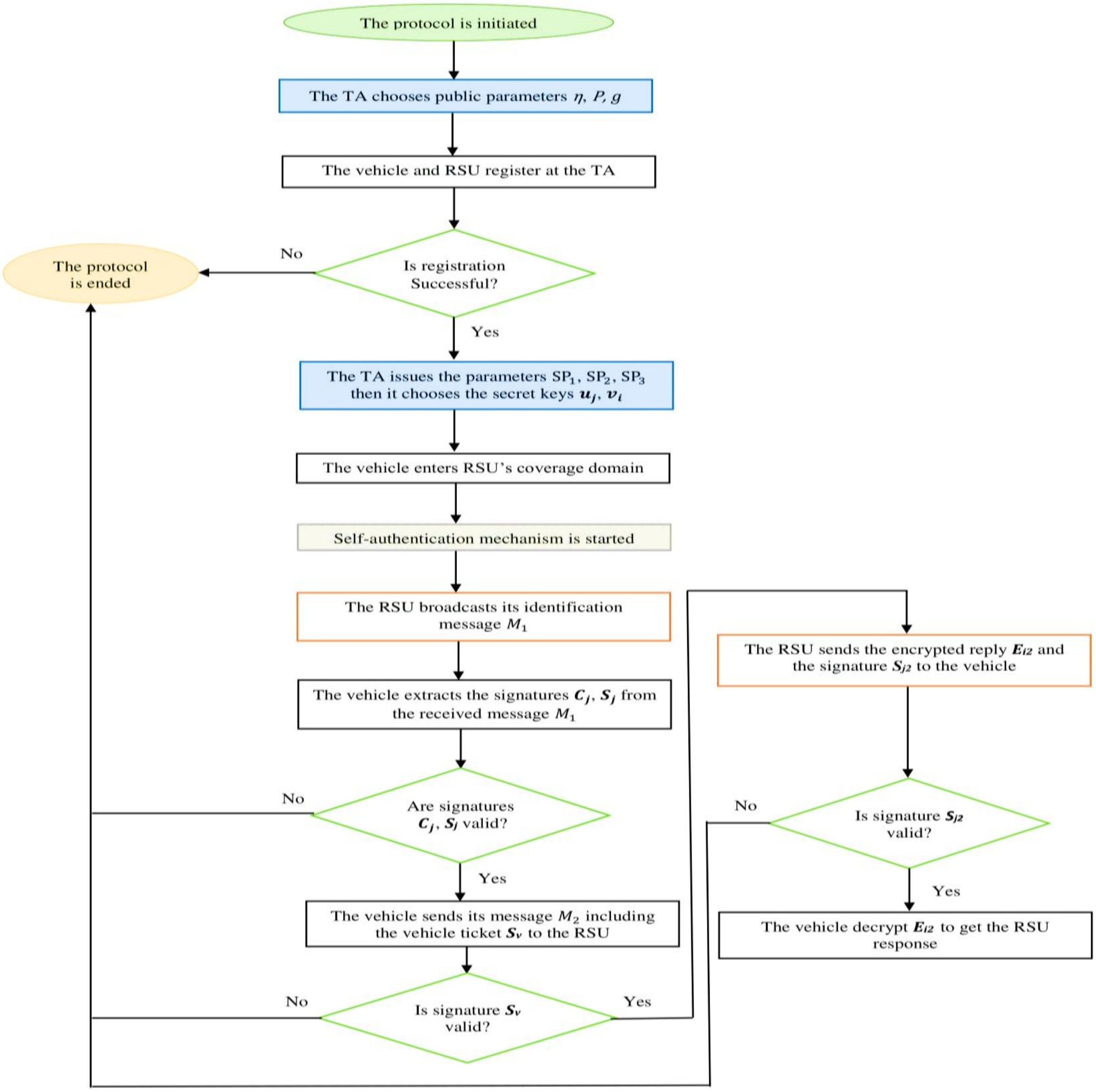

The protocol is initiated
The TA chooses public parameters η, P, g
The vehicle and RSU register at the TA
Is registration Successful?
No
The protocol is ended
Yes
The TA issues the parameters SP_1, SP_2, SP_3 then it chooses the secret keys u_j, v_i
The vehicle enters RSU's coverage domain
Self-authentication mechanism is started
The RSU broadcasts its identification message M_1
The vehicle extracts the signatures C_j, S_j from the received message M_1
No
Are signatures C_j, S_j valid?
Yes
The vehicle sends its message M_2 including the vehicle ticket S_v to the RSU
No
Is signature S_v valid?
Yes
The RSU sends the encrypted reply E_{i2} and the signature S_{j2} to the vehicle
No
Is signature S_{j2} valid?
Yes
The vehicle decrypt E_{i2} to get the RSU response

Figure 2. A comprehensive summarization of the proposed protocol's idea

The TA launches the first procedure by issuing the global network parameters η, P, and g as follows: A random integer η is selected from the interval [-1, 1]. Also, a large prime number P can be chosen to compute its generator g which fulfills the condition $[(g^{P-1}) \equiv 1 \mod P]$.

These parameters η, g, and P are defined to be public for all network participants. Besides, the TA declares the value of Δm to all network participants.

Next, the second procedure is started to generate the TA master secret key s and employ the Chebyshev map to obtain its corresponding public key S based on (5).

$$S = \mathrm{T}_{g^s}(\eta) \mod P \tag{5}$$

Then, the TA selects three random values n_1, n_2, and n_3 to aid in computing the network security parameters SP_1, SP_2, andSP_3, respectively. These parameters are involved in the exchanged signatures between various participants to secure the traffic information. The values g, s, and n_1 are integrated together using (6) to calculate the first parameter SP_1.

$$\mathrm{SP}_1 = \mathrm{T}_{g^s}(n_1) \mod P \tag{6}$$

Similarly, the two other parameters SP_2 and SP_3 are issued with the help of (7) and (8), respectively.

$$\mathrm{SP}_2 = \mathrm{T}_{g^s}(n_2) \mod P \tag{7}$$

$$\mathrm{SP}_3 = \mathrm{T}_{g^s}(n_3) \mod P \tag{8}$$

Following that, all the RSUs and vehicles must register at the TA and provide an authorized identification proving their legitimacy status. The RSU registration is firstly described and so is the vehicle registration.

a. RSU registration

The RSU registration process is illustrated in more detail as follows:

- Each RSU has to send a registration query that includes its unique location L_j to the TA.
- By comparing the received value of L_j to the TA embedded list, which contains all real locations for the installed RSUs inside the network, the TA can verify the correctness of the received location. As a consequence, the TA continues the registration process if the location is accurate. If not, the query is rejected.
- The TA issues the value $\mathrm{OID_j}$ which serves as the RSU original identification. Moreover, the TA depends on the Chebyshev chaotic map to compute the RSU public key U_j by first generating a private key for the RSU u_j and then utilizing (9) to do so. As a result, the TA begins to calculate the certified card C_j for the RSU public key in accordance with (10). Based on this card, the vehicle can check the authenticity of the RSU public key because the TA is the only entity that has the ability to issue C_j due to the fact that no RSU within the network is aware of the value of $\mathrm{SP_1}$ and no vehicle is able to determine the value of u_j.

$$U_j = \mathrm{T}_{g^{u_j}}(\eta) \mod P \tag{9}$$

$$C_j = \mathrm{T}_{g^{u_j - \mathrm{SP}_1}}(\eta) \mod P \tag{10}$$

Finally, the values $\{\mathrm{OID_j}, u_j, U_j, C_j, \mathrm{SP_2}, \mathrm{SP_3}\}$ are sent from the TA to the RSU via a wired channel. Besides, the TA broadcasts the public keys for all RSUs deployed in the network.

b. Vehicle registration

The vehicle registration procedure can be discussed in depth according to the following:

- Every vehicle sends a registration query to the TA with its genuine identity $\mathrm{RID_i}$ that contains the information of the driver's name, his national ID, and the vehicle license number.
- Upon receiving the previous query, the TA checks the validity of the vehicle identification information with the help of the motor-vehicle department. If the information is proved to be true, the TA proceeds the registration process. In any other case, the TA declines the query.
- The TA selects a random value for the vehicle anonymous identity $\mathrm{AID_i}$ that is changeable each communication session. Furthermore, the vehicle signature key v_i is chosen to compute its corresponding verification key V_i using (11).

$$V_i = \mathrm{T}_{g^{v_i}}(\eta) \mod P \tag{11}$$

- To prove the authenticity of V_i to the RSU, the TA calculates the certified card C_i by (12). Because the vehicle cannot acquire the value of $\mathrm{SP_2}$ and the RSU itself is unable to get the secret value of v_i, only the TA has the authority to generate this card C_i.

$$C_i = \mathrm{T}_{g^{v_i - \mathrm{SP}_2}}(\eta) \mod P \tag{12}$$

Lastly, the values $\{\mathrm{AID_i}, v_i, V_i, C_i, \mathrm{SP_1}, \mathrm{SP_3}\}$ are submitted to the vehicle by a wired channel.

A. Self-authentication stage

The timeline of the authentication stage is shown in Fig. 3. During this stage, both the vehicle and RSU try to authenticate each other without relying on the TA. The steps of this stage can be conducted using the security parameters generated in the previous stage as follows:

Step 1: The RSU aims to prove its legitimacy to the moving vehicles within the RSU coverage area. To accomplish this, the RSU obtains its own timestamp t_1 and retrieves the values $\{\mathrm{OID_j}, L_j, U_j, C_j, \mathrm{SP_3}\}$ from the memory before beginning the calculation of the authentication ticket S_j. Hence, this ticket is dependent on the sum of the three values $\mathrm{OID_j}$, L_j, and t_1. Let the term *x* be the sum result. With the help of the Chebyshev chaotic map, the formula of S_j can be constructed using *x*, the RSU private key u_j, and the security parameter $\mathrm{SP_3}$ as shown in (13).

$$S_j = \mathrm{T}_{g^{x + u_j - \mathrm{SP}_3}}(\eta) \mod P \tag{13}$$

Accordingly, the RSU broadcasts the message $M_1 = \{\mathrm{OID_j}, t_1, L_j, U_j, C_j, S_j\}$ over a wireless channel.

Step 2: After receiving the message M_1 at a timestamp t_1', the vehicle checks the refreshness of the received timestamp. The timestamp is fresh if (t_1' - t_1 < Δt) then the vehicle begins to get its own timestamp t_2 and continue the verification process. Otherwise, the communication session is closed. To accomplish the verification process, the vehicle gets its current location L_i from the embedded GPS. Based on ($|L_i$ - $L_j|$ < 600), the vehicle accepts the received message M_1. Otherwise, this message is declined. When the message M_1 is accepted, the vehicle restores the values of $\mathrm{SP_1}$ and $\mathrm{SP_3}$ from the memory and regenerates the value of *x* using the received values $\mathrm{OID_j}$, L_j, and t_1. The validation of the received signatures C_j and S_j can finally be performed using (14).

$$\mathrm{T}_{g^{\mathrm{SP}_1}}(C_j) \equiv \mathrm{T}_{g^{\mathrm{SP}_3 - x}}(S_j) \mod P \tag{14}$$

If the recalculated value of $\mathrm{T}_{g^{\mathrm{SP}_1}}(C_j) \bmod P$ equals the recomputed value of $\mathrm{T}_{g^{\mathrm{SP}_3 - x}}(S_j) \bmod P$, the vehicle initiates the Chebyshev cryptographic mechanism. This mechanism is primarily used to achieve the confidentiality because the vehicle private request, which includes a sensitive information about the driver and vehicle itself, is secured using a secret key K_2 against eavesdropping attacks. To generate this secret key, multiple steps are processed according to the following:

- The vehicle generates a random nonce n_4 to aid in the computation of the key identifier K_1 according to (15). This identifier is publicly transmitted from the vehicle to the RSU via the wireless channel and helps the RSU to recover the true value of the secret key K_2.

$$K_1 = \mathrm{T}_{g^{n_4}}(\eta) \mod P \tag{15}$$

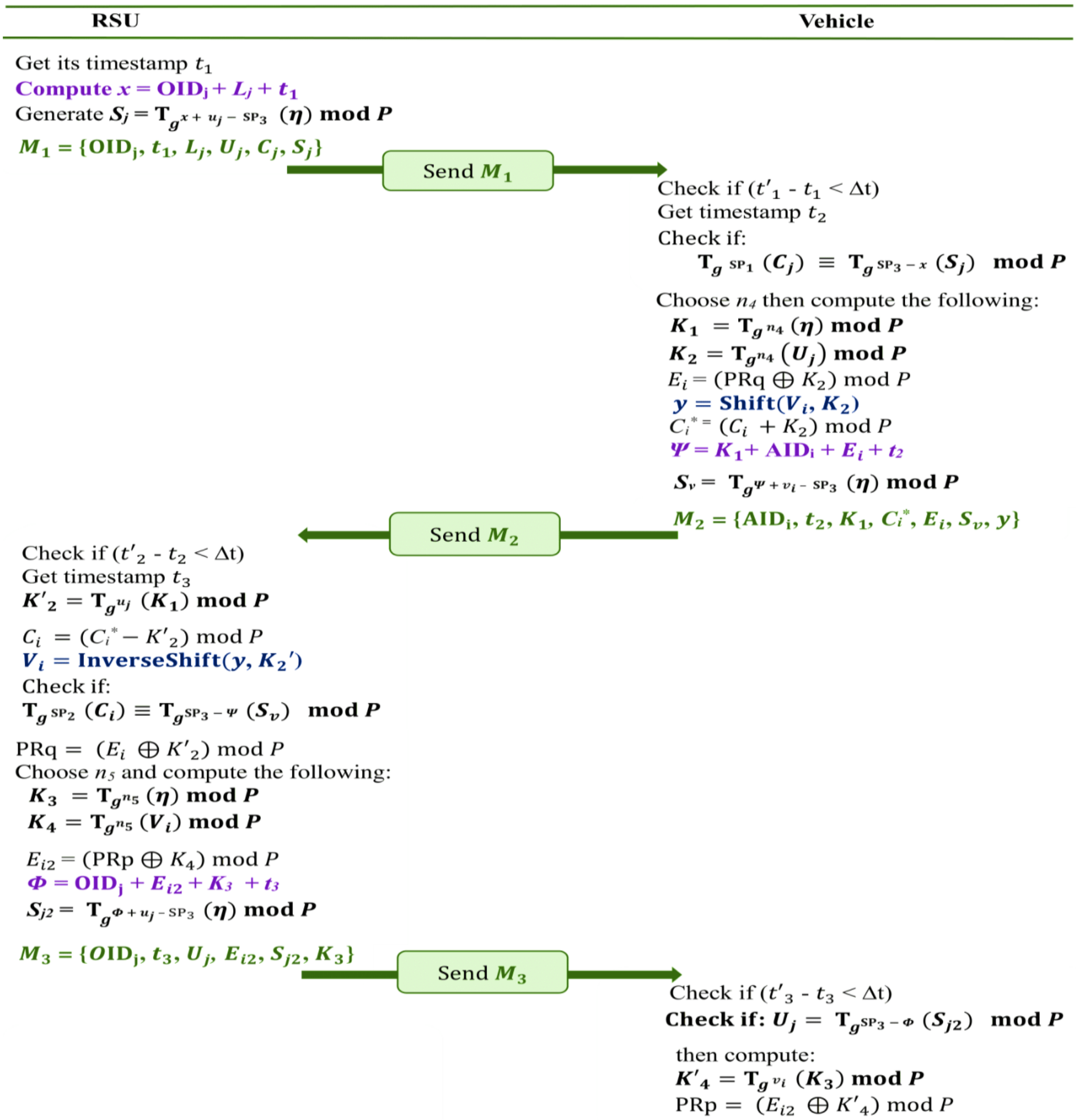

RSU
Vehicle
Get its timestamp t_1
Compute x = OID$_j$ + L_j + t_1
Generate $S_j = T_{g^{x+u_j-SP_3}}(\eta)$ mod P
M_1 = {OID$_j$, t_1, L_j, U_j, C_j, S_j}
Send M_1
Check if (t'_1 - t_1 < Δt)
Get timestamp t_2
Check if:
$T_{g^{SP_1}}(C_j) \equiv T_{g^{SP_3-x}}(S_j)$ mod P
Choose n_4 then compute the following:
$K_1 = T_{g^{n_4}}(\eta)$ mod P
$K_2 = T_{g^{n_4}}(U_j)$ mod P
E_i = (PRq ⊕ K_2) mod P
y = Shift(V_i, K_2)
C_i^* = (C_i + K_2) mod P
Ψ = K_1+ AID$_i$ + E_i + t_2
$S_v = T_{g^{\Psi+v_i-SP_3}}(\eta)$ mod P
M_2 = {AID$_i$, t_2, K_1, C_i^*, E_i, S_v, y}
Send M_2
Check if (t'_2 - t_2 < Δt)
Get timestamp t_3
$K'_2 = T_{g^{u_j}}(K_1)$ mod P
C_i = (C_i^* − K'_2) mod P
V_i = InverseShift(y, K_2')
Check if:
$T_{g^{SP_2}}(C_i) \equiv T_{g^{SP_3-\Psi}}(S_v)$ mod P
PRq = (E_i ⊕ K'_2) mod P
Choose n_5 and compute the following:
$K_3 = T_{g^{n_5}}(\eta)$ mod P
$K_4 = T_{g^{n_5}}(V_i)$ mod P
E_{i2} = (PRp ⊕ K_4) mod P
Φ = OID$_j$ + E_{i2} + K_3 + t_3
$S_{j2} = T_{g^{\Phi+u_j-SP_3}}(\eta)$ mod P
M_3 = {OID$_j$, t_3, U_j, E_{i2}, S_{j2}, K_3}
Send M_3
Check if (t'_3 - t_3 < Δt)
Check if: $U_j = T_{g^{SP_3-\Phi}}(S_{j2})$ mod P
then compute:
$K'_4 = T_{g^{v_i}}(K_3)$ mod P
PRp = (E_{i2} ⊕ K'_4) mod P

Figure 3. The timeline of authentication procedures in the proposed protocol.

Using (16), the vehicle relies on the public parameter g, the nonce n_4, and the RSU public key U_j to compute the secret key K_2. Hence, the vehicle private request PRq is secured using the key K_2 based on (17).

$$K_2 = \ T_{g^{n_4}}(U_j) \quad \text{mod}\ P \qquad (16)$$

$$E_i = (\text{PRq}\ \oplus\ K_2)\ \text{mod}\ P \qquad (17)$$

- To prevent tracking the vehicle using its static verification key V_i, this static key has to be securely exchanged between the vehicle itself and the RSU based on (18). Only the authorized RSU can recompute the value of the key K_2 and recover the real value of V_i. This results in preserving the vehicle identity privacy from unauthorized trackers.

$$y = \text{Shift}(V_i, K_2) \qquad (18)$$

- When the vehicle attempts to allow the RSU check the legitimacy of its verification key V_i, the certified card C_i that is previously generated by the TA has to be sent to the RSU itself. However, instead of sending the static value of C_i, the vehicle generates a temporary cover C_i^* to protect the vehicle certified card using (19).

$$C_i^* = (C_i + K_2)\ \text{mod}\ P \qquad (19)$$

- To help the RSU in determining whether or not the transmitted traffic is changed during the transmission over the wireless channel, the authentication ticket S_v is computed according to (20) with the help of several terms: v_i, ψ, and SP$_3$. The term ψ is the sum result of K$_1$, AID$_i$, E_i, and t_2. Furthermore, the vehicle itself cannot deny sending the ticket S_v because it is signed by the vehicle signature key v_i.

$$S_v = \ T_{g^{\psi+v_i-\text{SP}_3}}(\eta)\ \text{mod}\ P \qquad (20)$$

Finally, the vehicle sends the message M_2 = {AID$_i$, t_2, K_1, C_i^*, E_i, S_v, y} to the RSU using a wireless channel.

Step 3: When the RSU receives the message M_2 at a timestamp t_2', it verifies if the timestamp is fresh or not. According to (t_2' - t_2 < Δt), the timestamp is fresh and the RSU gets its current timestamp t_3 to continue the verification steps. Otherwise, the session is ended. To proceed the verification, the RSU begins to perform the following:

- The RSU recalculates the value of K_2' by (21). This value is utilized in recovering the original value of the vehicle certified card C_i using (22).

$$K_2' = \mathrm{T}_{g^{u_j}}(K_1) \bmod P \tag{21}$$

$$C_i = (C_i^* - K_2') \bmod P \tag{22}$$

- The RSU gets the true value of the vehicle verification key V_i according to (23). Therefore, it validates the correctness of the received signatures S_v and C_i by (24). Any attacker's attempt to alter the values of K_1, AID$_\mathrm{i}$, E_i, and t_2 leads to a mismatch in (24). If the term of $\mathrm{T}_{g^{\mathrm{sP}_2}}(C_i) \bmod P$ is equal to the term of $\mathrm{T}_{g^{\mathrm{sP}_3-\psi}}(S_v) \bmod P$, the RSU decrypts E_i to obtain the private service request PRq that is required by the vehicle according to (25).

$$V_i = \mathrm{InverseShift}(y, K_2') \tag{23}$$

$$\mathrm{T}_{g^{\mathrm{sP}_2}}(C_i) \equiv \mathrm{T}_{g^{\mathrm{sP}_3-\psi}}(S_v) \bmod P \tag{24}$$

$$\mathrm{PRq} = (E_i \oplus K_2') \bmod P \tag{25}$$

- To respond to the vehicle request PRq, the RSU generates its corresponding reply PRp and starts to encrypt this reply according to the Chebyshev cryptographic mechanism. Only three sub-steps have to be executed to compute the encrypted reply E_{i2} that can able to be transmitted over the wireless channel without exposing to the attacks such as eavesdropping attacks. These sub-steps can be summarized as follows: Firstly, a random nonce n_5 is selected to calculate the key identifier K_3 using (26). Secondly, to secure the reply PRp from eavesdropping attacks, the secret key K_4 is issued using the values n_5 and V_i according to (27). Thirdly, with the aid of K_4, the RSU private reply PRp is encrypted based on (28).

$$K_3 = \mathrm{T}_{g^{n_5}}(\eta) \quad \bmod P \tag{26}$$

$$K_4 = \mathrm{T}_{g^{n_5}}(V_i) \quad \bmod P \tag{27}$$

$$E_{i2} = (\mathrm{PRp} \oplus K_4) \bmod P \tag{28}$$

- To satisfy the non-repudiation feature, the RSU computes the authentication ticket S_{j2} as shown in (29). Besides, the term Φ can be defined as the summation of OID$_\mathrm{j}$, E_{i2}, K_3, and t_3.

$$S_{j2} = \mathrm{T}_{g^{\Phi + u_j - \mathrm{sP}_3}}(\eta) \bmod P \tag{29}$$

Consequently, the RSU sends the message M_3 = {OID$_\mathrm{j}$, t_3, K_3, U_j, E_{i2}, S_{j2}} to the vehicle by a wireless channel.

Step 4: Upon receiving the message M_3 at a timestamp t_3', the vehicle checks the refreshness of the received timestamp. Based on (t_3' - t_3 < Δt), the timestamp can be considered fresh and the vehicle verifies the received signature S_{j2} in addition to restoring the RSU private reply PRp. Otherwise, the session is closed. To check the validity of the received signature S_{j2}, the vehicle compares the value of $\mathrm{T}_{g^{\mathrm{sP}_3-\Phi}}(S_{j2}) \bmod P$ with the received value of U_j. In case of mismatching between the two previous values, the vehicle closes the session. Otherwise, the calculations are performed as follows: Firstly, the vehicle recomputes the value of K_4 using the key identifier K_3 and its verification key v_i as described in (30). Secondly, with the help of K_4', the private reply PRp is restored according to (31).

$$K_4' = \mathrm{T}_{g^{v_i}}(K_3) \bmod P \tag{30}$$

$$\mathrm{PRp} = (E_{i2} \oplus K_4') \bmod P \tag{31}$$

For the next session, the vehicle selects a new value for AID$_\mathrm{i}$. The vehicle anonymous identity is then updated with its new value NewAID$_\mathrm{i}$ and stored in the vehicle memory.

In case of misbehaving action: It is well-known that RSUs are network entities with less computation and storage capabilities than the TA [15], [20], [21]. Based on the step 3 of the self-authentication phase, when a vehicle sends multiple messages greater than Δm to the RSU in a single session, this is considered a possible attack. Subsequently, the RSU forwards these messages to the TA to deal with. Accordingly, the TA starts its verification procedures to determine the true identity of this vehicle. According to the Chebyshev chaotic map principle, the value of $\mathrm{T}_{g^{\mathrm{sP}_2}}(C_i) \bmod P$ is equal to the term $\mathrm{T}_{g^{\mathrm{sP}_3-\psi}}(S_v) \bmod P$. Also, the two previous values are equal to the value of $\mathrm{T}_{g^{v_i}}(\eta) \bmod P$ that refers to the vehicle static verification key V_i. This key can be an indicator to restore the corresponding stored values RID$_\mathrm{i}$ and v_i from the TA database. Besides, the TA puts the vehicle in the blacklist then this list is published to all RSUs to prevent dealing with the misbehaving vehicle.

VI. PERFORMANCE EVALUATION

In this section, various comparisons between existing schemes and the proposed protocol are conducted to emphasize the new protocol's relevance. Additionally, the Wolfram Mathematica simulation is utilized. This simulation can be defined as a mathematical software package that includes a number of built-in libraries for performing mathematical computations [22]. Moreover, the proposed protocol is compared with the most related scheme in terms of the computation, communication, and storage aspects. The simulation is run on a laptop with the following specifications: Intel (R) Core (TM) i7-3632QM CPU, 2.20 GHz, and RAM 8.00 GB.

A. Comparisons

As shown in Fig. 4, although the scheme [13] has the fewest number of tools, it is heavily based on cryptographic hash functions. Also, the scheme [9] has the highest tools. It is found that the main functions in the scheme [14] are hash, bilinear pairing, and elliptic curve operations that represent a complexity for the system implementation. The proposed protocol employs only 3 tools in its processes. According to Fig. 5, the scheme [10] has the least messages exchanged during the authentication phase because it can be specified as a decentralized scheme that achieves the self-authentication principle. However, it has the highest authentication steps. Subsequently, excessive authentication calculations are still a major problem in all existing schemes.

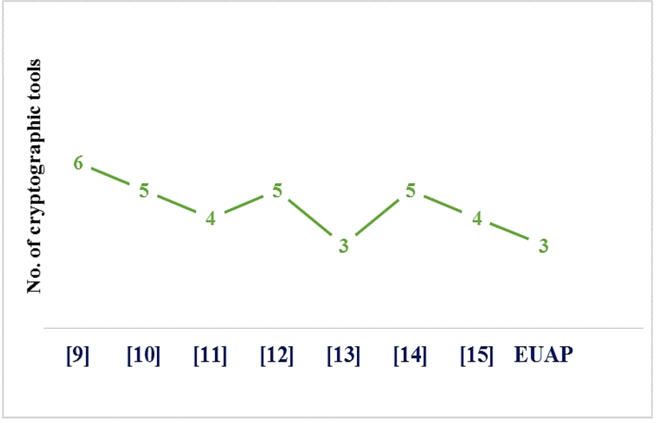


Figure 4. Number indicator of the various tools used in each protocol.

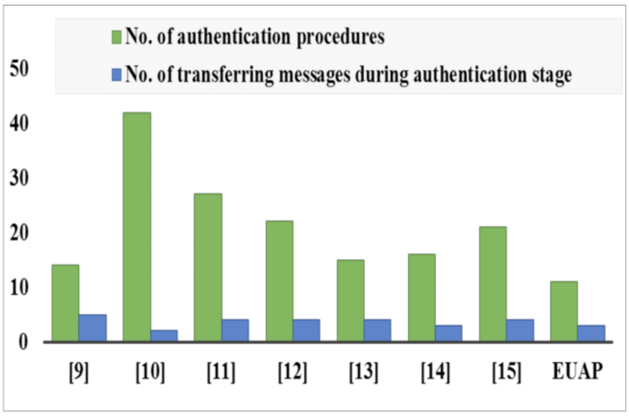


Figure 5. Comparison between different protocols according to the authentication process.

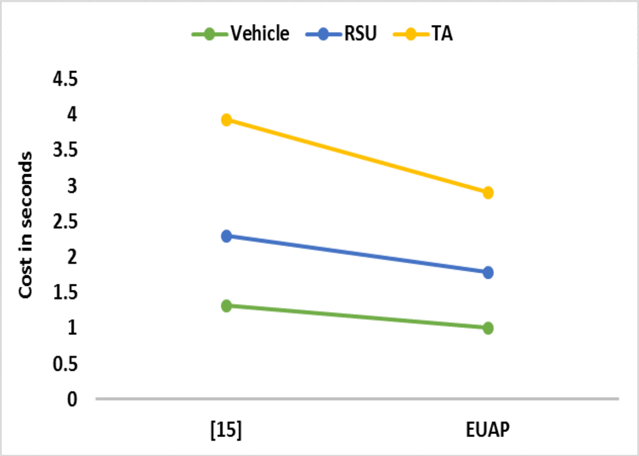


Figure 6. Reduction indicators in the computation costs for various network participants.

The scheme [15] is the most similar to the proposed protocol EUAP. The following are short summarizations of the similarity aspects between the two schemes:

- Both the schemes utilize the Chebyshev chaotic maps to issue the entity signatures. However, the scheme [15] depends on a key establishment mechanism to generate session keys between vehicles and RSUs, which causes key management issues.
- According to the two schemes, there is no continuous exchange of certificates between various network participants.

As indicated in Table 4, both the schemes achieve the data confidentiality feature in order to protect the vehicle private request and the RSU reply from any eavesdropping attempt over the wireless channel. According to the scheme [15], the authentication process between the vehicle and any RSU within the network is accomplished with the dependence on the TA. However, the proposed protocol is relied on the self-authentication mechanism to preserve the vehicle route privacy. On one hand, the symmetric key cryptography is incorporated with the public key signature to fulfill the lightweight property and non-repudiation characteristic in the scheme [15]. On the other hand, the proposed protocol is entirely based on public keys. The communication between RSUs and the TA is wireless in the scheme [15], but it is completely wired in the proposed protocol. The scheme [15] relies on assigning static public key for each vehicle, leading to a security breach. This breach may result in tracking a specific vehicle using its messages. No explicit transfer of the vehicle static public key over the wireless medium in the proposed protocol.

Table 4. Comparison between the scheme [15] and EUAP.

Characteristics	[15]	EUAP
Solve key management problem	No	Yes
Use lightweight operations	Yes	Yes
Confidentiality	Yes	Yes
Certificate independence	Yes	Yes
Route plan privacy	No	Yes

B. *Experimental simulations*

According to the previous subsection, the scheme [15] is the most similar scheme to the new proposed protocol. Both the schemes utilize the same tool, called “Chebyshev chaotic map” in its process. Additionally, both of them try to use lightweight operations. Subsequently, the performance of the new protocol is evaluated according to the simulation results previously indicated in the scheme [15]. The specifications of the simulation environment are the same in the two schemes. It is found that the new protocol is shown to be more lightweight than the scheme [15] in terms of computation, communication, and storage costs using Wolfram Mathematica simulation, as follows:

Firstly, significant reductions in the computation costs of the proposed protocol for the vehicle, RSU, and TA are introduced in Fig. 6. In this figure, the computational cost is estimated in seconds, and three indicator lines are used to represent the computation cost improvement for each network entity. The enhancement percentage on the vehicle side due to the new protocol is 24.21% based on the green line, but the RSU improvement percentage is 51.94% according to the blue line. Besides, the TA computation cost is enhanced by 60.28% using the proposed protocol.

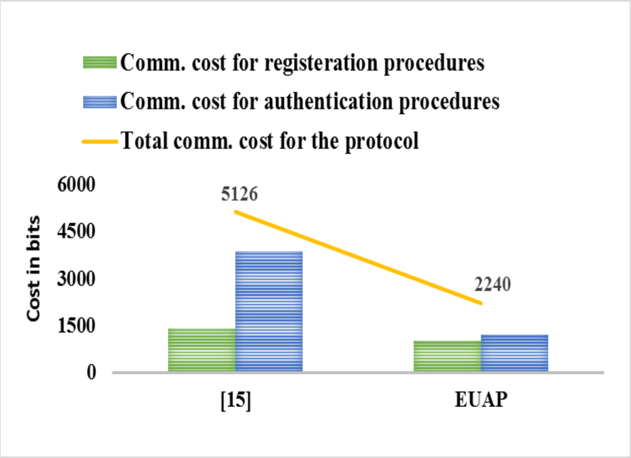


Figure 7. Communication overheads according to the different phases of each protocol.

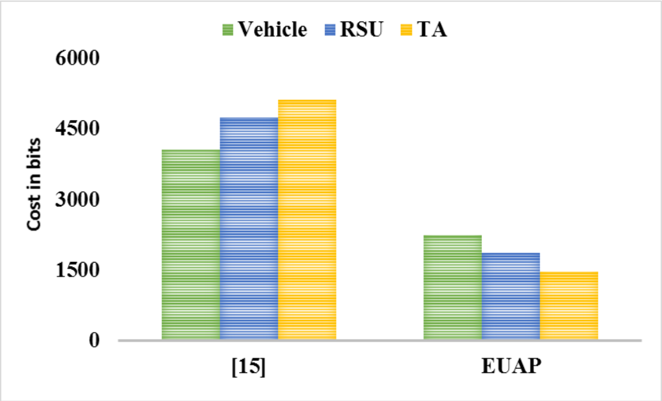


Figure 8. Storage overhead for each entity within different protocols.

Secondly, the communication cost refers to the number of bits transferred over the network during each protocol phase. Neither the scheme [15] nor the new protocol need more than 1500 bits for communication during the registration phase. As shown in Fig. 7, the communication cost for the proposed protocol throughout the authentication phase outperforms the scheme [15] with an improvement percentage 68.59%. Also, the yellow line in this figure represents 56.30% reduction in the total communication cost when using the new protocol versus the scheme [15].

Thirdly, the storage overhead is estimated in bits. According to Fig. 8, it is found that the vehicle storage in the proposed protocol is improved by 44.88%, compared to the scheme [15]. Moreover, the RSU and TA storage overheads are enhanced by 68.31% and 71.28%, respectively.

VII. SECURITY VERIFICATION

Throughout this section, two main verification methods are introduced to confirm the security robustness of the proposed protocol as follows: The first method is informal verification, which involves analyzing the core characteristics of the protocol procedures, whereas the second method includes a formal verification tool, which is utilized to test the resistance of the new protocol to various attacks.

A. *Informal security evaluation*

a. **Authentication:** Both the vehicle and RSU have to ensure the authenticity of each other by validating the correctness of the received signatures. On one hand, the vehicle verifies the legitimacy of the RSU by checking if the term of $\mathrm{T}_{g^{\mathrm{SP}_1}}(C_j) \bmod P$ equals the value of $\mathrm{T}_{g^{\mathrm{SP}_3 - x}}(S_j) \bmod P$. In case of matching, the RSU is authenticated to the vehicle because the value C_j is only issued by the TA for the authorized RSU. Besides, the TA is the only entity that can generate this value C_j using the RSU private key u_j and the security parameter SP_1, which the RSU does not know. On the other hand, when the vehicle attempts to confirm its authenticity to the RSU, it sends both the signatures C_i and S_v to the RSU. Subsequently, the RSU can verify if the value of $\mathrm{T}_{g^{\mathrm{SP}_2}}(C_i) \bmod P$ is equal to the value of $\mathrm{T}_{g^{\mathrm{SP}_3 - \psi}}(S_v) \bmod P$. Only the authorized vehicle has the true value of the certified card C_i that is specifically issued for it by the TA.

b. **Confidentiality:** To satisfy this feature, the vehicle request PRq and the RSU reply PRp are protected using the Chebyshev cryptographic mechanism. When the vehicle attempts to send an encrypted request E_i to the RSU, it issues a secret key K_2 based on a random nonce n_4 and the RSU public key U_j. Also, only the vehicle can know the real value of n_4. Although the authorized RSU can recover the value of K_2 with the help of the key identifier K_1, and the attackers cannot decrypt E_i without knowing the correct value of u_j. Similarly, the RSU reply PRp is secured according to the secret key K_4, which is relied on a random nonce n_5. This nonce is only known to the RSU. Additionally, without the vehicle signature key v_i, the attackers are unable to compute the value of K_4.

c. **Unlinkability:** Each vehicle has a unique anonymous identity $\mathrm{AID_i}$ that changes with each session. Furthermore, the attacker cannot identify a specific vehicle based on the traffic transmitted over the wireless channel because the message sent from the vehicle to the RSU must be distinct per session. To achieve this, the message M_2 are dependent on variable parameters such as a timestamp t_2 and a random key identifier K_1. It is found that the cover C_i^* is changeable according to K_2, which varies between sessions due to the changeable value of n_4. Also, the values E_i, S_v, and y are relied on the variable value of K_2.

d. **Traceability:** No entity within the network can know the value of $\mathrm{RID_i}$ except the TA and the vehicle itself. Subsequently the TA can retrieve the true identity of the vehicle $\mathrm{RID_i}$ from its database using the vehicle indicator that can be represented by one of the two terms $\mathrm{T}_{g^{\mathrm{SP}_2}}(C_i) \bmod P$ or $\mathrm{T}_{g^{\mathrm{SP}_3 - \psi}}(S_v) \bmod P$.

e. **Identity privacy:** The message M_2 does not have any static identifiers that reflect the real identity of a specific $^{\text{vehicle}}$ $\mathrm{RID_i}$. Moreover, a temporary identity $\mathrm{AID_i}$ is utilized during protocol procedures and is changeable between sessions. Although the vehicle verifies the authenticity of the RSU before sending it any messages, the vehicle verification key V_i is not transferred explicitly over the wireless channel. Using the secret key K_2, the value y is used to secure the transmission of V_i over the network. Hence, this key is only known to the vehicle itself and the authorized RSU that receives the vehicle traffic.

f. **Vehicle route privacy:** The TA is unaware of the vehicle trip route because both the vehicle and the RSU utilize the self-authentication principle and do not rely on the TA to complete the authentication procedures. The vehicle can ensure the authenticity of the RSU by validating the signatures C_j and S_j. Subsequently, if the value of $[\mathrm{T}_{g^{sP_1}}(C_j) \bmod P]$ is equal to the value of $[\mathrm{T}_{g^{sP_3-x}}(S_j) \bmod P]$, the RSU is authenticated to the vehicle. Also, the vehicle can ensure its legitimacy to the RSU according to the values of C_i^* and S_v. Thus, the RSU restores the value of C_i from the cover C_i^* then it verifies if the value of $[\mathrm{T}_{g^{sP_2}}(C_i) \bmod P]$ is equal to the term $[\mathrm{T}_{g^{sP_3-\psi}}(S_v) \bmod P]$. In case of matching, the vehicle is confirmed as an authorized entity to the RSU.

g. **High mobility:** The new protocol is primarily based on three tools as mentioned below:

- The Chebyshev chaotic map: It is increasingly applied in various recent research papers due to its lightweight computations [15]–[18], [23], [24].
- The logical shift function and arithmetic (addition/subtraction) operations: According to [24], it is found that these tools require a negligible execution time.

Additionally, according to Fig. 3, the RSU broadcasts the message M_1 that only requires 1 Chebyshev function to issue the signature S_j. To respond to the RSU message, the vehicle executes the following:

- Verifying the correctness of the received signatures C_j and S_j necessitate 2 Chebyshev functions.
- Issuing the values K_1, K_2, and S_v necessiate 3 Chebyshev processes.
- Generating the encrypted request E_i and the cover C_i^* need 2 modular arithmetic operations.
- Issuing the value of y requires 1 shift operation.

To accept the message M_2 at the RSU, 2 Chebyshev functions are needed to validate the values of C_i and S_v. Following that, the RSU starts to generate its message M_3 by performing the following:

- Regenerating of the secret key K_2' needs 1 Chebyshev function in addition to issuing the values K_3, K_4, and S_{j2} necessitate 3 Chebyshev processes.
- Recovering the vehicle request PRq from the value E_i and generating the encrypted reply E_{i2} need 2 modular arithmetic operations.
- Recovering the vehicle verification key V_i from the value y requires 1 shift function.

Upon receiving the message M_3, the vehicle performs the operations below:

- Validating the correctness of the received signature S_{j2} requires 1 Chebyshev process.
- Generating the secret key K_4 needs 1 Chebyshev operation.
- Recovering the RSU reply PRp from E_{i2} necessitates 1 modular arithmetic operation.

Thus, the total processes for the vehicle to send its private request and receive the corresponding reply are 7 Chebyshev, 3 modular arithmetic, and 1 shift operations. However, the RSU necessitates 7 Chebyshev, 2 modular arithmetic, and 1 shift processes to validate the vehicle request and allow the vehicle to access RSU resources. The protocol can be regarded as an ultralightweight scheme because of the following:

- As illustrated in Fig. 3, the authentication process of the proposed protocol only involves the exchange of 3 messages between the vehicle and the RSU.
- The new protocol decreases its computational cost as shown in Fig 6.

The reduction in the number of messages transferred across the network, as well as the decrease in the computing time at each network entity, can clearly show that the protocol is fast in its processing.

h. **Freshness:** All messages exchanged over the wireless network include timestamps. Before accepting a message, any network entity has to check if the value of $(t_s'$ - $t_s)$ is lower than Δt. Otherwise, the timestamp is out of date and the message is declined.

i. **Solution to key management problem:** The proposed protocol is strictly public key-based and it ignores the use of symmetric keys in its processes to solve the key management problem.

j. **Response to misbehaving action:** In case of misbehaving action, the TA recovers the verification key of the misbehaving vehicle by using the value of $\mathrm{T}_{g^{sP_2}}(C_i) \bmod P$, which should equal the value of $\mathrm{T}_{g^{v_i}}(\eta) \bmod P$ depending on the Chebyshev chaotic map principle. As a result, this key is added to the TA blacklist, which is distributed to all deployed RSUs in the network, preventing them from dealing with this vehicle.

k. **Resistance to various attacks:** The new proposed protocol is resistant to repudiation, modification, and impersonation attacks according to the following:

- The protocol employs digital signatures based on the Chebyshev chaotic map to withstand the repudiation attack. Specifically, the RSU is unable to deny the transmission of the messages M_1 and M_3 due to the signatures S_j and S_{j2}, which are signed with the RSU private key u_j. Furthermore, the vehicle incorporates the signature S_v with the message M_2 in order to achieve the non-repudiation feature. Hence, no entity in the entire network can issue the correct value of S_v without the knowledge of the vehicle signature key v_i.
- Because the term *x* is included in the signature S_j, any attempt by the attacker to change the values $\mathrm{OID_j}$, L_j, or t_1 can have a negative impact on the value of S_j and be easily detected. Moreover, the

vehicle checks the correctness of the received signatures C_j and S_j before accepting the message M_1. Similarly, any attacker's attempt to alter the message M_2 causes a change in the value of S_v. Also, the message M_3 is protected against a modification attack due to the value S_{j2} that is able to detect any modification in the message.

- To impersonate the RSU, the attackers have to issue the signatures S_j and S_{j2}, which are signed by the RSU private key u_j. Only the authorized RSU knows the real value of u_j. Additionally, the authorized vehicle is the only entity that has the signature key v_i to generate S_v.

B. *Formal verification analysis*

The new protocol security has assessed using the Scyther formal validation tool because of its flexibility and reliability. This tool can be defined as a push-button tool with a graphical user interface (GUI) that analyzes the security properties of the protocol and validates its security strength in response to various attack scenarios.

Some of the Scyther features are illustrated below:

- The Scyther can detect a wide range of attacks.
- The roles can be described as a series of events.
- Each role can interact with the others through the channels denoted by the terms "send" and "recv."
- To build the protocol model in the Scyther environment, the Security Protocol Description Language (SPDL) is utilized to write the code.

According to Fig. 9, the Scyther result shows that the proposed protocol is secured against attacks. Besides, the term "Secret" refers to protecting the data from an attacker during protocol sessions. Hence, based on the Scyther simulation, it is proved that the private key of the RSU "u" in addition to the TA private key "s" are "Secret". Also, the real identity of the vehicle is represented by "IDi" and is considered "Secret". The random values "n1", "n2", and "n3" are confirmed as "Secret". Although the vehicle request PRq is denoted by "Reqt" in the Scyther, the RSU reply PRp is symbolized by "Reply". The term "Alive" refers to successfully accomplishing the authentication process at the entity. Moreover, the term "Weakagree" refers to completing a run of the scheme, apparently with another entity. According to the Scyther script, the key K4 is expressed as "mod(Cheby(g,n5,V(Vehicle)),P)". More detailed information about the Scyther characteristics can be found in [25]–[27].

Finally, the proposed protocol is shown to be efficient throughout this paper for the following reasons:

- Based on Fig. 4, the proposed protocol utilize few number of tools. According to [15]-[18], [24], these tools are considered as lightweight functions.
- As previously illustrated in the section VI, the performance of the new protocol has evaluated according to the Wolfram Mathematica program, proving that the proposed protocol has lower computational, communication, and storage costs than the most closely related scheme [15].
- According to Fig. 9, the Scyther tool confirms that the proposed protocol is secure against attacks.

VIII. Conclusion

This paper introduces a VANET authentication protocol that is based on the Chebyshev cryptographic mechanism to secure the vehicle sensitive information exchanged over wireless channels. Despite the fact that this protocol addresses the key management issue by ignoring the use of symmetric keys within its configuration, it modifies the traditional public key infrastructure principle in order to avoid the incessant reliance on certificate exchange among network entities.

Comparisons with existing schemes have been performed to highlight the proposed protocol significance and its key attributes.The usage of lightweight operations such as Xor, the logical shift, and Chebyshev chaotic processes throughout the protocol structure, as well as the reduction in the number of the authentication procedures, result in an ultralightweight protocol that supports the high mobility feature. Therefore, the Wolfram Mathematica simulation reveals that the proposed protocol outperforms the most related scheme in terms of the vehicle computation and total communication costs by 24.21% and 56.30%, respectively. Furthermore, the Scyther simulation has been utilized to formally validate the proposed protocol's security robustness.

Funding:
This research has not received any type of funding.

Conflicts of Interest:
The authors declare that there is no conflict of interest.

References

[1] Kashif Naseer Qureshi, Adi Alhudhaif, Syed Wasim Haidar, Saqib Majeed, and Gwanggil Jeon, "Secure data communication for wireless mobile nodes in intelligent transportation systems," in *Microprocessors and Microsystems*, vol. 90, pp. 104501, Apr. 2022, doi: 10.1016/j.micpro.2022.104501.

[2] Besma Zeddini, Mohamed Maachaoui, and Youssef Inedjaren, "Security Threats in Intelligent Transportation Systems and Their Risk Levels," in *Risks*, vol. 10, no. 5, pp. 91, Apr. 2022, doi: 10.3390/risks10050091.

[3] Amandeep Verma, Rahul Saha, Gulshan Kumar, and Tai-hoon Kim, "The Security Perspectives of Vehicular Networks: A Taxonomical Analysis of Attacks and Solutions," in *Applied Sciences*, vol. 11, no. 10, pp. 4682, May 2021, doi: 10.3390/app11104682.

[4] Michael Lee, and Travis Atkison, "VANET applications: Past, present, and future," in *Vehicular Communications*, vol. 28, pp. 100310, Apr. 2021, doi: 10.1016/j.vehcom.2020.100310.

[5] Fabio Arena, Giovanni Pau, and Alessandro Severino, "A Review on IEEE 802.11p for Intelligent Transportation Systems," in *JSAN*, vol. 9, no. 2, pp. 22, Apr. 2020, doi: 10.3390/jsan9020022.

[6] Muhammad Naeem Tahir, Pekka Leviäkangas, and Marcos Katz, "Connected Vehicles: V2V and V2I Road Weather and Traffic Communication Using Cellular Technologies," in *Sensors*, vol. 22, no. 3, pp. 1142, Feb. 2022, doi: 10.3390/s22031142.

[7] Sagheer Ahmed Jan, Noor Ul Amin, Mohamed Othman, Mazhar Ali, Arif Iqbal Umar, and Abdul Basir, "A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues," in *IEEE Access*, vol. 9, pp. 153701–153726, 2021, doi: 10.1109/ACCESS. 2021.3125521.

[8] Thenuka Karunathilake and Anna Förster, "A Survey on Mobile Road Side Units in VANETs," in *Vehicles*, vol. 4, no. 2, pp. 482–500, May 2022, doi: 10.3390/vehicles4020029.

[9] Haobin Jiang, Lei Hua, and Lukuman Wahab, "SAES: A self checking authentication scheme with higher efficiency and security for VANET,"

in *Peer-to-Peer Netw. Appl.*, vol. 14, no. 2, pp. 528–540, Mar. 2021, doi: 10.1007/s12083-020-00997-0.

[10] Tarak Nandy, Mohd Yamani Idna Idris, Rafidah Md Noor, Ashok Kumar Das, Xiong Li, Norjihan Abdul Ghani, and Sananda Bhattacharyya, "An enhanced lightweight and secured authentication protocol for vehicular adhoc network," in *Computer Communications*, vol. 177, pp. 57–76, Sep. 2021, doi: 10.1016/j.comcom.2021.06.013.

[11] Chen Wang, Rui Huang, Jian Shen, Jianwei Liu, Pandi Vijayakumar, and Neeraj Kumar, "A Novel Lightweight Authentication Protocol for Emergency Vehicle Avoidance in VANETs," in *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14248–14257, Sep. 2021, doi: 10.1109/JIOT.2021.3068268.

[12] Songzhan Lv and Yining Liu, "PLVA: Privacy-Preserving and Lightweight V2I Authentication Protocol," in *IEEE Trans. Intell. Transport Syst.*, vol. 23, no. 7, pp. 6633–6639, Jul. 2022, doi: 10.1109/TITS.2021.3059638.

[13] Udit Bansal, Jayaprakash Kar, Ikram Ali, and Kshirasagar Naik, "IDCEPPA: Identity-based Computationally Efficient Privacy-Preserving Authentication scheme for vehicle-to-vehicle communications," in *Journal of Systems Architecture*, vol. 123, pp. 102387, Feb. 2022, doi: 10.1016/j.sysarc.2021.102387.

[14] Peng Wang and Yining Liu, "SEMA: Secure and Efficient Message Authentication Protocol for VANETs," in *IEEE Systems Journal*, vol. 15, no. 1, pp. 846–855, Mar. 2021, doi: 10.1109/JSYST.2021.3051435.

[15] Roayat I. Abdelfatah, Nermeen M. Abdal-Ghafour, and Mohamed E. Nasr, "Secure VANET Authentication Protocol (SVAP) Using Chebyshev Chaotic Maps for Emergency Conditions," in *IEEE Access*, vol. 10, pp. 1096–1115, 2022, doi: 10.1109/ACCESS.2021.3137877.

[16] Jihyeon Ryu, Dongwoo Kang, Dongho Won, and A. Braeken, "Improved Secure and Efficient Chebyshev Chaotic Map-Based User Authentication Scheme," in *IEEE Access*, vol. 10, pp. 15891–15910, 2022, doi: 10.1109/ACCESS.2022.3149315.

[17] Jing Li, Tianshu Fu, Changfeng Fu, and Lianfu Han, "A Novel Image Encryption Algorithm Based on Voice Key and Chaotic Map," in *Applied Sciences*, vol. 12, no. 11, pp. 5452, May 2022, doi: 10.3390/app12115452.

[18] Rasika B. Naik and Udayprakash Singh, "A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption," in *Ann. Data Sci.*, pp. 1–26, 2022, doi: 10.1007/s40745-021-00364-7.

[19] Wen-Kai Tai, Hao-Cheng Wang, Cheng-Yu Chiang, Chin-Yueh Chien, Kevin Lai, Tseng-Chang Huang, "RTAIS: Road Traffic Accident Information System," in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2018, doi: 10.1109/HPCC/SmartCity/DSS44701.2018.

[20] Guangquan Xu, Xiaotong Li, Litao Jiao, Weizhe Wang, Ao Liu, Chunhua Su, Xi Zheng, Shaoying Liu, and Xiaochun Cheng, "BAGKD: A Batch Authentication and Group Key Distribution Protocol for VANETs," in *IEEE Communications Magazine*, vol. 58, no. 7, pp. 35–41, July 2021, doi: 10.1109/MCOM.001.2000118.

[21] Meng Li, Liehuang Zhu, and Xiaodong Lin, "Efficient and Privacy-Preserving Carpooling Using Blockchain-Assisted Vehicular Fog Computing," in *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4573–4584, June 2019, doi: 10.1109/JIOT.2018.2868076.

[22] Fadi T. El-Hassan, "Experimenting With Sensors of a Low-Cost Prototype of an Autonomous Vehicle," in *IEEE Sensors Journal*, vol. 20, no. 21, pp. 13131-13138, Nov. 2021, doi: 10.1109/JSEN.2020.3006086.

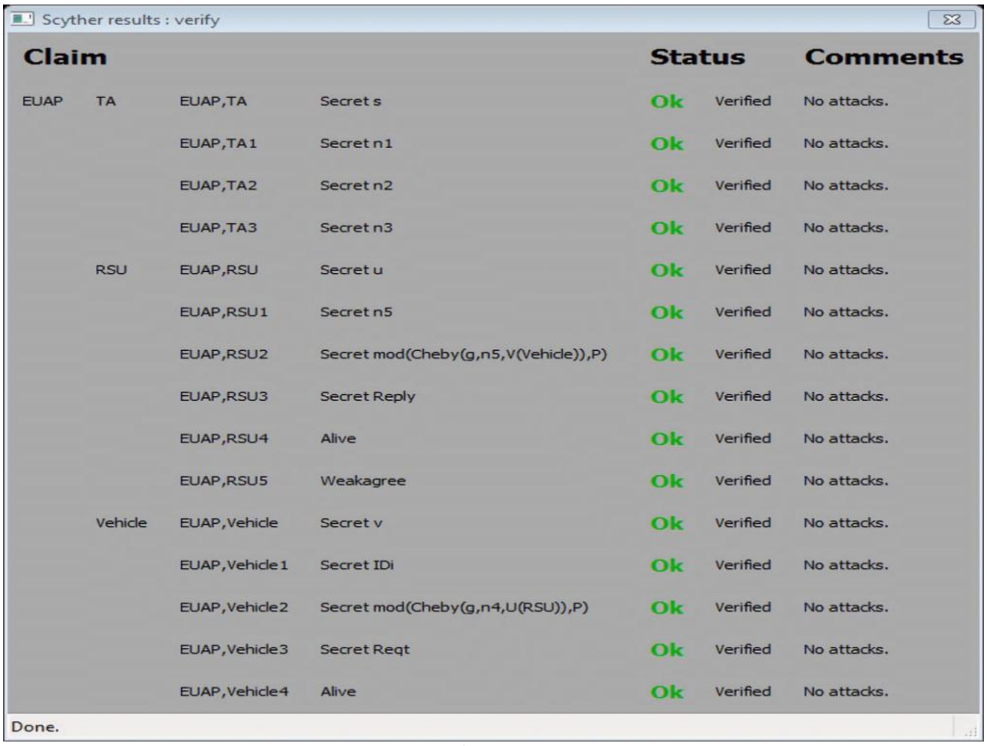
[23] Mahmood A. Al-Shareeda, Selvakumar Manickam, Badiea Abdulkarem Mohammed Alshaibani, Zeyad Ghaleb Al-Mekhlafi, Amjad Qtaish, Abdullah J. Alzahrani, Gharbi Alshammari, Amer A. Sallam, and KHALIL ALMEKHLAFI, "Chebyshev Polynomial-Based Scheme for Resisting Side Channel Attacks in 5G-Enabled Vehicular Networks," in *Applied Sciences*, vol. 12, no. 12, pp. 5939, Jun. 2022, doi: 10.3390/app12125939.

[24] Muhammed Jassem Al-Muhammed and Raed Abu Zitar, "Light and Secure Encryption Technique Based on Artificially Induced Chaos and Nature Inspired Triggering Method," in *Symmetry*, vol. 14, no. 2, pp. 218, Jan. 2022, doi: 10.3390/sym14020218.

[25] Ruhul Amin, Isha Pali, and Venkatasamy Sureshkumar, "Software Defined Network enabled Vehicle to Vehicle secured data transmission protocol in VANETs," in *Journal of Information Security and Applications*, vol. 58, pp. 102729, May 2021, doi: 10.1016/j.jisa.2020.102729.

[26] P. R. Babu, R. Amin, A. G. Reddy, A. K. Das, W. Susilo, and Y. Park, "Robust Authentication Protocol for Dynamic Charging System of Electric Vehicles," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11338–11351, Nov. 2021, doi: 10.1109/TVT.2021.3116279.

[27] Manojkumar Vivekanandan, Sastry V. N., and Srinivasulu Reddy U., "Blockchain based privacy preserving user authentication protocol for distributed mobile cloud environment," in *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1572–1595, May. 2021, doi: 10.1007/s12083-020-01065-3.



Scyther results : verify

Claim				Status		Comments
EUAP	TA	EUAP,TA	Secret s	Ok	Verified	No attacks.
		EUAP,TA1	Secret n1	Ok	Verified	No attacks.
		EUAP,TA2	Secret n2	Ok	Verified	No attacks.
		EUAP,TA3	Secret n3	Ok	Verified	No attacks.
	RSU	EUAP,RSU	Secret u	Ok	Verified	No attacks.
		EUAP,RSU1	Secret n5	Ok	Verified	No attacks.
		EUAP,RSU2	Secret mod(Cheby(g,n5,V(Vehicle)),P)	Ok	Verified	No attacks.
		EUAP,RSU3	Secret Reply	Ok	Verified	No attacks.
		EUAP,RSU4	Alive	Ok	Verified	No attacks.
		EUAP,RSU5	Weakagree	Ok	Verified	No attacks.
	Vehicle	EUAP,Vehicle	Secret v	Ok	Verified	No attacks.
		EUAP,Vehicle1	Secret IDi	Ok	Verified	No attacks.
		EUAP,Vehicle2	Secret mod(Cheby(g,n4,U(RSU)),P)	Ok	Verified	No attacks.
		EUAP,Vehicle3	Secret Reqt	Ok	Verified	No attacks.
		EUAP,Vehicle4	Alive	Ok	Verified	No attacks.

Done.

Figure 9. Simulation result of the proposed protocol based on the Scyther