IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 19, 2021, accepted December 16, 2021, date of publication December 23, 2021,
date of current version January 5, 2022.

Digital Object Identifier 10.1109/ACCESS.2021.3137877

Secure VANET Authentication Protocol (SVAP) Using Chebyshev Chaotic Maps for Emergency Conditions

ROAYAT I. ABDELFATAH, NERMEEN M. ABDAL-GHAFOUR, AND MOHAMED E. NASR
Electronics and Electrical Communications Engineering Department, Faculty of Engineering, Tanta University, Tanta 31527, Egypt
Corresponding author: Nermeen M. Abdal-Ghafour (nermeenmohamed@f-eng.tanta.edu.eg)

ABSTRACT It is crucial to support emergency applications provided by vehicular adhoc network (VANET) through enabling vehicles to quickly access to the infrastructure and consequently request rescue services. Additionally, the communication channels between vehicles and the infrastructure lack various security features due to the inferior wireless characteristics of their environment. However, most of the existing authentication schemes which are used to fix the security drawbacks lead to heavy computations and large storage burdens on the vehicle onboard unit (OBU). These schemes utilize secure channels while distributing the network parameters between the various participants. Yet, it is not efficient to establish secure channels during the interactions between entities. Furthermore, lightweight cryptography is an efficient security solution which is adequate for OBU to maintain a reasonable efficiency with low computational and communication costs. Two basic demerits for lightweight authentication protocols are highlighted as follows: Firstly, symmetric key-based authentication protocols dismiss achieving non-repudiation feature, leading to several security attacks in VANET. Secondly, public key-based authentication schemes are relied on elliptic curve cryptography (ECC) which makes the protocol implementation more difficult. Hence, this paper introduces a novel authentication protocol that utilizes Chebyshev chaotic maps to secure connectivity between the vehicles and infrastructure without using secure channels to distribute the network parameters. The new protocol combines the concept of the symmetric key cryptography with the public key signature to satisfy both the lightweight property and non-repudiation feature. Thus, this protocol introduces a novel network model which is the lowest hardware complexity, compared with others. The performance analysis is performed by Wolfram Mathematica, proving that the proposed protocol is superior in terms of security and performance aspects; its computation and storage costs of OBU are enhanced with 24.09% and 16.99%, respectively, compared to the most competing scheme. Besides, the Scyther simulation confirms the security of the protocol.

INDEX TERMS Vehicles, infrastructure, security, authentication, lightweight, non-repudiation.

I. INTRODUCTION

Due to the massive deployment of intelligent transportation system (ITS) in smart cities, the vehicular adhoc network (VANET) has attracted a deliberate attention in the research domain; the major goals of VANET are to support numerous applications in terms of infotainment, emergency, and traffic safety services [1], [2]. In general, VANET structure has three main components as follows: Firstly, onboard units (OBUs) mounted on vehicles to allow them connect with each other by the dedicated short range communication (DSRC) protocol. As long as vehicles move on the road, sharing messages and requesting keys are continuous processes [3]. Secondly, roadside units (RSUs) are wireless units distributed along the road to collect and analyze messages, and take intelligent traffic actions. Thirdly, the trusted authority (TA) is responsible for managing the whole entities in the network and issuing the system parameters. All vehicles and RSUs must register at the TA, which has the highest capabilities in terms of storage and communication, before allowing them to join VANET [1]. Although the secure communication channels are used to exchange messages between the RSUs

The associate editor coordinating the review of this manuscript and approving it for publication was Yassine Maleh.

and TA, the open wireless medium is utilized for transmitting messages between the vehicles and RSUs [4]. Hence, various attacks are subjected on the wireless environment, resulting in a shortage in the security efficiency of VANET. These attacks are rising to track, monitor, and alter the traffic exchanged between the vehicles and infrastructure as indicated in [5]. Accordingly, several authentication protocols are previously proposed to strengthen the security of VANET against attacks [6]–[14]. In this paper, a new classification of authentication schemes is introduced. The authentication protocols can be classified into two recent categories as mentioned below:

- Protocols with certification dependency.
- Protocols without certification dependency.

Although the first category includes traditional public key infrastructure-based authentication protocols, the second one introduces symmetric key-based authentication schemes and certificateless-based authentication protocols. To provide a more detailed overview of the new classification, comprehensive short notes about the protocols in each category are outlined as follows: Discussing the first category of the new classification, it is found that a conditional privacy preserving authentication scheme using short-time region based certificate is introduced in [6]. Although the scheme does not require a fully trusted TA to generate the vehicle secrets, exchanging certificates is still a communication drawback in this scheme. Additionally, an identity-based authentication scheme that utilizes pseudonyms to ensure the privacy of the vehicle's driver is presented in [7]. This scheme achieves non-repudiation feature, however, it is mainly focused on the certificate revocation list (CRL) that hinders the communication process. In [8], an efficient authentication protocol which transmits a symmetric key in the public channel depending on Chinese remainder theorem (CRT) is proposed. The protocol uses low-level computing operations such as XOR operator and hash functions, but the certificate management is its main demerit. Moreover, a secure authentication protocol is introduced in [9] to successfully achieve the data confidentiality between the vehicle and infrastructure, but the secure channels are required for exchanging keys. Besides, the proposed scheme in [10] utilizes long-term certificate for each entity in the network to revoke the vehicle identity in the case of attack.

Highlighting on the second category of the new classification, an efficient certificateless authentication scheme that does not need bilinear pairing is discussed in [11]. Despite the scheme claims alleviating excessive authentication burden in the OBU side, it is mostly based on three cryptographic tools: CRT, elliptic curves, and hash functions, which negatively affect the system complexity. Lightweight authentication protocol-based on message authentication code (MAC) technique is described in [12]. In this scheme, the vehicle depends on using biological passwords to verify the authenticity of multiple drivers. However, its computation capability is constrained by the use of two classes for upgrading keys. In [13], a secure authentication protocol using Chebyshev chaotic map for remote diagnosis services of a vehicle is outlined. Although the protocol provides a strong security to the vehicle's owner depending on the complex properties of the chaotic map, it mainly requires a password and biometric template in its process. An additional hardware such as a biometric sensor is also needed for this scheme to capture the template.

According to [14], a lightweight authentication protocol for a vehicle to infrastructure communication is introduced using the principle of symmetric key cryptosystems. The protocol shares a secret key between the vehicle and RSU to allow them to communicate after the successful authentication with the TA is executed. Although this scheme attempts to utilize lightweight operations such as hash function and XOR operator, it is still not appropriate for the OBU limited resources. Furthermore, it is based on SHA-256 hash function that wastes a large storage space for storing its secret parameters. To state another drawback, the scheme needs a secure channel and does not achieve non-repudiation feature.

The major contributions of this research are as follows:

1) A novel network model is introduced with no secure channels through the whole design in order to reduce the cost of network deployment.
2) Secure VANET Authentication Protocol (SVAP) is proposed, providing non-repudiation feature with high speed connectivity between vehicles and infrastructure.
3) The new protocol balances security and efficiency by emerging lightweight operations such as rotation and XOR functions with Chebyshev chaotic maps.
4) Performance comparisons are conducted, revealing that the proposed protocol is superior to the resource constrained environment such as VANET, especially in case of emergency services.

The rest of this article is organized as follows: The preliminaries for the proposed protocol are presented in Section II. In Section III, the new protocol is elaborated. The performance of the proposed protocol is evaluated with respect to the most recent competing protocol in Section IV. The security analysis is given in Section V. The formal security verification of the new protocol with the help of Scyther simulation is introduced in Section VI. The conclusion is outlined in Section VII.

II. PRELIMINARY

In this section, all cryptographic tools used throughout this paper are shortly described for easy understanding of the proposed protocol. In addition, all notations used in this article are described. The required security features that should be achieved by the new protocol are illustrated, too. A new proposed structure design for the VANET model is also introduced. To show the major significance of the protocol proposed in section III, comprehensive comparisons with the existing schemes are finally given.

A. CRYPTOGRAPHIC TOOLS

The proposed protocol depends on two main cryptographic tools: The Chebyshev chaotic map and rotation according to RR method. The primary goal of Chebyshev map in this paper is to perform key establishment between entities in addition to executing entity signature on the transmitted traffic. One more merit is the integration of a new rotation mechanism called RR method with the new protocol to securely transfer messages within the network. To enhance the security of the proposed VANET model, modular addition and XOR operators are also emerged within the phases of the new protocol. Although the combination of various cryptographic tools balances efficiency and security, only lightweight operations are presented. The following are just two mathematical explanations of the two previously-discussed cryptographic tools:

1) CHEBYSHEV CHAOTIC MAP

Let p be a big prime number, φ be a real number within the range [-1, 1], ω be an integer, and y be the Chebyshev output. The Chebyshev Polynomial $T_\omega(\varphi)$ of degree ω is defined as indicated in (1). Its recurrence formula can be specified according to (2).

$$T_\omega(\varphi) = \cos\left(\omega \cdot \cos^{-1}(\varphi)\right) \tag{1}$$

$$T_\omega(\varphi) = \begin{cases} 1, & \text{if } \omega = 0 \\ \varphi, & \text{if } \omega = 1 \\ 2\varphi \cdot T_{\omega-1}(\varphi) - T_{\omega-2}(\varphi), & \text{if } \omega \geq 2 \end{cases} \tag{2}$$

Besides, a modified Chebyshev polynomial is described using (3) to improve the properties of the Chebyshev chaotic map, whereas, g is assumed to be a generator of the prime p. This map is described with full detail in [15]–[21].

$$y = T_g(\varphi) \bmod p \tag{3}$$

It is clearly found that Chebyshev chaotic map achieves high performance when combined with other cryptographic functions due to its strong randomness and complex dynamic features, as shown below:

- *Discrete Logarithm Problem (DLP):* Given two elements y and φ, it is computationally infeasible to get the value of g that satisfies (3).
- *Computational Diffie-Hellman problem (CMDHP):* According to the chaotic map, it is computationally infeasible to satisfy (4) in order to get the value of $T_{g\omega}(\varphi)$ for any given φ, $T_\omega(\varphi)$, and $T_g(\varphi)$.

$$T_\omega(T_g(\varphi)) \equiv T_g(T_\omega(\varphi)) \equiv T_{g\omega}(\varphi) \bmod p \tag{4}$$

2) ROTATION ACCORDING TO RR METHOD

A wealth of information about this rotation technique can be outlined in [22]. According to the RR method, the rotation of parameters X and Y is carried out depending on the following steps:

- Estimating the length of Y parameter: (L).
- Computing the modular arithmetic of Y parameter by the value of L: $(Y \bmod L)$.
- Calculating XOR operator of both parameters X and Y: $(X \oplus Y)$.
- Performing left circular shift of $(X \oplus Y)$ by the value of $(Y \bmod L)$.
- The result of the previous step can be considered to be $\mathrm{Rot}(X, Y)$.

However, the function $\mathrm{RRot}(X, Y)$ can be considered as the inverse operation of $\mathrm{Rot}(X, Y)$.

B. NOTATIONS

All parameters presented in this article and their definitions are indicated in Table 1. For easy comprehension of the proposed protocol, the table also describes the symbols used within the cryptographic functions.

TABLE 1. Symbols and their descriptions used in the new proposed protocol.

Symbol	Description
mod	Modular function
$\mathrm{OBU_i}$	Onboard unit of i^{th} vehicle
$\oplus$	XOR operator
R_j	j^{th} Roadside unit
$\mathrm{ID_i}$	Original identity of i^{th} vehicle
$\mathrm{PID_i}$	Pseudo-identity of i^{th} vehicle
$\mathrm{ID_j}$	True identity of R_j
L_j	Location of R_j
S	Shared symmetric key between $\mathrm{OBU_i}$ and the TA
$\mathrm{Cert_i}$, $\mathrm{Cert_j}$	The TA certificate for $\mathrm{OBU_i}$ and R_j, respectively
a, b, c	Private keys for $\mathrm{OBU_i}$, R_j, and the TA, respectively
+	Modular addition
Q	Shared symmetric key between R_j and the TA
A, B, C	Public keys for $\mathrm{OBU_i}$, R_j, and the TA, respectively
Emreqt	Emergency request sent by $\mathrm{OBU_i}$ to R_j
Emrep	Emergency reply sent by R_j to $\mathrm{OBU_i}$
S', Q'	Recalculated values of S and Q at the entity
Snky	Shared session key between $\mathrm{OBU_i}$ and R_j
t_m	Current timestamps, where: m is index ranging from 1 to 8
t'_m	Timestamps of received messages
g	Integer within a group $[1, \ldots, (p - 1)]$ with order $(p - 1)$ modulo p

C. SECURITY REQUIREMENTS

To strengthen the security of the new network model presented in this paper, various security features should be achieved by the new protocol as follows:

1) EFFICIENT AUTHENTICATION

Each entity in VANET has to verify the legitimacy of the others before allowing them to communicate with each other.

2) NON-REPUDIATION

This feature is defined as no entity within the entire network can deny sending a specific message. To achieve this, digital signatures using the entity private key are required.

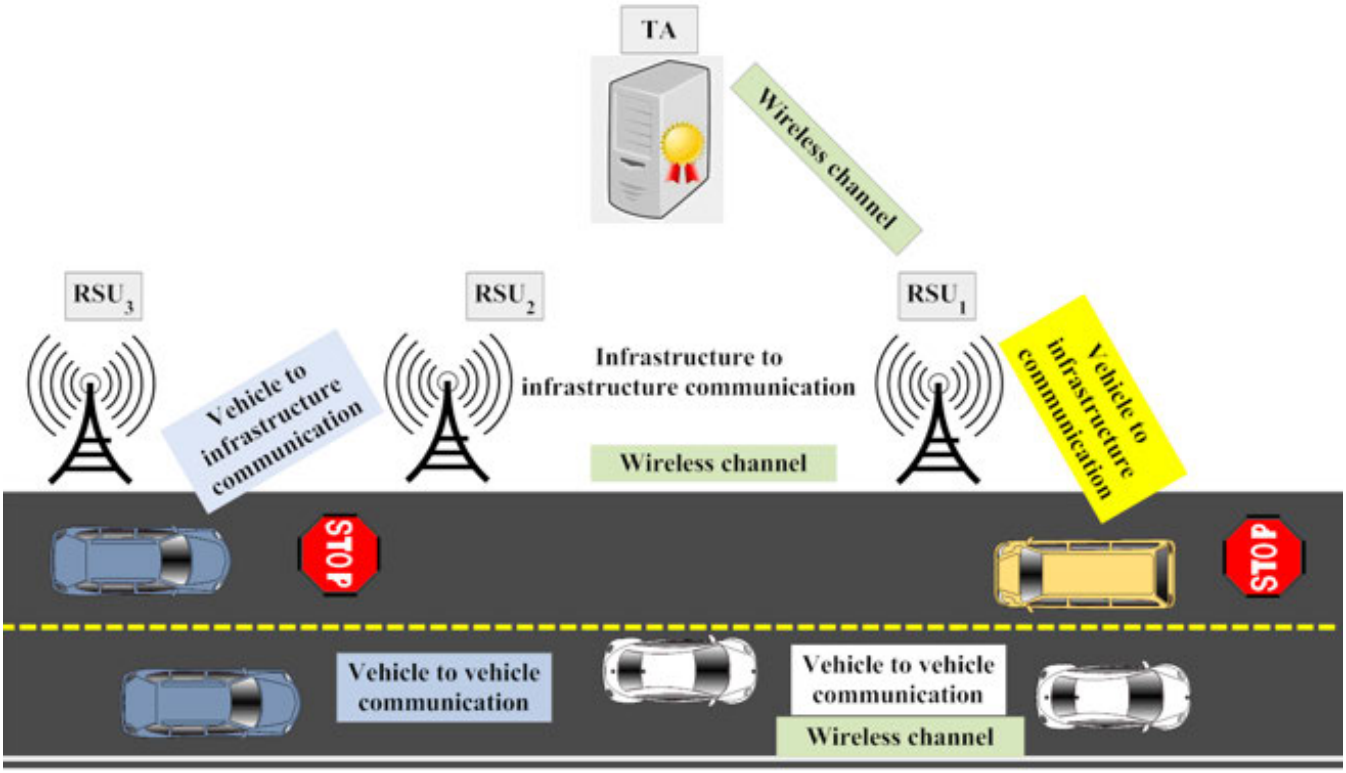


FIGURE 1. The proposed structure of VANET model: Considering the new assumptions to have a wireless connectivity between all network participants.

3) TRACEABILITY

Only the TA has the ability to trace the misbehaved vehicle using its real identity that is only known to both this authorized center and the vehicle itself.

4) UNLINKABILITY

Various pseudo-identities are utilized to define the vehicle in different communication sessions. It is also crucial to prevent the attacker from linking between two messages to recognize a particular vehicle.

5) PRESERVING IDENTITY PRIVACY

The predominant goal of this feature is to secure the vehicle true identity. Instead of identifying the vehicle based on its real identity, a pseudo-identity is explicitly exchanged throughout the network.

6) NO CERTIFICATE DEPENDENCY

The critical importance of this feature depends on neglecting the continuous transmission of the entity certificate during the entire process. This leads to a lightweight communication cost for the protocol.

7) FAST RESPONSE IN EMERGENCY CONDITIONS

The proposed protocol introduces this novel feature for the first time in the VANET domain. For example, in case of medical rescue conditions, the vehicle can send a fast emergency appeal to the nearest RSU. This appeal is also secured to protect the secret information in the vehicle request. Moreover, the private appeal can be used to allow the vehicle's driver to gather information about the closest health care centers for patient treatment.

8) RESISTANCE TO SEVERAL ATTACKS

The new proposed protocol should resist the well-known attacks such as forgery, impersonation, and replay attacks. To resist a forgery attack, the protocol should be able to reveal any attempt from the attacker to alter the transferred traffic over the transmission medium. Besides that, the protocol ability to prevent any attacker from impersonating an authorized entity results in a strong protocol against an impersonation attack. Similarly, it is primarily required from the protocol to counter a replay attack by incorporating a nonce or a timestamp into its messages to protect its traffic from being retrieved in another session.

D. THE NEW PROPOSED VANET MODEL

This subsection introduces a novel network model for VANET. The new proposed model has no secure channels to exchange the system secrets between network participants. The new structure of VANET model is shown in Fig. 1. For the first time in the VANET domain, all entities in the network are able to interact wirelessly. The novel structure has three main components: Mobile vehicles on the road,

fixed RSUs, and TA. Each vehicle has an OBU which supports a DSRC protocol during its communication with the other vehicles and RSUs. Multiple RSUs are also deployed along the road to handle the traffic received from the nearby vehicles. In addition, the TA acts as a trusted entity with the highest communication and storage capacities among all participants within the network. Working as a certificate issuing center can be considered as another function of the TA. However, it is defined that the VANET is a resource constrained environment in terms of computing and storage capabilities for an OBU. To strengthen the security of the new model, vehicles, RSUs, and TA are assumed to be partial trusted entities within the network. To fulfill these assumptions, the following procedures are taken into account during the protocol design:

- The vehicle cannot request an emergency service from the nearest RSU until its self-authentication with the TA is successful. Additionally, the RSU has to verify its legitimacy to the TA before allowing it to serve the vehicle emergency request. As a result of this, the TA acts as a central bridge between the vehicle and RSU.
- The TA is the only entity that has the ability to check the authenticity of both the vehicle and RSU before generating the partial session key Snky. This key is a part of the full session key K which is used to secure further communication between the vehicle and RSU in case of rescue operations.
- The TA does not have the privileges to access to the total session key K. On the vehicle side, this key K is generated with the help of Snky and the vehicle private key a. However, on the RSU side, it is formed by Snky and the RSU private key b. It is well defined that the private key of the entity is only known to the entity itself.

Consequently, the connectivity between the vehicle and RSU is partially controlled by the TA depending on the session key Snky issued by the TA itself. Although this session key is kept hidden from the public and is only known to the vehicle and RSU when they use the TA to authenticate each other, it is not the only parameter used to control the connectivity. This communication is also controlled by other secret parameters generated by the vehicle and RSU, respectively. Additionally, RSUs work as intermediate bridges between the vehicles and TA. Moreover, the TA has its official website in which its public parameters are published. A comprehensive description of the new model construction is discussed in section III.

E. COMPARISONS WITH THE EXISTING SCHEMES

For a comprehensive understanding of the new protocol significance, comparisons between the proposed protocol and the current existing schemes are outlined in this subsection. The comparisons are performed in terms of three main axes: Security features, network structure basics, and cryptographic tools used.

1) COMPARISON BASED ON SECURITY FEATURES

According to Table 2, the security analysis is evaluated to gain a full understanding of the security properties that are negligible in each scheme. It is found that the schemes [6], [7] achieve non-repudiation based on exchanging certificates between the entities within the network. As a result of this, a high communication burden is introduced, leading to a waste in the network bandwidth. In addition, none of the current schemes addresses the issue of exchanging emergency appeals between the vehicle and infrastructure in case of real-time critical conditions.

2) COMPARISON BASED ON NETWORK STRUCTURE

To transfer the secret parameters during the registration process or establish a communication with other entities, such as RSU-TA connectivity, the current schemes mentioned in Table 3 require secure channels. This raises the cost of network deployment that is seen to be a massive obstacle in the VANET realistic implementation. Since the entire authentication process is controlled by one entity, most current schemes do not depend on the concept of distributed entities.

3) COMPARISON BASED ON CRYPTOGRAPHIC TOOLS

The existing schemes in Table 4 cannot balance the protocol security and OBU limited resources in terms of computations. Since these schemes utilize cryptographic methods, they necessitate many calculations due to their complex operations. As a result of these complex functions, there is a delay in responding to the vehicle request, which is undesirable in emergency situations.

According to the following tables, it is found that the most recent scheme, related to the new proposed protocol is [14]. However, there are some fundamental similarities between the two protocols, as mentioned below:

- Lightweight operations are utilized in both protocols.
- They do not depend on time consuming functions such as bilinear pairing operations.
- A shared symmetric key between the vehicle and RSU is generated.

In contrast, the main demerits of scheme [14] are as follows:

- The scheme relies on SHA-256 hash function that consumes large storage overhead.
- Non-repudiation feature is not achieved.
- A secure channel is needed to exchange secrets.
- The shared key generated between the vehicle and RSU is fully controlled by the TA.
- It does not present a solution to emergency appeals since it ignores the transmission of the rescue requests in its timeline.

The proposed protocol attempts to avoid the demerits of scheme [14] in its design. As a result, the new protocol integrates the concepts of three cryptosystems: Symmetric key mechanism, traditional public key cryptosystem, and certificateless technique. Hence, the proposed protocol takes the advantage of each cryptosystem. According to the symmetric

TABLE 2. Security features analysis.

Features	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	SVAP
Efficient Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Non-repudiation	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes
Traceability	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes
Unlinkability	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes
Identity privacy preserving	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
No certificate dependency	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
Fast response in emergency conditions	No	No	No	No	No	No	No	No	Yes	Yes
Resistance to forgery attack	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Resistance to impersonation attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resistance to replay attack	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

TABLE 3. Network structure components.

Elements	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	SVAP
No secure channel used	No	No	No	No	No	No	No	No	No	Yes
Distributed entities	Yes	Yes	No	No	No	Yes	No	Yes	No	Yes

TABLE 4. Cryptographic methods used.

Tools	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	SVAP
Bilinear pairing	No	Yes	No	No	Yes	No	Yes	No	No	No
Elliptic curves	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No
Hash function	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Biometric password login	No	No	No	No	No	No	Yes	Yes	No	No
Chinese remainder	No	No	Yes	No	No	Yes	No	No	No	No
Chebyshev chaotic map	No	No	No	No	No	No	No	Yes	No	Yes

key mechanism, the new protocol tries to use lightweight operations such as Chebyshev map and rotation technique to perform authentication and key agreement between entities. Therefore, the length of each operation output is controlled by the size of its input. Based on the traditional public key cryptosystem, the proposed protocol uses the concept of digital signatures to achieve non-repudiation feature. Besides, the new protocol uses the concept of certificateless technique to avoid the continuous transmission of certificates during the whole process of authentication. Despite the fact that the key is provided entirely by the TA using the certificateless principle, the new protocol attempts to solve the key escrow issue. Although a part of the session key shared between the vehicle and RSU is controlled by the TA, its other part is managed by the vehicle and RSU together. The main aim is to prevent the whole control of the TA on the session key shared between the vehicle and RSU. Also, the proposed protocol replaces a secure channel used in [14] with a key establishment mechanism using the chaotic map.

III. PROPOSED PROTOCOL

The new proposed protocol has four main stages: The network deployment phase, the set up phase, the registration phase, and the authentication phase. A detailed description of each phase is outlined as follows:

A. NETWORK DEPLOYMENT PHASE

In this phase, the VANET is started to be deployed within the country. Thus, the TA generates its public parameters such as w, p, and g as follows: Firstly, a random integer w and a large prime number p are generated. Secondly, an accurate selection of the parameter g is performed to satisfy (5). Hence, according to (6), the smallest exponent that fulfills the equation is (p - 1). Then, the TA selects a secret value c to be considered as its private key. Additionally, it uses the Chebyshev chaotic map to issue its corresponding public key C according to (7).

$$g^{\text{exponent}} \bmod p \neq 1, \quad \text{for exponent} < (p\text{ - }1) \tag{5}$$

$$g^{(p-1)} \bmod p = 1 \tag{6}$$

$$C = \mathrm{T}_{g^c}(\omega) \bmod p \tag{7}$$

After that, the TA puts its public parameters C, w, p, and g in the software which is going to be downloaded on each vehicle OBU during the vehicle's manufacturing process. Similarly, these parameters are also installed on the memory of each RSU before allowing the RSU to be set in its location along the road. Locations of all deployed RSUs are listed in the TA which publishes its own public key C on its official website.

B. SET UP PHASE

Throughout this phase, the vehicle and RSU internally generate their own private/public key pairs using a discrete Chebyshev polynomial. Also, each entity tries to compute a shared key with the TA to secure its further communication. The generation of keys are illustrated as follows:

1) GENERATION OF KEYS AT VEHICLE

Inside the vehicle itself: The vehicle randomly generates its private key a, then computes its own public key A by (8). Additionally, the vehicle calls the TA public key C from its memory. With the aid of C and a, the vehicle computes a symmetric key S which will be used to securely exchange authentication messages between the vehicle and TA. This symmetric key is calculated by (9). After the generation of the shared key S, the vehicle splits this key into two separated sub-keys: S_1 and S_2 to be utilized in further computations. Moreover, the vehicle starts to compute the ticket X_1 by the help of (10).

$$A = \mathrm{T}_{g^a}(\omega) \bmod p \tag{8}$$

$$S = \mathrm{T}_{g^a}(C) \bmod p \tag{9}$$

$$X_1 = \mathrm{Rot}(A \oplus S_1, S_2) \tag{10}$$

Furthermore, the private ticket X_1 is stored inside the vehicle memory to be used for securing further exchange of the vehicle public key A across the network. Hence, any attempt to tamper the value of A throughout the transmission over a wireless channel will negatively affect X_1.

2) GENERATION OF KEYS AT RSU

Inside the RSU itself: A secret value b is randomly chosen to act as the RSU private key. Then, the RSU calculates its corresponding public key B by (11). After that, it recovers the public parameter C from its memory to help in computing the secret key Q. This key can be considered as a shared key used for the private communication between the RSU and TA. The calculation of Q is performed depending on (12).

$$B = \mathrm{T}_{g^b}(\omega) \bmod p \tag{11}$$

$$Q = \mathrm{T}_{g^b}(C) \bmod p \tag{12}$$

The splitting process of the shared symmetric key Q into two sub-keys: Q_1 and Q_2 contributes in computing the ticket X_2 using (13). This ticket is stored in the RSU memory to be utilized to prevent altering the public key B during the transmission in the network.

$$X_2 = \mathrm{Rot}(B \oplus Q_2, Q_1) \tag{13}$$

According to the set up phase, it is found that both tickets X_1 and X_2 are used to protect the public keys A and B, respectively from the attacker impersonation. Each entity has the ability to verify the legitimacy of another entity public key before dealing with it. This strategy is a cost-effective solution for the continuous certificate transmission over the network, resulting in a reduction in the protocol overall communication overhead.

C. REGISTRATION PHASE

The two phases previously discussed act as a detailed summarization of the new model construction of the VANET.

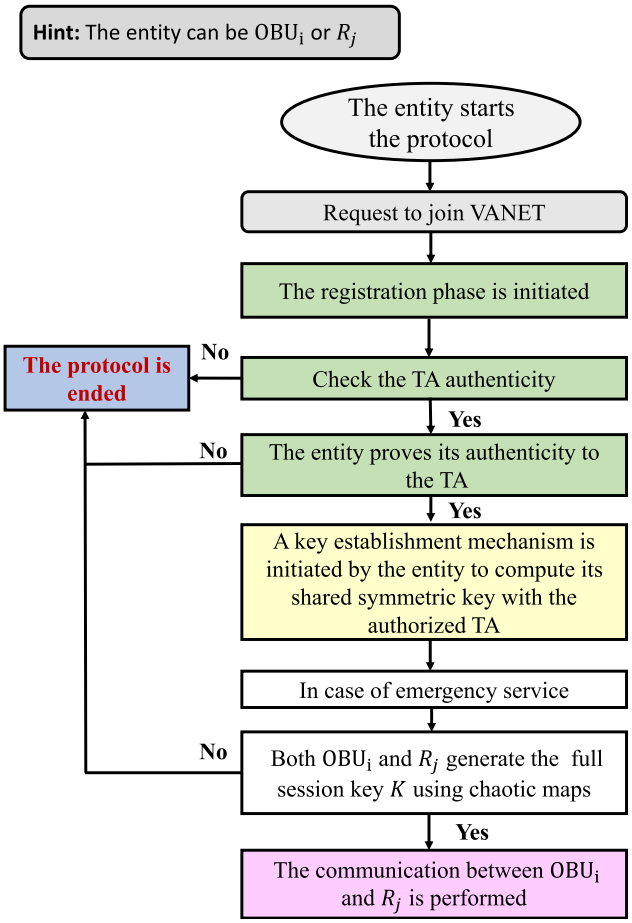


FIGURE 2. A flow diagram for the main guidelines of the new protocol.

Accordingly, a flow diagram that illustrates the general idea of the proposed protocol is shown in Fig. 2. Hence, the primary goal of the registration stage is the investigation of both the vehicle and RSU at the TA before allowing them to join the VANET. The following are the two main tasks to achieve this goal:

- Each entity proves its authenticity to the TA, then it requests the TA certificate for its self-generated public key.
- The registration processes for both the vehicle and RSU are accomplished.

For a detailed illustration of the two previous tasks, the investigation of the RSU at the TA is firstly discussed and so is the vehicle investigation. When the RSU attempts to access the resources of the VANET, it issues a request to be sent to the TA in order to get a permission to join the network. To form this request, the RSU generates its own timestamp t_1 and recalls the ticket X_2 from its memory. Then, the RSU computes the ticket X_3 according to its location L_j by (14). The ticket X_3 is utilized in verifying the RSU to the TA, based on its unique location. The combination between both the timestamp t_1 and shared secret key Q prevent changing t_1 during the transmission over the wireless channel.

Thus, the request reqt is finally formed as indicated in (15).

$$X_3 = \text{Rot}(L_j, Q \oplus t_1) \tag{14}$$

$$\text{reqt} = \{B, X_2, t_1, X_3\} \tag{15}$$

When the TA receives the RSU request at a timestamp t_1', it checks the refreshness of the timestamp. According to (t_1' - $t_1 > \Delta t$), the timestamp is not fresh and the session is terminated. Otherwise, the TA extracts the RSU public key B from the received request and computes the shared key Q' using the TA private key c by (16).

$$Q' = \text{T}_{g^c}(B) \bmod p \tag{16}$$

According to the properties of the chaotic maps, it is known that $\text{T}_{g^c}(B) \bmod p$ should equal to $\text{T}_{g^b}(C) \bmod p$. In case of no error transmission, the value of Q' should be equal to the value of Q. Hence, the key Q' is stored in the TA database with its sub-keys: Q_1 and Q_2 after the key splitting process is performed. Besides, the TA starts to recalculate the value X_2 using the received B and the calculated Q' to check the integrity of the received X_2 by comparing its recalculated value at the TA with its received value from the RSU. If the match is successful, the TA accepts the ticket X_2 and stores the value of B in its database as an authorized public key. To make the TA ensure the authenticity of the RSU, recovering the RSU location L_j from the received ticket X_3 has to be performed by the TA. Consequently, the TA issues a certificate Cert_j for the RSU as follows:

$$R_r = \text{Rot}(L_j, B \oplus Q_1) \tag{17}$$

$$S_r = \text{T}_{g^{c-R_r}}(\omega) \bmod p \tag{18}$$

This certificate has three basic components:$\{B, R_r, S_r\}$. The first component B is the RSU public key after ensuring that its value is not changed during the transmission from the RSU to the TA. The second component R_r is to prove the authenticity of the RSU location L_j. Furthermore, the third component S_r is the signature of the TA on the value of R_r using the TA private key c. The significance of S_r comes from its ability to detect any attempt from the attacker to alter data stored in the ticket R_r. To respond to the RSU request, the TA generates its own timestamp t_2 and assigns a real identity ID_j for the RSU. As a result of this, the TA computes the value of the ticket X_4 by (19).

$$X_4 = \text{ID}_\text{j} \oplus \text{Rot}(t_2, Q_2) \tag{19}$$

Finally, the TA sends its reply rep to the RSU as follows:

$$\text{rep} = \{\text{Cert}_\text{j}, t_2, X_4\} \tag{20}$$

When the RSU receives the TA reply at a timestamp t_2', it checks if the timestamp is fresh or not. If (t_2' - $t_2 > \Delta t$), the timestamp is not fresh and the session is ended. Otherwise, the RSU starts to check the received certificate before storing it in its memory. To verify the RSU certificate, the RSU utilizes the received values of R_r and S_r to recalculate Q according to (21).

$$Q' = \text{T}_{g^{b+R_r}}(S_r) \bmod p \tag{21}$$

According to the properties of the Chebyshev chaotic map, the value of $\text{T}_{g^{b+R_r}}(S_r) \bmod p$ has to match the value of $\text{T}_{g^{b+R_r}}(\text{T}_{g^{c-R_r}}(\omega)) \bmod p$ which is equal to the value $\text{T}_{g^{b+c}}(\omega) \bmod p$ when no modification attack is occurred during the transmission over the wireless channel. Therefore, the value of $\text{T}_{g^{b+c}}(\omega) \bmod p$ is proved to be equal $\text{T}_{g^b}(C) \bmod p$. In case of matching between the recalculated value of Q and its stored value, the RSU accepts its certificate and stores it in its memory. Hence, the RSU gets its identity ID_j from X_4 using (22).

$$\text{ID}_\text{j} = X_4 \oplus \text{Rot}(t_2, Q_2) \tag{22}$$

When the vehicle tries to verify itself at the TA and request issuing its certificate for its own public key, the following steps are executed:

Step 1: The vehicle's driver logs into the TA official web site using the vehicle computer to download the published value of the TA public key.

Step 2: The vehicle compares the downloaded value of the TA public key with the stored value in its memory to ensure that this website is authenticated. This step is the first wall to protect the vehicle from dealing with a fake public key announced to the public as if it is the true public key of the TA.

Step 3: When the match is executed, the vehicle's driver requests a challenge to ensure the ability of the TA to compute the shared key S. This challenge is the second defense line to protect the vehicle from dealing with a fake TA. Hence, a challenge-response mechanism is started. To perform the challenge, the vehicle's driver starts to enter the vehicle public key A into the TA website. The authorized TA can easily utilize its private key c to compute the symmetric key S and store its value in the TA database. This stored key S is calculated according to $\text{T}_{g^c}(A) \bmod p$. To prove the TA legitimacy to the vehicle, the TA challenges the vehicle's driver to enter a nonce n, encrypted with S into the TA website. To achieve this requirement, the vehicle selects a random nonce n and separates it into two parts: n_1 and n_2. This nonce with its components are stored in the vehicle memory for future comparisons. The vehicle challenge Ch is computed according to (23), then its value is published into the TA website.

$$\text{Ch} = \text{Rot}(n \oplus S_1, S) \tag{23}$$

As a result, the TA uses the symmetric key S to recover the vehicle nonce n' from the challenge Ch to help in computing its response Rp using (24).

$$\text{Rp} = \text{Rot}(n' \oplus S_2, S_1) \tag{24}$$

Step 4: The vehicle's driver downloads the published value of Rp to enable the vehicle recover its nonce to be compared with its stored value. If the match is performed, the TA proves its authenticity to the vehicle. After that, it is allowable for the driver to prove the vehicle authenticity to the TA by filling up the application form, published in the TA website by the correct information about the vehicle itself according to the following:

- The application form asks the driver about the crucial information related to the vehicle such as the car plate number, manufacturing date, and model year. It can also be information about the vehicle's owner and his address.
- Based on the entered information, the TA starts to verify its correctness. If the entered information is correct, the TA chooses a real identity ID_i and a pseudo-identity PID_i for the vehicle. As a response to the application form, these values should be securely published to the vehicle's driver on the TA website.
- To secure the values of ID_i and PID_i, the TA computes the private ticket X_1 internally and stores its value in the TA database. This private ticket is emerged with the selected identity ID_i to form the ticket D by (25). The ticket D is utilized to securely transfer ID_i from the TA to the vehicle.

$$D = ID_i \oplus X_1 \tag{25}$$

- Subsequently, the TA starts to generate the private ticket X_5 internally to aid in calculating the ticket U which is necessary to exchange PID_i between the vehicle and the TA as follows:

$$X_5 = \text{Rot}(ID_i \oplus S_2, S_1) \tag{26}$$
$$U = PID_i \oplus X_5 \tag{27}$$

- According to this, the TA publishes the two tickets D and U into its website. So, there is no ability to alter ID_i or PID_i without affecting the value of X_5.

Step 5: Consequently, the TA issues the vehicle certificate $Cert_i$ for the vehicle authorized public key A according to the following:

$$R_v = \text{Rot}(ID_i, A \oplus S_2) \tag{28}$$
$$S_v = T_{g^{c-R_v}}(\omega) \bmod p \tag{29}$$

This certificate has three main components: $\{A, R_v, S_v\}$. The component R_v is used to bind the public key A with the vehicle real identity ID_i. Additionally, the value S_v acts as the signature of the TA on the ticket R_v using its private key c. The usage of S_v is to prevent modifying the value of R_v without the knowledge of the TA itself. Besides, the vehicle certificate is published on the TA website to enable the vehicle's driver to download it on OBU memory.

Step 6: The vehicle's driver downloads this certificate in addition to the parameters D and U from the TA website. Then, the vehicle restores the private ticket X_1 from its memory to aid in recovering its real identity ID_i using (30). After that, this identity ID_i is utilized in the vehicle to calculate the ticket X_5 before being stored in the vehicle memory. The pseudo-identity PID_i is recovered with the aid of the downloaded ticket U and the calculated value of X_5 according to (31).

$$ID_i = D \oplus X_1 \tag{30}$$
$$PID_i = U \oplus X_5 \tag{31}$$

The vehicle also starts to verify its received certificate before storing it in its memory. To check the vehicle certificate, the vehicle uses the received tickets R_v and S_v to recompute the value of S by (32). According to the Chebyshev chaotic map, it is clearly known that $T_{g^{a+R_v}}(S_v) \bmod p$ is equal to $T_{g^{a+R_v}}(T_{g^{c-R_v}}(\omega)) \bmod p$ which matches the value of $T_{g^{a+c}}(\omega) \bmod p$. In case of the matching between the recomputed value of S and its stored value, the vehicle accepts its certificate and stores it in its memory. It is also found that any attacker's attempt to alter the value of the recovered identity ID_i will negatively affect the received ticket R_v.

$$S' = T_{g^{a+R_v}}(S_v) \bmod p \tag{32}$$

D. AUTHENTICATION PHASE

The primary goal of this phase is to accomplish the authentication process between the vehicle and RSU in addition to providing emergency services to the vehicle, moving along the road. To satisfy this goal, the authentication phase can be separated into two sub-phases as follows:

- Initiating the vehicle to the RSU communication.
- Serving emergency requests.

To simplify comprehension of the message flow within the authentication phase, the unified modeling language (UML) diagram is utilized. The UML diagram can be considered as a visual representation of the interactions between different entities in the protocol [23]. A short summarization that reflects the general idea of this phase is given in Fig. 3. As shown in this figure, the vehicle requests communication with the RSU by sending the request M_1. This request acts as an identification message for the vehicle to verify its authenticity to the TA. Consequently, the RSU utilizes the vehicle request M_1 to form its authentication request M_2. After receiving the request M_2 at the TA, the verification process is executed. When the TA ensures the legitimacy of the vehicle and RSU, it starts to generate M_3 that can be considered as a reply to M_2. This reply includes the partial session key Snky that has to be exchanged between the vehicle and RSU. When the RSU receives the authentication message M_3, it extracts its session key Snky and forms its authentication reply M_4. Subsequently, the authentication message M_4 acts as a reply to the vehicle request M_1. After receiving the partial session key Snky at the vehicle, each entity can form its full session key K internally to securely communicate with each other. Hence, the vehicle can request access to the emergency services by sending an urgent appeal M_5 to the RSU. This emergency appeal is secured by the total session key K. Then, the RSU replies with the message M_6 which includes the required service. It is found that the authentication process must be successfully accomplished before allowing the vehicle to access the RSU resources. In addition, the keystone of this phase is the TA that plays a role of a bridge between the vehicle and RSU. For more illustration, the key steps of the authentication phase can be discussed as follows:

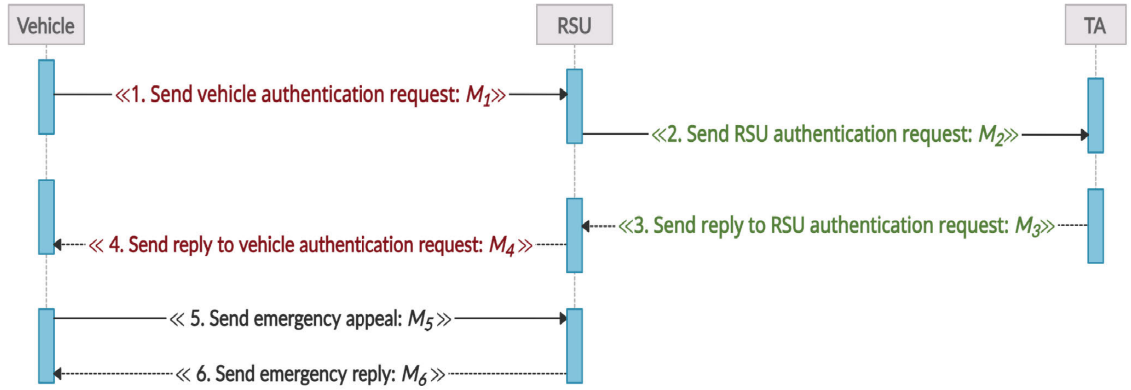


FIGURE 3. The flow of messages throughout the SVAP authentication phase.

1) INITIATING VEHICLE TO RSU COMMUNICATION

The timeline of this sub-phase is given in Fig. 4. Accordingly, the following are the two primary tasks for this sub-phase:

- Authenticating the vehicle and RSU to the TA.
- Generating the partial session key Snky that has to be exchanged between the vehicle and RSU.

Before allowing the vehicle to access the RSU resources, both the vehicle and RSU have to verify the authenticity of each other. As a result, this sub-phase emphasizes on illustrating the authentication process between the vehicle and RSU, using the TA as a central bridge between them according to 5 steps as follows:

Step 1: When the vehicle enters the coverage area of the nearest RSU, it starts to authenticate itself to the TA throughout this RSU. Thus, the vehicle gets its current timestamp t_3 and uses its stored sub-keys S_1 and S_2 to compute the following:

$$r_1 = \mathrm{Rot}(\mathrm{ID_i} \oplus t_3, \mathrm{PID_i} \oplus S_1) \tag{33}$$

$$Y_1 = \mathrm{T}_{g^{a-r_1}}(\omega) \bmod p \tag{34}$$

The value of r_1 acts as an identification ticket for the vehicle to enable the TA easily recognize it by its true $\mathrm{ID_i}$. In addition, this ticket is secured by the sub-key S_1 which is privately shared between the vehicle and TA. Moreover, the ticket Y_1 is considered as the vehicle signature on the ticket r_1. The aim of this vehicle signature is to perform non-repudiation feature, whereas no other entity in the whole network can be able to generate Y_1 without using the vehicle private key a. The TA can verify this signature using the vehicle public key A. Then, the vehicle sends the message $M_1 = \{\mathrm{PID_i}, t_3, r_1, Y_1\}$ to the RSU through a wireless channel.

Step 2: When the RSU receives the message M_1 at a timestamp t_3', it checks if the timestamp is fresh or not. Based on $(t_3' - t_3 > \Delta t)$, the timestamp is not fresh and the session is closed. Otherwise, the RSU gets its timestamp t_4 and computes the following:

$$r_2 = \mathrm{Rot}(\mathrm{ID_j}, t_4 \oplus Q_1) \tag{35}$$

$$Y_2 = \mathrm{T}_{g^{b-r_2}}(\omega) \bmod p \tag{36}$$

The first ticket r_2 is utilized to secure $\mathrm{ID_j}$ from being changed by the attacker during the transmission over the channel. This ticket is protected by the sub-key Q_1 which is privately shared between the RSU and TA. Furthermore, the second ticket Y_2 is the signature of the RSU on the ticket r_2 to achieve non-repudiation feature. Besides, the third ticket C_1 is computed to identify the RSU to the TA, depending on the RSU location L_j by (37). Both tickets r_2 and C_1 can be considered as identification tickets for the RSU to be identified to the TA. Therefore, the RSU sends the message $M_2 = \{M_1, \mathrm{ID_j}, t_4, r_2, Y_2, C_1\}$ to the TA using a wireless channel.

$$C_1 = ((L_j \oplus t_4) + Q_2) \bmod p \tag{37}$$

Step 3: When the TA receives the message M_2 at a timestamp t_4', it checks the refreshness of the timestamp. According to $(t_4' - t_4 > \Delta t)$, the timestamp is considered to be not fresh and the session is terminated. Otherwise, the TA gets its timestamp t_5 and starts verifying the received values. To prove the authenticity of the RSU, the TA utilizes the two received tickets r_2 and Y_2 to recompute the shared key Q using (38). If its recalculated value is equal to its stored value, the TA accepts the RSU signature Y_2. Next, the TA extracts L_j from the encrypted ticket C_1 as in (39) and compares its value with the list that has all the authorized locations of the deployed RSUs within the country. In case of matching, the RSU is authenticated to the TA.

$$Q' = \mathrm{T}_{g^{c+r_2}}(Y_2) \bmod p \tag{38}$$

$$L_j = ((C_1 - Q_2) \oplus t_4) \bmod p \tag{39}$$

To verify the authenticity of the vehicle, the TA starts the recalculation of the shared symmetric key S using (40). The computations of S' depend on the two received tickets r_1 and Y_1. Any attempt from the attacker to change r_1 or Y_1 leads to the mismatch between the recomputed value of S at the TA and its stored value, so the session is ended. Otherwise, the TA extracts the vehicle true identity $\mathrm{ID_i}$ from the ticket r_1 according to (41).

$$S' = \mathrm{T}_{g^{c+r_1}}(Y_1) \bmod p \tag{40}$$

$$\mathrm{ID_i} = \mathrm{RRot}(r_1, \mathrm{PID_i} \oplus S_1) \oplus \mathrm{PID_i} \oplus S_1 \oplus t_3 \tag{41}$$

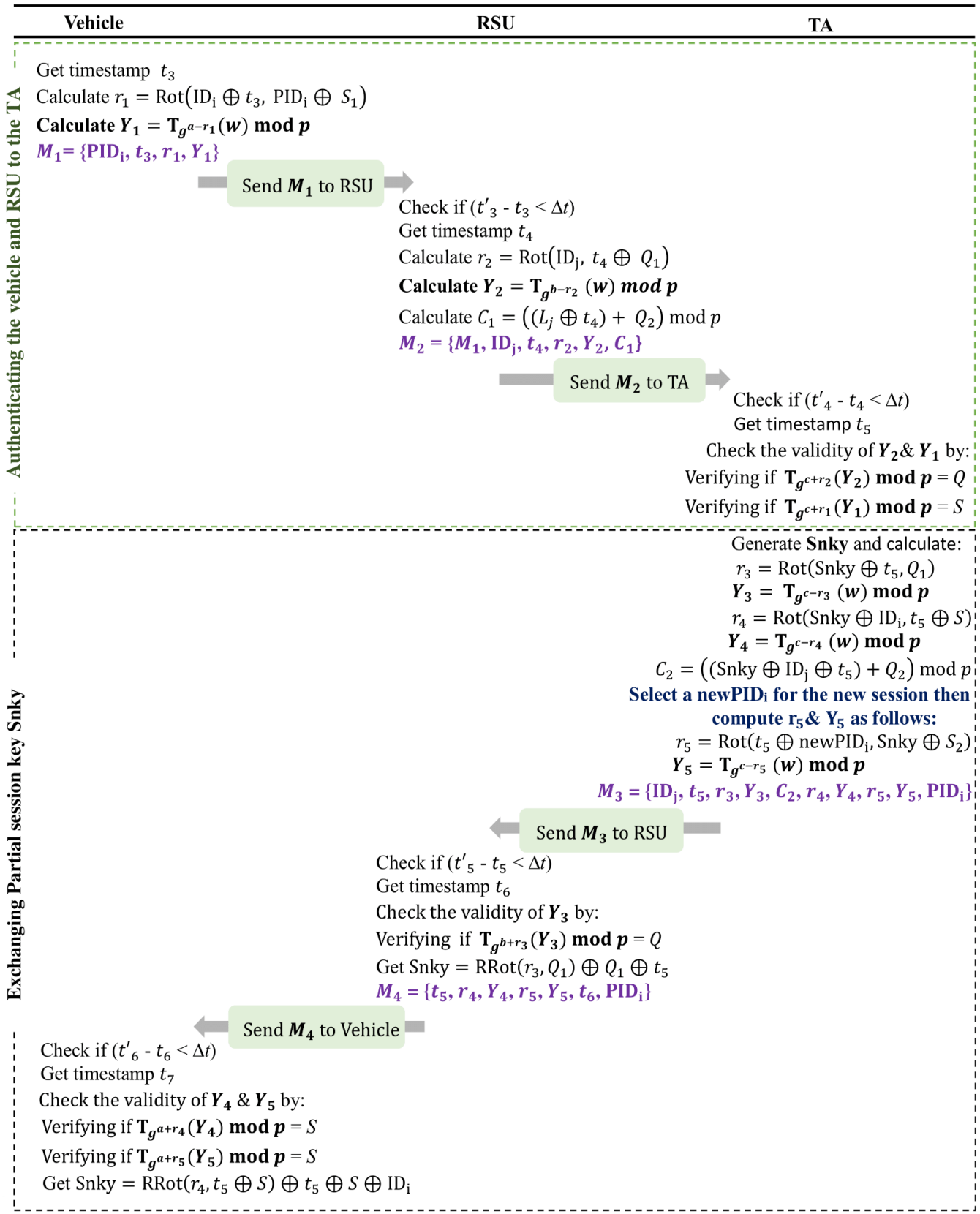


FIGURE 4. The timeline of authentication process and session key exchanging during the SVAP authentication phase.

The TA generates the partial session key Snky after successfully verifying the validity of both the vehicle and the RSU, and uses it to compute the following two tickets:

$$r_3 = \text{Rot}(\text{Snky} \oplus t_5, Q_1) \quad (42)$$

$$Y_3 = \text{T}_{g^{c-r_3}}(\omega) \bmod p \quad (43)$$

The ticket r_3 is used to securely transfer Snky to the RSU. Additionally, the ticket Y_3 acts as the TA signature on the ticket r_3 by the TA private key c to achieve the non-repudiation feature. The ticket C_2 is generated to preserve the integrity of the RSU identity ID_j using (44).

$$C_2 = ((\text{Snky} \oplus \text{ID}_\text{j} \oplus t_5) + Q_2) \bmod p \quad (44)$$

To deliver the partial session key Snky from the TA to the vehicle, the TA issues the ticket r_4 as follows:

$$r_4 = \text{Rot}(\text{Snky} \oplus \text{ID}_\text{i}, t_5 \oplus S) \quad (45)$$

This ticket is used for transferring Snky to the vehicle. Likewise, the ticket r_4 is signed using the TA private key c to generate its signature Y_4 by (46).

$$Y_4 = \text{T}_{g^{c-r_4}}(\omega) \bmod p \quad (46)$$

After that, the TA assigns a new random value for the pseudo-identity of the vehicle newPID_i. This new value is assigned to be used in the next session. To securely transfer newPID_i from the TA to the vehicle, the TA issues the ticket r_5 using (47). This ticket is protected by Snky and S_2. Consequently, the TA signature on the ticket r_5 is generated using (48). As a result, the TA sends the message $M_3 = \{\text{ID}_\text{j}, t_5, r_3, Y_3, C_2, r_4, Y_4, r_5, Y_5, \text{PID}_\text{i}\}$ to the RSU.

$$r_5 = \text{Rot}(t_5 \oplus \text{newPID}_\text{i}, \quad \text{Snky} \oplus S_2) \quad (47)$$

$$Y_5 = \text{T}_{g^{c-r_5}}(\omega) \bmod p \quad (48)$$

Step 4: When the RSU receives the message M_3 at a timestamp t_5', it checks the refreshness of the timestamp. If (t_5' - $t_5 > \Delta t$), the timestamp is not fresh and the session is ended. Otherwise, the RSU gets its timestamp t_6 and starts to compare between the shared key Q, recalculated by (49) and its stored value.

$$Q' = \text{T}_{g^{b+r_3}}(Y_3) \bmod p \quad (49)$$

Based on the previous comparison, the RSU terminates the session or continues the computations. If the recomputed value of Q matches its stored value, the RSU recovers Snky from r_3 according to (50). Accordingly, the RSU sends the message $M_4 = \{t_5, r_4, Y_4, r_5, Y_5, \text{PID}_\text{i}, t_6\}$ to the vehicle.

$$\text{Snky} = \text{RRot}(r_3, Q_1) \oplus Q_1 \oplus t_5 \quad (50)$$

Step 5: When the vehicle receives the message M_4 at a timestamp t_6', it checks if the timestamp is fresh or not. Based on (t_6' - $t_6 > \Delta t$), the timestamp can be considered to be not fresh and the session is closed. Otherwise, the vehicle gets its timestamp t_7 and starts to check the validity of the signatures Y_4 and Y_5 as follows:

$$S' = \text{T}_{g^{a+r_4}}(Y_4) \bmod p \quad (51)$$

$$S' = \text{T}_{g^{a+r_5}}(Y_5) \bmod p \quad (52)$$

Based on (51), if the recalculated value of S is equal to its stored value, the vehicle gets Snky from the ticket r_4 by (53). Similarly, if the match is successful according to (52), the values of r_5 and t_5 are stored inside the vehicle memory for further computations.

$$\text{Snky} = \text{RRot}(r_4, t_5 \oplus S) \oplus t_5 \oplus S \oplus \text{ID}_\text{i} \quad (53)$$

After the successful execution of this sub-phase, the vehicle can request access to the emergency services that are provided by the RSU as shown in Fig. 5.

2) SERVING EMERGENCY REQUESTS

This sub-phase is an add-on to the previous one. In case of disasters, the vehicle attempts to request an emergency service. To perform this, it starts to compute its full session key K with the RSU using (54). This key is split into two separated parts: K_1 and K_2.

$$K = (\text{Snky} + \text{T}_{g^a}(B) \bmod p) \bmod p \quad (54)$$

Besides, the first part K_1 is utilized to secure the ticket r_6 that includes the emergency request Emreqt using (55). The ticket signature is generated by the vehicle private key a using (56).

$$r_6 = \text{Rot}(\text{Emreqt}, K_1 \oplus t_7) \quad (55)$$

$$Y_6 = \text{T}_{g^{a-r_6}}(\omega) \bmod p \quad (56)$$

With reference to (54), the overall session key K between the vehicle and RSU is not solely dependent on the session key Snky provided by the TA. In the new protocol, it is assumed that the TA is a partial trusted entity. As a result, a portion of the key K is self-generated by the vehicle and RSU without the knowledge of TA itself. On the vehicle side, this key K is dependent on the term $\text{T}_{g^a}(B) \bmod p$. However, it is based on the term $\text{T}_{g^b}(A) \bmod p$ on the RSU side. Thus, the TA cannot generate the two previous terms without the knowledge of the vehicle private key a and the RSU private key b. As a consequence, the communication between the vehicle and RSU is protected from the TA interception on their connectivity. Therefore, the vehicle sends the message $M_5 = \{t_7, r_6, Y_6, \text{PID}_\text{i}\}$ to the RSU.

Step 6: When the RSU receives the message M_5 at a timestamp t_7', it checks the refreshness of the timestamp. If (t_7' - $t_7 > \Delta t$), the timestamp is not fresh and the session is ended. Otherwise, the RSU gets its timestamp t_8 and checks the correctness of the received signature Y_6 using the vehicle public key A by (57).

$$H = \text{T}_{g^{b+r_6}}(Y_6) \bmod p \quad (57)$$

In case of the correct reception of the signature Y_6, the value of H should match $\text{T}_{g^b}(A) \bmod p$. To recover the vehicle request, the RSU starts to generate its full session key K with

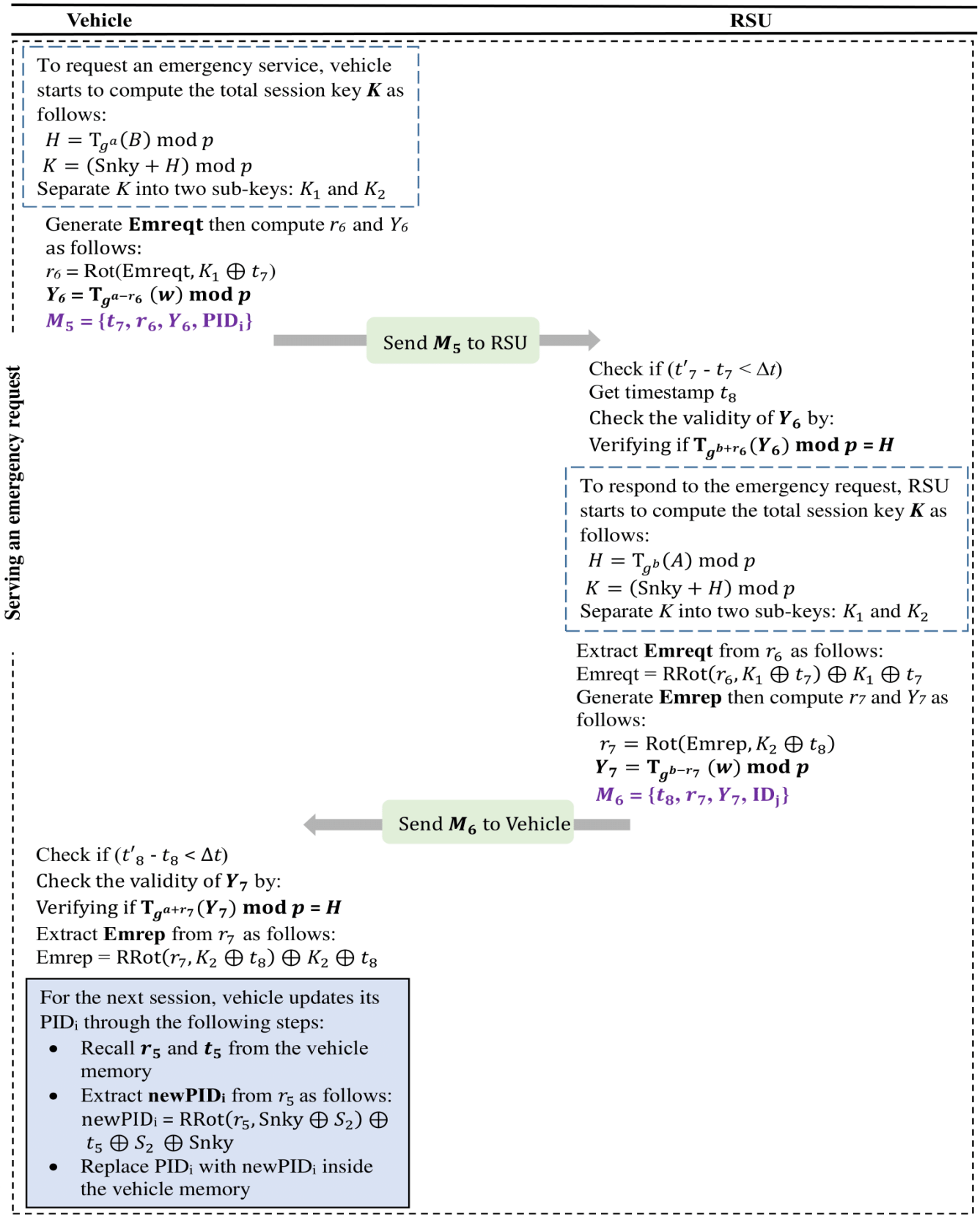


FIGURE 5. The timeline of serving emergency appeals throughout the SVAP authentication phase.

the vehicle according to (58). This key K is formed on the RSU side using the partial key Snky, the RSU private key b, and the vehicle public key A. The TA cannot compute the term $T_{g^b}(A)$ mod p without having the RSU private key b.

$$K = (\text{Snky} + T_{g^b}(A) \mod p) \mod p \tag{58}$$

After splitting the key K into two sub-keys: K_1 and K_2, the RSU utilizes the sub-key K_1 in addition to the timestamp t_7 to get Emreqt using (59).

$$\text{Emreqt} = \text{RRot}(r_6, K_1 \oplus t_7) \oplus K_1 \oplus t_7 \tag{59}$$

Next, the RSU issues an emergency reply Emrep and securely transfers it to the vehicle based on the sub-key K_2 using (60).

$$r_7 = \text{Rot}(\text{Emrep}, K_2 \oplus t_8) \tag{60}$$

After that, the RSU signs the ticket r_7 by its private key b to generate Y_7 according to (61). Hence, the RSU sends the message $M_6 = \{t_8, r_7, Y_7, \text{ID}_\text{j}\}$ to the vehicle.

$$Y_7 = T_{g^{b-r_7}}(\omega) \mod p \tag{61}$$

In the new proposed VANET model, the RSU is assumed to be a partial trusted entity. To satisfy this, the RSU cannot have the ability to extract the vehicle request Emreqt from r_6 without having the sub-key K_1. This sub-key is a part of the total key K that is dependent on Snky. Moreover, the TA does not generate Snky until the verification process of the RSU authenticity is successful. As a result, the total control of the RSU on the key K is prevented.

Step 7: when the vehicle receives the message M_6 at a timestamp t_8', it checks the refreshness of the timestamp. If (t_8' - $t_8 > \Delta t$), the timestamp is not fresh and the session is closed. Otherwise, the vehicle checks the value of H using its private key a and the RSU public key B using (62). If the value of the received ticket H matches its stored value $T_{g^a}(B)$ mod p, the vehicle accepts the ticket H and recovers Emrep from the ticket r_7 by (63). Finally, it is announced that a successful connectivity between the vehicle and RSU is securely achieved according to the full session key K.

$$H = T_{g^{a+r_7}}(Y_7) \mod p \tag{62}$$

$$\text{Emrep} = \text{RRot}(r_7, K_2 \oplus t_8) \oplus K_2 \oplus t_8 \tag{63}$$

For the next session, the vehicle starts to update its pesudo-identity. To achieve this task, the vehicle recalls the values r_5 and t_5 from its memory. Then, it starts to extract newPID_i from r_5 according to (64). The vehicle replaces the value of PID_i with its new value newPID_i inside its memory.

$$\text{newPID}_\text{i} = \text{RRot}(r_5, \text{Snky} \oplus S_2) \oplus t_5 \oplus S_2 \oplus \text{Snky} \tag{64}$$

To emphasize the significance of the new protocol, the following are the most important applications that the proposed protocol might help in a way that benefits the society:

1) *Natural Disasters and Rescue Operations:* Transporting patients to the hospital in a timely manner to avoid death is a top priority. Hence, the proposed protocol is used to establish a fast connection between the vehicle and infrastructure to quickly respond to the emergency appeal from the vehicle. This emergency appeal can be one of the different forms mentioned below:
   - Navigation to the closest hospital for patients.
   - Requesting an emergency vehicle such as a police car or an ambulance in case of accidents and disasters.
   - Finding the nearest epidemic treatment centers for any medical staff.
   - Reporting any abnormal behavior by the other drivers that may lead to a traffic jam.
   - Requesting maintenance services for the vehicle in case of sudden breakdown in remote places.
2) *Terrorist Attacks:* In the occurrence of terrorist threats against the state, the proposed protocol will assist the army vehicles in connecting quickly to the networks in order to access the network resources and act against the terrorist attacks. Several citizens' lives will be saved as a result of this.

IV. PERFORMANCE ANALYSIS

This section is performed with the aid of Wolfram Mathematica program, simulated on Intel (R) Core (TM) i7-3632QM CPU, 2.20 GHz, and RAM 8.00 GB. This simulation helps in comparing the new protocol with the most recent related protocol [14] in terms of computing, communication, and storage costs. The following is a detailed comparison of the proposed protocol with the scheme in [14], emphasizing the superiority of the new protocol.

A. COMPUTATION COST

In scheme [14], the whole process depends on the two main cryptographic tools: SHA-256 hash function and XOR operator. The running time for hash function is t_h and t_x refers to the time cost of XOR operator. In contrast, the proposed protocol utilizes a variety of multiple cryptographic functions to strengthen the protocol security. Besides, it switches between four different operations as follows:

- Chebyshev chaotic maps.
- XOR operator.
- Rotation according to RR method.
- Modular addition/subtraction operations.

The time used to perform the Chebyshev maps is indicated as t_c. It is well defined that the Chebyshev map is more lightweight than the general hash function [24]. In addition, the rotation and modular addition operations act as lightweight functions, compared to the hash function [22]. Therefore, the execution time to achieve the modular addition/subtraction operation is t_m and for the rotation function is t_r. Moreover, Table 5 illustrates all operations performed by the vehicle, RSU, and TA throughout the new protocol from the registration phase, reaching the authentication phase. Furthermore, Table 6 illustrates the total cost in seconds to perform various functions in the vehicle, RSU, and TA.

TABLE 5. Various cryptographic operations.

Participants	Scheme [14]	SVAP
Vehicle	$6t_h + 5t_x$	$8t_c + 6t_x + 1t_m + 9t_r$
RSU	$4t_h + 2t_x$	$7t_c + 4t_x + 2t_m + 8t_r$
TA	$14t_h + 7t_x$	$10t_c + 7t_x + 2t_m + 12t_r$

TABLE 6. Time cost for multiple operations in seconds.

Participants	Scheme [14]	SVAP
Vehicle	1.747	1.326
RSU	1.606	0.98
TA	2.076	1.622

TABLE 7. Communication overhead for the registration phase.

Items	Scheme [14]	SVAP
Transmitted elements during the registration phase	$\mathrm{PID_i}$, A_1, A_2, $\mathrm{ID_i}$, $\mathrm{ID_j}$, K_j	C, reqt, rep, Rp, $\mathrm{Cert_i}$, U, D
Comm. burden in bits	992	1408

TABLE 8. Communication overhead for the authentication phase.

Items	Scheme [14]	SVAP
Transmitted messages during the authentication phase	M_1, M_2, M_3, M_4	M_1, M_2, M_3, M_4, M_5, M_6
Comm. burden in bits	5408	3872

TABLE 9. Overall communication overhead.

Items	Scheme [14]	SVAP
Total transmitted parameters throughout the protocol	$\mathrm{ID_j}$, A_1, A_2, $\mathrm{ID_i}$, M_1, M_2, M_3, M_4, K_j, $\mathrm{PID_i}$	M_1, M_2, M_3, M_4, M_5, M_6, reqt, C, rep, $\mathrm{Cert_i}$, Rp, U, D
Comm. burden in bits	6400	5280

TABLE 10. Storage overhead in bits.

Participants	Scheme [14]	SVAP
Vehicle	4896	4064
RSU	5856	4736
TA	7392	5126

According to the previous tables, the proposed protocol is investigated to have a much higher level of effectiveness than the scheme in [14]. Consequently, the time cost required to perform various cryptographic functions in the vehicle, RSU, and TA is reduced in a distinctive manner using the proposed protocol. Due to this reduction, the computation cost of the vehicle OBU is improved with 24.09%, compared to the scheme [14]. This proves that the proposed protocol is better suited for the VANET limited resources. Also, the computation costs of both the RSU and TA are significantly improved throughout the proposed protocol by 38.98% and 21.87%, respectively.

B. COMMUNICATION COST

In this subsection, the calculations of the communication overhead are performed when the vehicle and RSU attempt to join the VANET and access its resources. Hence, the registration phase is initiated and the comparison between the proposed protocol and its related scheme [14] is achieved. Based on the registration phase, the scheme [14] requires a transmission of 992 bits; the parameters A_1 and A_2 need 256 bits and it is assumed that the identities of the vehicle and RSU have lengths of 160 bits. Although the new protocol demands 736 bits for the vehicle registration, only 672 bits are used for the RSU registration, as indicated in Table 7.

The communication cost of the new protocol is also compared with the related protocol [14] during the authentication phase as in Table 8. It is found that only 4 messages: M_1, M_2, M_3, and M_4 are exchanged between the entities in the scheme [14], compared to 6 messages in the new proposed protocol. The scheme [14] requires fewer messages to be exchanged, but each message bit length is longer than the one that is used in the proposed protocol. The key reason of this is that scheme [14] depends heavily on SHA-256 hash function.

The overall communication overhead is calculated by adding the values from Table 7 and Table 8 as shown in Table 9. In comparison to [14], the overall communication overhead of the new protocol is reduced by 17.5%.

C. STORAGE COST

A comparison between the proposed protocol and its competing scheme [14] in terms of the storage overhead is indicated in Table 10. The main drawback of the scheme [14] is its dependence on SHA-256 hash function that has an output size limitation of 256 bits. The more usage of this function, the more storage space is wasted. As a result of this, the scheme [14] needs a vehicle storage space greater than the proposed protocol with 832 bits. Due to the limited storage overhead of the OBUs, the new proposed protocol is more appropriate for the practical implementation in the VANET domain.

Comparing the proposed protocol with the scheme [14], it is found that the storage costs for the vehicle, RSU, and TA are improved by the new protocol with 16.99%, 19.13%, and 30.65%, respectively.

V. SECURITY ANALYSIS

In this section, by analyzing the security features provided by the new protocol, it is proved that the proposed protocol meets all the security properties previously discussed in section II.

A. EFFICIENT AUTHENTICATION

In the new protocol, there are three forms of mutual authentication between the following different entities: RSU-TA, vehicle-TA, and vehicle-RSU: The first authentication form is RSU-TA that is responsible for the mutual verification between the RSU and TA before allowing the RSU to access the VANET resources. It is well defined that the entity private

key is only known to the entity itself. In step 3 in the proposed protocol authentication phase, the TA checks the integrity of the RSU signature Y_2 and recovers L_j. The only authorized RSU can consequently compute the correct value of Y_2 using its private key b. When the signature Y_2 is verified at the TA by the RSU public key B, the RSU is proved to be authenticated to the TA. The TA is also challenged to compute its self-signature Y_3 to safely transfer the partial key Snky to the RSU. The only authorized TA can issue this signature by its private key c.

Besides, the second authentication form is vehicle-TA. In this form, the vehicle proves its authenticity to the TA which verifies its legitimacy to the vehicle. To verify the vehicle authenticity at the TA, the vehicle signature Y_1 has to be checked. In addition, the TA can recover the vehicle true identity ID_i from the ticket r_1 using the shared sub-key S_1. This sub-key is only defined to both the TA and vehicle. Moreover, the vehicle verifies the authenticity of the TA by checking the correctness of the signature Y_4. Only the authorized TA can issue the correct value of Y_4 using its private key c. Furthermore, the ticket r_4 is protected by the shared key S that is typically calculated according to one of the two choices mentioned below:

- With the aid of the TA private key c and vehicle public key A at the TA side.
- Using the TA public key C and vehicle private key a at the vehicle side.

The third form of authentication is vehicle-RSU. Based on this form, the authenticity of the vehicle and RSU can be verified by a challenge for both of them to have the ability to form the full session key K. Both the vehicle and RSU have the partial session key Snky after their successful authentication with the TA. No authentication is performed between the vehicle and RSU until each of them verifies its legitimacy to the TA. This key Snky is safely delivered to the RSU according to the ticket r_3 that is secured by the sub-key Q_1. Additionally, the ticket r_4 is utilized to privately exchange Snky between the TA and vehicle, protected by the key S. The shared sub-key Q_1 is only defined to the TA and RSU despite the fact that only the TA and vehicle know the symmetric key S. When the vehicle attempts to request an emergency service from the RSU, it generates the full session key K according to Snky, the vehicle private key a, and RSU public key B. Then, the RSU proves the authenticity of the vehicle by the ticket r_6 that is secured by the sub-key K_1. The RSU is proved to be authorized to the vehicle according to the ticket r_7 which can only be issued by the sub-key K_2.

B. NON-REPUDIATION

All the messages exchanged within the proposed protocol must be incorporated with the entity signature using its private key. The vehicle cannot deny the transmission of the tickets r_1 and r_6 when they are securely signed by the vehicle private key a. Hence, the only authorized vehicle can issue the signatures Y_1 and Y_6. Besides, the tickets Y_2 and Y_7 can be considered as the RSU signatures on the values r_2 and r_7 using the RSU private key b. All messages sent by the TA to both the vehicle and RSU such as r_3, r_4, and r_5 are signed by the TA private key c. Thus, no entity in the whole network has the ability to generate the signatures of the TA: Y_3, Y_4, and Y_5 without the knowledge of c.

C. TRACEABILITY

This feature is achieved in the proposed protocol, where the TA is the only entity within the network that can recover the vehicle true identity ID_i in case of any misbehaving actions. According to this, the TA can extract the correct value of ID_i from the ticket r_1 using the secret sub-key S_1 that is only exchanged between the TA and vehicle itself.

D. UNLINKABILITY

The protocol ensures that the vehicle pseudo-identity PID_i has to be unique for different sessions. The exchanged traffic between entities in each session has to be changeable as well. Thus, the messages r_1, r_2, and C_1 are distinct per session according to the change of the timestamps t_3 and t_4. The values of both r_3 and r_4 are changeable based on the partial session key Snky. It is well-known that Snky is different in each session, where the change of PID_i results in a different value for r_5. The values r_6 and r_7 are protected using K_1 and K_2, respectively, whereas, this sub-keys are changeable according to the change in Snky.

E. PRESERVING IDENTITY PRIVACY

In the proposed protocol, the real identity of the vehicle ID_i is protected from being eavesdropped during the transmission. Specifically, the tickets r_1 and r_4 that have ID_i are sent, secured by the sub-key S_1 and secret key S, respectively. No entity has the ability to reveal the true value of ID_i without the knowledge of S.

F. NO CERTIFICATE DEPENDENCY

The proposed protocol relies on the certificate transmission during the registration phase. Each entity attempts to join the VANET has to prove its authenticity to the TA which issues a certificate for the authorized entity public key. This certificate is used to bind the authorized entity with its public key by the TA private key c. After that, a key establishment mechanism is started to share a symmetric key between the entity and TA. All the subsequent transmissions between the entity and TA are protected using this symmetric key. In the authentication phase: all the exchanged tickets between the vehicle and TA: r_1, r_4, and r_5 are protected using the symmetric key S and its separated values S_1 and S_2. The entire traffic exchanged between the RSU and TA is also secured using Q_1 and Q_2.

G. FAST RESPONSE IN EMERGENCY CONDITIONS

The new proposed protocol serves the emergency appeal sent from the vehicle to the nearest RSU. Each vehicle can request an emergency service from the RSU and this request r_6 is secured by a full session sub-key K_1 that is changeable in each session. Besides, the RSU responds to the vehicle using the

ticket r_7. Only the lightweight operations such as rotation and XOR functions are utilized to ensure a fast response to any request received from the vehicle. Moreover, the signatures Y_6 and Y_7 are executed by the Chebyshev chaotic map that is defined to be more lightweight than the general hash function. According to Fig. 5, the vehicle sends its emergency request to the RSU as follows:

- Generating the full session key K requires 1 Chebyshev function in addition to 1 modular operation.
- Encrypting the emergency appeal Emreqt needs 1 rotation process and the creation of the signature Y_6 requires 1 Chebyshev computation.

Accordingly, the execution time for the vehicle to execute its operations is $2t_c + 1t_m + 1t_r$. Also, the RSU itself replies to the vehicle emergency appeal according to the following:

- Checking the validity of the received signature Y_6 requires 1 Chevbyshev function.
- Generating the total session key K needs 1 Chebyshev function and 1 modular operation.
- Recovering the vehicle appeal Emreqt from r_6 needs 1 rotation process in addition to 1 XOR operator.
- Encrypting the emergency reply Emrep requires 1 rotation function. Besides, the creation of the signature Y_7 needs 1 Chebyshev process.

Hence, the execution time for the RSU to perform the previous operations is $3t_c + 1t_x + 1t_m + 2t_r$. Furthermore, the vehicle can extract the emergency reply as follows:

- Checking the validity of the received signature Y_7 necessitates 1 Chevbyshev function.
- Recovering the RSU reply Emrep from r_7 requires 1 rotation process and 1 XOR operator.

Thus, the total execution time for the vehicle to send the emergency appeal and recover the reply is $3t_c + 1t_x + 1t_m + 2t_r$. However, several schemes such as [25]–[28] ignore the values of t_x and t_r due to their negligible execution time. Furthermore, the Chebyshev chaotic map is widely utilized in the VANET domain as it is proved to be appropriate for computationally limited devices [13], [20], [27]–[29].

H. RESISTANCE TO SEVERAL ATTACKS

The proposed protocol is proved to be effective in countering forgery, impersonation, and replay attacks as follows: Firstly, the new protocol utilizes the digital signatures based on the Chebyshev chaotic map to achieve data integrity and prevent any forgery attack. Any attacker's attempt to alter the traffic transferred over the medium is easily detected and the attacker cannot alter the signature itself without the entity private key. In details, the tickets r_1 and r_6 are signed by the vehicle private key a to generate the signatures Y_1 and Y_6. Similarly, the values r_2 and r_7 are signed by the RSU private key b to generate the signatures Y_2 and Y_7. In addition, the values Y_3, Y_4, and Y_5 can be considered as the TA signatures on the messages r_3, r_4, and r_5, respectively. Moreover, the attacker cannot modify the values of the messages C_1 and C_2 without having Q_2. Secondly, the attacker cannot impersonate the identity of any entity within the network.

TABLE 11. Security claims of Scyther and their definitions.

Claim	Definition
Secret	The parameter can be considered as Secret if it is protected from the adversary during the execution of the protocol
Alive	Based on this claim, the authentication feature between two entities is evaluated
Weakage	The protocol can ensure that this claim is satisfied when each entity has the ability to complete a run of the protocol, apparently with another entity
Niagree	This claim indicates that both the sender and receiver agree on their shared parameters exchanged
Nisynch	This term reflects the synchronization status between the communicating participants in the protocol

To impersonate the vehicle, the attacker has to find the true values of both ID_i and S which are only known to the TA and vehicle. Furthermore, the authorized TA is the only entity that can recognize the real location of the authenticated RSU L_j. Additionally, the attacker has to discover the value of Q to impersonate the RSU. The public key of the authorized TA is also downloaded into the memory of the vehicle and RSU during the network deployment phase. Hence, the transmission of the digital signatures, which are generated by the entities private keys and cannot be forged, protects the entire traffic within the VANET. Thirdly, no replay attack can be carried out against the new protocol. All the tickets from r_1 to r_7 as well as the values C_1 and C_2 are emerged with the timestamps. The new proposed protocol clearly states that if $(t'_m - t_m > \Delta t)$, the timestamp is not fresh and the session is terminated.

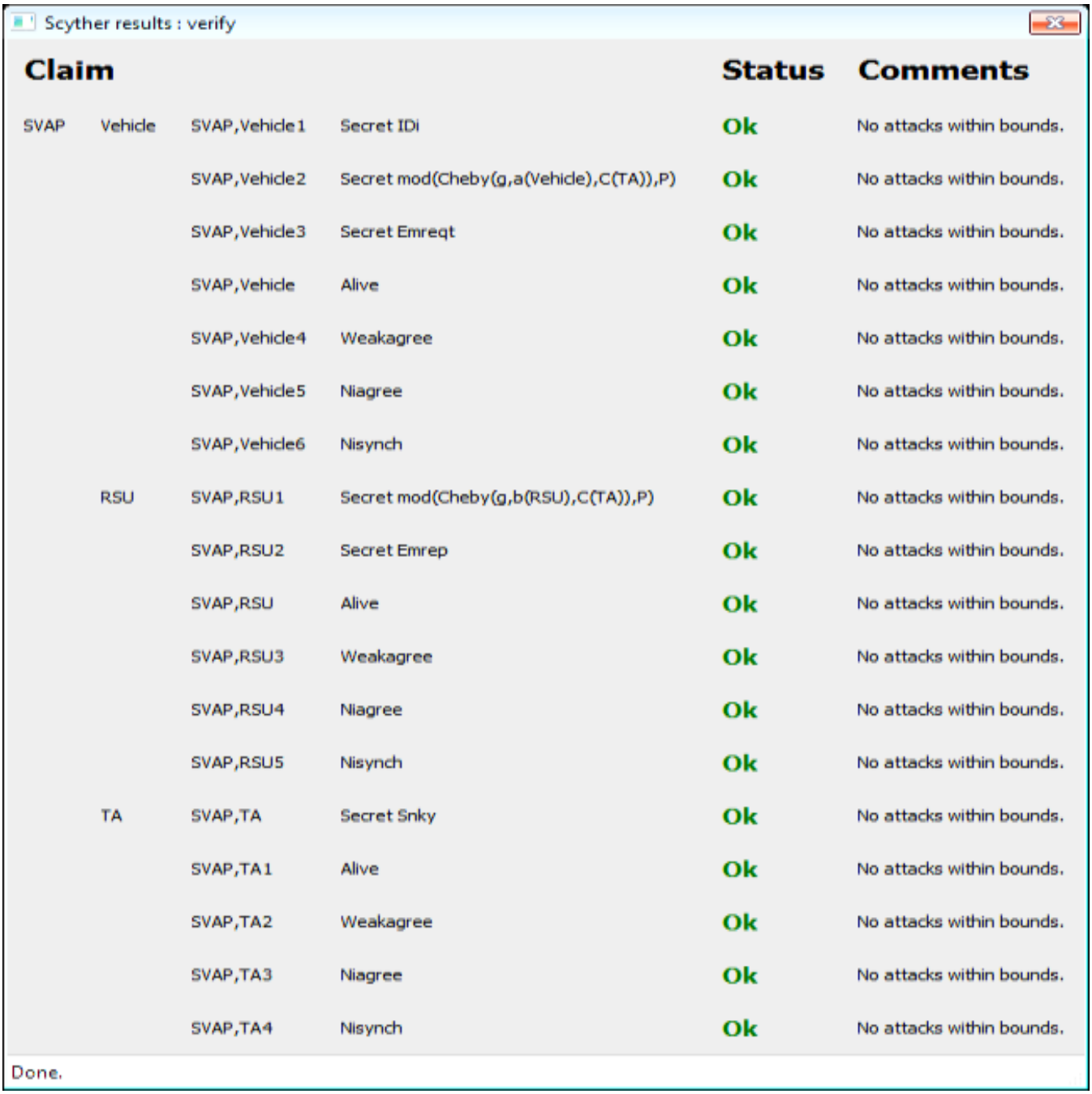
VI. FORMAL SECURITY EVALUATION USING SCYTHER

In this section, the security robustness of the proposed protocol is analyzed using a cryptographic verification tool. The main aim of this tool is to evaluate the security properties of the proposed protocol to show any detected attacks on the analyzed scheme. To perform this evaluation, the Scyther is chosen according to its free usage and high performance [13]. The Scyther can be considered as a widely accepted security verification tool in the academic field as it provides a reliable simulation environment to reveal various vulnerabilities of the protocol that can be misused by the attacker [30], [31]. Accordingly, the simulation is mainly based on various security claims as indicated in Table 11.

The proposed protocol is modelled using Security Protocol Description Language (SPDL) to allow Scyther analyze the security properties included in the model. To build the protocol code, 4 terms have to be specified as follows:

- Role.
- Functions that are used within the protocol.
- Parameters which are required to be defined.
- Security claims.

In the Scyther code, the role can be described as any entity that has the ability to take actions to be performed within the protocol. These actions may be sending or receiving



Scyther results : verify

Claim				Status	Comments
SVAP	Vehicle	SVAP,Vehicle1	Secret IDi	Ok	No attacks within bounds.
		SVAP,Vehicle2	Secret mod(Cheby(g,a(Vehicle),C(TA)),P)	Ok	No attacks within bounds.
		SVAP,Vehicle3	Secret Emreqt	Ok	No attacks within bounds.
		SVAP,Vehicle	Alive	Ok	No attacks within bounds.
		SVAP,Vehicle4	Weakagree	Ok	No attacks within bounds.
		SVAP,Vehicle5	Niagree	Ok	No attacks within bounds.
		SVAP,Vehicle6	Nisynch	Ok	No attacks within bounds.
	RSU	SVAP,RSU1	Secret mod(Cheby(g,b(RSU),C(TA)),P)	Ok	No attacks within bounds.
		SVAP,RSU2	Secret Emrep	Ok	No attacks within bounds.
		SVAP,RSU	Alive	Ok	No attacks within bounds.
		SVAP,RSU3	Weakagree	Ok	No attacks within bounds.
		SVAP,RSU4	Niagree	Ok	No attacks within bounds.
		SVAP,RSU5	Nisynch	Ok	No attacks within bounds.
	TA	SVAP,TA	Secret Snky	Ok	No attacks within bounds.
		SVAP,TA1	Alive	Ok	No attacks within bounds.
		SVAP,TA2	Weakagree	Ok	No attacks within bounds.
		SVAP,TA3	Niagree	Ok	No attacks within bounds.
		SVAP,TA4	Nisynch	Ok	No attacks within bounds.

Done.

FIGURE 6. Security analysis result of the proposed protocol using Scyther.

messages and are specified by send or recv events. Hence, the code has 3 roles as follows:

- Vehicle.
- RSU.
- TA.

Also, all related functions have to be declared at the beginning of the simulation code. Although the private key of each entity is declared as Secret, the public key is defined as Const. In addition, the timestamp declarations are utilized to define the timestamps from t_1 to t_8. The security claims are the events that are used in the definition of each role to model the security properties of the protocol as previously indicated in Table 11. The Scyther report in Fig. 6 confirms the security of the proposed protocol. According to this report, it is proved that the new protocol is not vulnerable to attacks. Additionally, the real identity of the vehicle ID_i is proved to be Secret within the protocol. The term $T_{g^a}(C)$ mod p in the proposed protocol can be written as mod(Cheby(g,a(Vehicle),C(TA)),P) in the Scyther code. This term defines the value of the shared symmetric key S between the vehicle and TA and it is proved to be Secret in the Scyther simulation. Besides, both Emreqt and Emrep satisfy

the Secret claim. The shared key Q between the RSU and TA is described as $T_{g^b}(C)$ mod p in the proposed protocol and can be written as mod(Cheby(g,b(RSU),C(TA)),P) according to the Scyther. Based on the simulation, it is found that Q is Secret. Moreover, the shared session key Snky between the vehicle and RSU is proved to be Secret according to the Scyther claims.

Altogether, the proposed protocol can be considered appropriate for the VANET domain due to the following:

- The new protocol attempts to be adequate for the limited storage overhead of the OBU by ignoring the usage of the hash function SHA-256 due to its output limitation size of 256 bits. This results in a reduction in the storage space of the OBU.
- Based on Wolfram Mathematica, the performance evaluation is performed in the section IV, proving that the proposed protocol has less computational, communication, and storage costs than the scheme [14].
- The security of the proposed protocol is also verified according to the Scyther simulation. The result report in Fig. 6 proves that the protocol is secured against attacks.
- The core operations which are utilized throughout all phases of the new protocol are lightweight processes. The protocol is mainly based on the rotation, modular, and XOR operations in addition to the Chebyshev function. According to [25]–[28], the execution time of the rotation and XOR operations can be ignored as each process consumes a negligible time.
- In [24], the Chebyshev chaotic map is defined to be more lightweight than the hash function. Furthermore, this map is frequently applied in the VANET authentication protocols [13], [20], [27]–[29] due to its lightweight computational properties.

VII. CONCLUSION

This paper proposes for the first time in the VANET domain a novel authentication protocol for emergency applications. The new protocol is integrated with a key establishment mechanism based on the Chebyshev chaotic map. It also takes the advantage of lightweight computations of the symmetric key cryptosystem with non-repudiation feature achieved by the public key cryptosystem. Hence, the paper introduces a new design for the VANET with no secure channels between entities within the entire structure. Comparing to the most recent related scheme, it is revealed that the computing and storage costs of the OBU are improved by the proposed protocol with 24.09% and 16.99%, respectively. Besides, the new protocol is proved to be superior according to the comparison with the other schemes in terms of security features and network characteristics. The new structure of the VANET contributes in the reduction of network deployment cost due to the usage of lightweight functions such as rotation, modular addition, and XOR operations. Moreover, the Scyther is utilized to evaluate the proposed protocol and its simulation result confirms the security robustness of the new protocol.

REFERENCES

[1] 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, 2020, doi: 10.1109/ACCESS.2020.3024587.

[2] 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, doi: 10.1109/ACCESS.2021.3053043.

[3] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A new and efficient RSU based authentication scheme for VANETs," *Wireless Netw.*, vol. 26, pp. 3083–3098, Jun. 2020, doi: 10.1007/s11276-019-02039-x.

[4] H. Jiang, L. Hua, and L. Wahab, "SAES: A self-checking authentication scheme with higher efficiency and security for VANET," *Peer Peer Netw. Appl.*, vol. 14, no. 2, pp. 528–540, Mar. 2021, doi: 10.1007/s12083-020-00997-0.

[5] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101664, doi: 10.1016/j.cose.2019.101664.

[6] Z.-C. Liu, L. Xiong, T. Peng, D.-Y. Peng, and H.-B. Liang, "A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 26307–26317, 2018, doi: 10.1109/ACCESS.2018.2834224.

[7] J. Qi and T. Gao, "A privacy-preserving authentication and pseudonym revocation scheme for VANETs," *IEEE Access*, vol. 8, pp. 177693–177707, 2020, doi: 10.1109/ACCESS.2020.3027718.

[8] I. Z. Ahmed, T. M. Mohamed, and R. A. Sadek, "A low computation message delivery and authentication VANET protocol," in *Proc. 12th Int. Conf. Comput. Eng. Syst. (ICCES)*, Cairo, Egypt, Dec. 2017, pp. 204–211, doi: 10.1109/ICCES.2017.8275303.

[9] S. Mirzaee and L. Jiang, "Fast confidentiality-preserving authentication for vehicular ad hoc networks," *J. Shanghai Jiaotong Univ., Sci.*, vol. 24, no. 1, pp. 31–40, Feb. 2019, doi: 10.1007/s12204-019-2038-x.

[10] S. Wang, K. Mao, F. Zhan, and D. Liu, "Hybrid conditional privacy-preserving authentication scheme for VANETs," *Peer Peer Netw. Appl.*, vol. 13, no. 5, pp. 1600–1615, Sep. 2020, doi: 10.1007/s12083-020-00916-3.

[11] H. Tan, Z. Gui, and I. Chung, "A secure and efficient certificateless authentication scheme with unsupervised anomaly detection in VANETs," *IEEE Access*, vol. 6, pp. 74260–74276, 2018, doi: 10.1109/ACCESS.2018.2883426.

[12] Z. Benyamina, K. Benahmed, and F. Bounaama, "ANEL: A novel efficient and lightweight authentication scheme for vehicular ad hoc networks," *Comput. Netw.*, vol. 164, Dec. 2019, Art. no. 106899, doi: 10.1016/j.comnet.2019.106899.

[13] R. Ma, J. Cao, D. Feng, H. Li, B. Niu, F. Li, and L. Yin, "A secure authentication scheme for remote diagnosis and maintenance in Internet of Vehicles," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Seoul, South Korea, May 2020, doi: 10.1109/WCNC45663.2020.9120719.

[14] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for VANETs," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3547–3557, Sep. 2020, doi: 10.1109/JSYST.2020.2991168.

[15] X.-Y. Guo, D.-Z. Sun, and Y. Yang, "An improved three-factor session initiation protocol using Chebyshev chaotic map," *IEEE Access*, vol. 8, pp. 111265–111277, 2020, doi: 10.1109/ACCESS.2020.3002558.

[16] R. I. Abdelfatah, M. E. Nasr, and M. A. Alsharqawy, "Encryption for multimedia based on chaotic map: Several scenarios," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19717–19738, Jul. 2020, doi: 10.1007/s11042-020-08788-8.

[17] T. T. K. Hue, T. M. Hoang, and A. Braeken, "Lightweight signcryption scheme based on discrete Chebyshev maps," in *Proc. 12th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Cambridge, MA, USA, Dec. 2017, pp. 43–47, doi: 10.23919/ICITST.2017.8356343.

[18] Z. Shen, P. Zeng, Y. Qian, and K.-K.-R. Choo, "A secure and practical RFID ownership transfer protocol based on Chebyshev polynomials," *IEEE Access*, vol. 6, pp. 14560–14566, 2018, doi: 10.1109/ACCESS.2018.2809480.

[19] R. I. Abdelfatah, "Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations," *IEEE Access*, vol. 8, pp. 69894–69907, 2020, doi: 10.1109/ACCESS.2020.2987197.
[20] J. Cui, Y. Wang, J. Zhang, Y. Xu, and H. Zhong, "Full session key agreement scheme based on chaotic map in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8914–8924, Aug. 2020, doi: 10.1109/TVT.2020.2997694.
[21] R. I. Abdelfatah, "Secure image transmission using chaotic-enhanced elliptic curve cryptography," *IEEE Access*, vol. 8, pp. 3875–3890, 2020, doi: 10.1109/ACCESS.2019.2958336.
[22] S. F. Aghili and H. Mala, "Security analysis of an ultra-lightweight RFID authentication protocol for m-commerce," *Int. J. Commun. Syst.*, vol. 32, no. 3, p. e3837, Feb. 2019, doi: 10.1002/dac.3837.
[23] C. Alvin, B. Peterson, and S. Mukhopadhyay, "Static generation of UML sequence diagrams," *Int. J. Softw. Tools Technol. Transf.*, vol. 23, no. 1, pp. 31–53, Feb. 2021, doi: 10.1007/s10009-019-00545-z.
[24] B. D. Deebak, F. Al-Turjman, and A. Nayyar, "Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care," *Multimedia Tools Appl.*, vol. 80, no. 11, pp. 17103–17128, Nov. 2020, doi: 10.1007/s11042-020-10134-x.
[25] Y. Chen, J. Yuan, and Y. Zhang, "An improved password-authenticated key exchange protocol for VANET," *Veh. Commun.*, vol. 27, Jan. 2021, Art. no. 100286, doi: 10.1016/j.vehcom.2020.100286.
[26] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment," *IEEE Trans. Ind. Informat.*, vol. 16, no. 11, pp. 7081–7093, Nov. 2020, doi: 10.1109/TII.2019.2942389.
[27] J. Miao, Z. Wang, X. Miao, and L. Xing, "A secure and efficient lightweight vehicle group authentication protocol in 5G networks," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–12, Sep. 2021, doi: 10.1155/2021/4079092.
[28] B. D. Deebak and F. Al-Turjman, "A smart lightweight privacy preservation scheme for IoT-based UAV communication systems," *Comput. Commun.*, vol. 162, pp. 102–117, Oct. 2020, doi: 10.1016/j.comcom.2020.08.016.
[29] D. Abbasinezhad-Mood, A. Ostad-Sharif, S. M. Mazinani, and M. Nikooghadam, "Provably secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection," *IEEE Trans. Ind. Informat.*, vol. 16, no. 12, pp. 7287–7294, Dec. 2020, doi: 10.1109/TII.2020.2974258.
[30] M. Safkhani, C. Camara, P. Peris-Lopez, and N. Bagheri, "RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing," *Veh. Commun.*, vol. 28, Apr. 2021, Art. no. 100311, doi: 10.1016/j.vehcom.2020.100311.
[31] R. Amin, I. Pali, and V. Sureshkumar, "Software-defined network enabled vehicle to vehicle secured data transmission protocol in VANETs," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102729, doi: 10.1016/j.jisa.2020.102729.

ROAYAT I. ABDELFATAH received the B.Sc. degree in electronics and electrical communications engineering and the M.Sc. and Ph.D. degrees from Tanta University, Egypt, in 2000, 2005, and 2011, respectively. She was an Associate Professor from Tanta University, in 2020. The M.Sc. is dedicated to encryption algorithms and their applications. The Ph.D. is devoted to introducing new encryption, digital signature, and hash function algorithms for securing the digital data over communication networks. Her research interests include network security and multimedia applications.

NERMEEN M. ABDAL-GHAFOUR received the B.Sc. and M.Sc. degrees in electronics and electrical communications engineering from Tanta University, Egypt, in 2012 and 2017, respectively. She is currently pursuing the Ph.D. degree in the security of vehicular *ad hoc* networks. Her M.Sc. is dedicated to improving the authentication protocols of electronic passports to counter the terrorist attacks. Her research interests include network security and emergency applications.

MOHAMED E. NASR received the B.Sc. degree (Hons.) in electronics, in 1975, and the M.Sc. and Ph.D. degrees, in 1979 and 1985, respectively. He is currently a Professor of digital communications and computer networks with the Department of Electronics and Communications, Faculty of Engineering, Tanta University, Egypt. From 2001 to 2007, he was the Head of the department. He has published more than 170 journals and conference scientific papers. He was the Vice Chairperson of the 25th National Radio Science Conference (NRSC), Tanta, Egypt, in 2008. From 2006 to 2009, he was the President of the Administration Board for Information and Communication Technology Project (ICTP) at Tanta University, and the Leader of the technical team to manage and modify Tanta University Network. Since September 2009, he has been a Chief Information Officer (CIO) and the Coordinator at Tanta University, until January 2010. From September 2014 to August 2016, he was the Dean of the Alexandria Higher Institute of Engineering and Technology, Alexandria, Egypt. His current research interests include wireless communication systems and network security.