Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 4079092, 12 pages
https://doi.org/10.1155/2021/4079092

Research Article

A Secure and Efficient Lightweight Vehicle Group Authentication Protocol in 5G Networks

Junfeng Miao, Zhaoshun Wang, Xue Miao, and Longyue Xing

The School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China

Correspondence should be addressed to Zhaoshun Wang; zhswang@sohu.com

Received 3 July 2021; Accepted 13 August 2021; Published 22 September 2021

Academic Editor: Weizhi Meng

When mobile network enters 5G era, 5G networks have a series of unparalleled advantages. Therefore, the application of 5G network technology in the Internet of Vehicles (IoV) can promote more intelligently vehicular networks and more efficiently vehicular information transmission. However, with the combination of 5G networks and vehicular networks technology, it requires safe and reliable authentication and low computation overhead. Therefore, it is a challenge to achieve such low latency, security, and high mobility. In this paper, we propose a secure and efficient lightweight authentication protocol for vehicle group. The scheme is based on the extended chaotic map to achieve authentication, and the Chinese remainder theorem distributes group keys. Scyther is used to verify the security of the scheme, and the verification results show that the security of the scheme can be guaranteed. In addition, through security analysis, the scheme can not only effectively resist various attacks but also guarantee security requirements such as anonymity and unlinkability. Finally, by performance analysis and comparison, our scheme has less computation and communication overhead.

1. Introduction

It is an inevitable trend that all things are connected. With the development of the IoV, vehicular networks are becoming more and more important in modern life [1]. By the continuous increase of motor vehicles, road traffic has become gradual complex, which results in higher requirements for the IoV [2, 3]. As mobile cellular networks rapidly develop, 5G networks have officially entered our lives. Due to the characteristics of 5G networks (high speed, low latency, high reliability, and wide coverage) and the newly concomitant technologies (millimeter wave communication, MIMO, D2D, etc.), it greatly improves the mobile Internet field of IoV [4–6]. Supporting Internet of Vehicles services through 5G network technology can overcome the limitations of current IoV. Recently, more attention is paid on the integration of 5G technology and the IoV [7].

The deepening application of 5G technology provides a strong guarantee for the vehicular networks. The current research of vehicular networks focuses on driving safety, improving the traffic efficiency of vehicles, ensuring the safe and efficient communication between vehicle and vehicle (V2V) and vehicle and roadside infrastructure (V2I), and realizing the vehicle safety applications such as emergency braking warning [2]. This can effectively avoid vehicle collisions or reduce the personal injury caused by traffic accidents. Vehicular network communication mainly relies on Cellular Vehicle to Everything (C-V2X) [8]. Through the communication among vehicle to vehicle, vehicle to person, vehicle to infrastructure, and vehicle to network, it can ensure the driving safety and comfort and drive the realization of automatic driving.C-V2X includes two standards: Long-Term Evolution Vehicle to Everything (LTE-V2X) and 5G Vehicle to Everything (5G-V2X). Compared with the two standards, the performance of 5G-V2X is better than that of LTE-V2X [9]. LTE-V2X has insufficient delay and reliability, while 5G-V2X has the advantages of long coverage time, low delay and high reliability. It can obtain various state information of the road timely and accurately, interact with each other in real time, and complete the driving task better. It is the key technology of the future of the Internet of vehicles application, especially the autonomous driving and overtake, which require very low network latency [10]. At the same time, as a kind of ultrareliable and low-latency

communications (URLLC), it requires safe and reliable authentication and low computation overhead [11, 12]. Therefore, a better solution is to use group key agreement (GKA) in vehicle group [13]. In this way, the vehicle group communicate safely. So, our paper mainly studies the key agreement scheme between groups in the Internet of Vehicles under the 5G networks. In addition, due to the openness of the wireless channel, the signal exposed in the open environment is likely to be stolen, interfered, or even modified by the attacker, which brings adverse effects to the vehicular networks [14–17].

This paper proposes a vehicle group authentication protocol based on extended chaotic mapping in 5G networks. This solution enables the participating vehicles to communicate securely through the group key in the 5G networks. Therefore, this paper mainly does the following work:

(1) This paper proposes a vehicle group authentication scheme under the 5G network architecture. In order to protect the security of RSU, the shared key will be updated. In addition, this scheme is a lightweight authentication scheme based on extended chaotic mapping and distributes group key through Chinese remainder theorem

(2) This paper verifies the security of the scheme by using the Scyther tool

(3) By comparing the existing schemes, this scheme can effectively reduce the computation and communication overhead

Other parts of this paper are as follows. Section 2 reviews the related research work of this paper. Section 3 introduces the preliminary knowledge of this paper. Section 4 introduce a lightweight and secure vehicle group authentication protocol in detail. We carried out security and performance analysis, respectively, in Sections 5 and 6. Finally, Section 7 summarizes the full paper.

2. Related Work

At present, in order to solve the problems faced by vehicular networks, the scholars have proposed many authentication schemes for vehicular networks. The following mainly introduces from three aspects: group signature authentication, group key agreement, and based on trusted authority.

First, we introduce the authentication protocol based on group signature. In 2011, Huang et al. [18] proposed an anonymous batch identity authentication and key agreement protocol in the Internet of Vehicles. The scheme could not only authenticate request messages from multiple vehicles but also carry out key agreement. Cui et al. [19] proposed a solution based on software without relying on any special hardware. In the batch verification stage, it adopted cuckoo filtering and binary search methods, which achieved a higher success rate than previous solutions. Vijayakumar et al. [20] proposed a privacy preserving anonymity scheme with high computational efficiency. At the same time, an efficient anonymous batch authentication protocol was introduced to authenticate multiple vehicles on the road of the Internet of Things, which reduced the authentication time and was more efficient in certificate and signature verification. These schemes can complete the certification of vehicle group. However, these schemes will bring higher verification costs, thereby affecting the performance of the schemes.

Next, we introduce the related group key agreement. In 2016, Han et al. [21] established an efficient group authentication scheme by adopting a self-certification without certification authority. The scheme could set up groups between roadside units and vehicles. In [22], Vijayakumar et al. proposed a dual group key scheme, which distributed the group keys to each vehicle and ensured that the group keys were updated. In [23], Vijayakumar et al. proposed an effective anonymous group key distribution protocol, which can safely distribute the group key to the vehicle group. The RSU can use the group key to send location-based information to the vehicle group in a secure way. In 2018, Cui et al. [24] proposed a conditional privacy preserving authentication scheme based on hash function. The scheme distributed group keys through the mechanism of the Chinese remainder theorem (CRT) and provided update mechanism for vehicles to join and leave. Zhang et al. [25] proposed an identity authentication scheme based on the Chinese remainder theorem (CRT). This scheme avoided the use of bilinear pairing operations and solved the leakage problem of side channel attacks, and both safety and performance were guaranteed. In [26], Lai et al. proposed a lightweight group access authentication scheme based on message authentication code aggregation technology, which could resist DoS attacks. In 2019, Zhang et al. [27] proposed a group key agreement protocol, in which directional attribute layering was used. Shi et al. [28] proposed a password-based conditional confidentiality authentication and group key generation protocol. The protocol provided the generation of group keys, and the calculation and communication overheads were small. In 2020, Gharsallah et al. [29] proposed a scheme to authenticate a group of vehicles in 5G networks. The protocol supported group authentication of vehicle equipment in 3GPP network. Cui et al. [13] proposed a session key agreement scheme based on chaotic mapping. In this scheme, the fog server was introduced, and the chaotic mapping algorithm was used for group key agreement between vehicles. In this group, vehicles could communicate with each other through group key. Zhang et al. [30] proposed a privacy preserving authentication framework based on edge technology in 5G-enabled vehicular networks. In this scheme, edge computing was used to calculate and verify on vehicles, so as to achieve the communication between vehicles. Ouaissa et al. [31] proposed an authentication protocol for a large number of vehicle equipment following 5G-AKA authentication framework. The protocol used ECDH algorithm to establish the key and authenticate the identity, which ensured the information security and integrity. Although the scheme could resist a variety of attacks, the computation overhead was relatively large. Although these schemes reduced the cost of verification, some schemes had a large computation and communication overhead, which affected the performance of the schemes.

Thirdly, we introduce the authentication protocol based on trusted authority. Azees et al. [32] proposed an effective anonymous authentication scheme. The scheme provided a conditional tracking mechanism to prevent malicious vehicles from entering the VANET. Zhang et al. [33] proposed a many-to-many authentication and key agreement scheme for security authentication between multiple vehicles and CSP. Under the premise of information leakage, this scheme could prevent illegal access and provide key security. In 2019, Cui et al. [34] proposed a lightweight authentication protocol based on reputation system for 5G-enabled vehicular networks. The authority was responsible for reputation management, and vehicles with low reputation score could not participate in communication, which significantly reduces the possibility of untrusted vehicles entering IoV. Huang et al. [35] proposed a new privacy preserving authentication scheme based on 5G software-defined vehicular networks. This scheme uses 5G software to define the advantages of the network, so that the vehicle certification process will only need light-weighted hash operation, thus greatly reducing the computation overhead. Li et al. [36] proposed a lightweight authentication scheme. In this scheme, only hash function and XOR operations are used to realize vehicle identity authentication and anonymity. Wang et al. [37] proposed a lightweight authentication protocol that could avoid emergency vehicles in VANET. After the first authentication with the nearest roadside unit, the scheme could complete the mutual authentication with the subsequent roadside unit without repeating the cumbersome calculation. Although these schemes can resist various attacks and ensure the safety of vehicles, they are not suitable for vehicle group authentication, and some schemes have relatively large computation overhead.

3. Preliminaries

3.1. System Model. This paper mainly studies the vehicle communication in the same RSU range in V2V communication. As shown in Figure 1, the specific system model includes the following communication entities.

5G core (5GC): 5GC controls the entire 5G-V2X network and provides mobile data connection and services. 5GC is divided into access and mobility management function (AMF), security anchor function (SEAF), authentication server function (AUSF), authentication credential repository and processing function (ARPF), and unified data management (UDM) [38]. AMF is responsible for handling connection and mobility management tasks. SEAF is used for authentication and communication. AUSF performs identity verification. ARPF calculates authentication data and keys. UDM carries functions related to data management. According to literature [38], UDM should be protected from physical attacks. In addition, in order to ensure the security of vehicle identity, the security is provided and insured by technical and legal [39]. In order to simplify the certification process and facilitate research, they are collectively referred to as 5GC.

Trusted authority (TA): TA is a completely trusted public organization, which is mainly responsible for system initialization, generation of public parameters, and registration for other entities participating in communication. In the registration stage, TA generates the pseudonym of the vehicle, then records the real identity of the vehicle, and shares the data with 5GC through the secure channel [29]. When a malicious vehicle is found, the 5GC can directly identify the opponent by searching for the malicious vehicle.

Roadside unit (RSU): RSU is an important communication entity in the system. It acts as a roadside unit to communicate with the vehicle in real time.

Vehicles: Each vehicle has an on-board unit (OBU), and each OBU has an antitampering device to protect secret information. It is responsible for collecting relevant information and transmitting other vehicles and RSU.

3.2. Security Requirements. The main goal of this article is to design a lightweight, safe, and effective vehicle group communication solution in the 5G networks to ensure the safe communication of the vehicular networks. Therefore, here are the security requirements to be met [13, 29–31, 34–37, 40–45].

(1) Anonymity: the true identity of the vehicle must not be disclosed to any organization or user other than the authority and 5GC. To ensure that the attacker cannot obtain the true identity of the vehicle from the transmitted data, the vehicles participating in the communication should use fake identities

(2) Message authentication and integrity: in the process of vehicle communication, the authenticity and integrity of the transmitted data should be guaranteed. The receiver can confirm that the received content is a true and complete message by authenticating the sender, rather than a message forged or modified by others

(3) Traceability: when there is a malicious vehicle that releases false information, the authority can quickly trace the real identity of the malicious vehicle and broadcast its real identity to the outside world

(4) Unlinkability: the attacker cannot link different messages of the same vehicle through intercepted transmission data.

(5) Common attack resistance: it can resist common attacks such as replay attacks, man-in-the-middle attacks, and modification attacks in the Internet of Vehicles

3.3. Chebyshev Chaotic Mapping. Bergamo et al. [46] clearly proposed that public-key cryptographic algorithms designed based on the semigroup characteristics of Chebyshev polynomial did not satisfy security. Therefore, the solution in this paper adopts the more secure extended Chebyshev polynomial proposed by Zhang [47], which is defined as follows:

Definition 1. Let n be a positive integer, $x \in (-\infty, +\infty)$, n -order Chebyshev polynomial is defined as:

$$T_n(x) = \cos\left(n \arccos(x)\right) \bmod P. \tag{1}$$

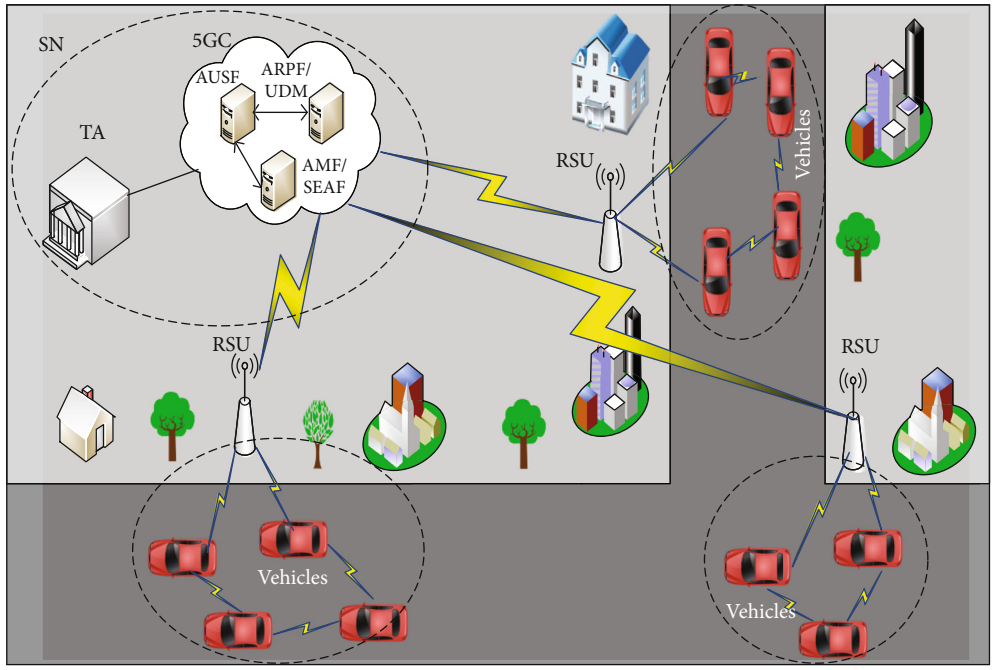

Figure 1: System model.

The iterative relation of Chebyshev polynomial is as follows:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) \bmod P, \tag{2}$$

where $T_0(x) = 1$, $T_1(x) = x \bmod P$, $n \geq 2$, and P is a large prime [48].

Property 2. Semigroup property

Let n, r, and s be positive integers, and $n \geq 2, x \in (-\infty, +\infty)$:$T_r(T_s(x)) = T_s(T_r(x)) = T_{rs}(x) \bmod P$.

Property 3. Discrete logarithm problem of extended Chebyshev polynomials

Here, the value of the extended Chebyshev polynomial is $T_n(x) = y(\text{mod } p)$, given x, y, and a large prime number p, then solve for n' so that $T_{n'}(x) = y(\text{mod } p)$, which is a discrete logarithm difficult problem.

Property 4. Extended Chebyshev polynomial DH problem

Given $x \in (-\infty, +\infty)$, a large prime number p, and the value of the extended Chebyshev polynomial $T_r(x)(\text{mod } p)$, $T_s(x)(\text{mod } p)$ (r and s are positive integers), solving the value of the extended Chebyshev polynomial $T_{rs}(x)(\text{mod } p)$ is a Diffie-Hellman difficult problem [49].

3.4. Chinese Remainder Theorem. The definition of Chinese remainder theorem [50, 51] is as follows: Let $p_1, p_2, \cdots, p_n$ be pairwise prime integers.

$$\begin{cases} c \equiv y_1(\text{mod } p_1), \\ c \equiv y_2(\text{mod } p_2), \\ \vdots \\ c \equiv y_n(\text{mod } p_n). \end{cases} \tag{3}$$

Then, the positive integer solution of the congruence equation system can be expressed as:

$$c \equiv y_1P_1P_1' + y_2P_2P_2' + \cdots + y_nP_nP_n'(\text{mod } P), \tag{4}$$

where:-

$P = p_1p_2 \cdots p_n = p_1P_1 = p_2P_2 = \cdots = p_nP_n$.$P_i = P/p_i(i = 1, 2, \cdots, n)$; P_i' is an integer solution satisfying $P_iP_i' \equiv 1(\text{mod } p_i)(i = 1, 2, \cdots, n)$.

4. Proposed Scheme

Based on research [13, 18–36, 48], this paper proposes a vehicle group authentication protocol based on extended chaotic mapping in 5G networks. This solution enables the participating vehicles to communicate securely through the group key in the 5G networks. Table 1 lists the main notations used here. Figure 2 shows the detailed authentication process of the protocol.

4.1. System Setup. In this stage, TA generates public parameters and master private key for the system and preloads the public parameters to the RSU and vehicle. TA selects large prime numbers p and q, randomly selects a secret value $s_{TA} \in Z_q^*$ as the system key, selects $x \in (-\infty, +\infty)$, and

calculates the system public key $P_{TA} = T_{s_{TA}}(x)$. TA chooses the safe anticollision hash function, namely, $H_1 : \{0,1\}^* \longrightarrow Z_q^*, H_2 : \{0,1\}^* \longrightarrow \{0,1\}^*$. {G} is a prime number generation library, which contains infinite nonrepeated positive integers, and these positive integers are prime numbers to each other. The numbers are randomly selected for use and then discarded after use. This ensures that each number is not reused. Finally, TA publishes the system parameters $\{p, q, P_{TA}, x, H_1, H_2, \{G\}\}$.

4.2. Registration. At this stage, the vehicle and RSU obtain the required system parameters from TA and register with TA. The specific registration process is as follows.

(1) RSU registration

RSU_i first safely sends the network messages connected with TA.TA assigns unique identity EID_i to RSU_i, selects secret value $e_i \in Z_q^*$, and sends (EID_i, e_i) to RSU_i through secure channel. e_i is shared by RSU_i and TA, and $\{EID_i, e_i\}$ is stored in TA.

(2) Vehicle registration

The vehicle U_j first sends its real identity VID_j to TA through secure channel. TA selects $n_j \in Z_q^*$, and calculates $PID_j = H_1(VID_j \| s_{TA} \| n_j)$. TA stores VID_j in the database, then sends PID_j to the vehicle U_j and saves it to the OBU_j.

Here, the registration data stored in TA are shared with 5GC through secure channel.

4.3. Access Authentication

(1) When RSU_i detects that there is a group communication between vehicles, it broadcasts a group access authentication notification message to the surroundings

(2) When the vehicle receives the notification, the OBU_j of the vehicle that needs to access the network first generates a random number $h_j \in Z_q^*$, a prime number $y_j \in \{G\}$, and current timestamp T_j and calculates. $A_{j_1} = T_{h_j}(x), A_{j_2} = T_{h_j}(P_{TA})$
,-
$MAC_j = H_2(VID_j \| A_{j_2} \| A_{j_1} \| PID_j \| T_j), A_{j_3} = H_1(A_{j_2} \| T_j \| PID_j) \oplus (VID_j \| y_j \| MAC_j)$. Then OBU_j sends the message $\{PID_j, A_{j_1}, A_{j_3}, T_j\}$

(3) RSU_i receives authentication request messages from n members of the group and first verifies the validity of the timestamps. If they are legal, it selects the current timestamp T_i, generates group identity GID_i, and calculates $MAC_i = H_2(GID_i \| e_i \| EID_i \| T_i)$. Finally, RSU_i packages the generated message and received vehicle messages into $\{(PID_j, A_{j_1}, A_{j_3}, T_j)_{j=1,2\cdots,n}, GID_i, EID_i, MAC_i, T_i\}$ and sends them to 5GC

Table 1: Notations.

Notations	Definitions
TA	A trusted authority
RSU	A roadside unit
OBU	On-board units
H_i	The hash function
{G}	Mutually prime nonrepeating positive integer library
$\oplus$	Exclusive-OR operation
$\|\|$	Concatenation operation
T_x	The timestamp
p, q	The large prime number
P_{TA}	The system public key
s_{TA}	The system master key
MAC_x	Message authentication code

(4) When 5GC receives the message, it first verifies the validity of the timestamp T_i. If it is legal, it calculates $MAC_i' = H_2(GID_i \| e_i \| EID_i \| T_i)$ and verifies whether MAC_i and MAC_i' are equal. If they are equal, the validity of RSU_i is verified and authentication continues. Otherwise, authentication is terminated. Then, 5GC verifies the validity of vehicle timestamp T_j. If it is equal, it calculates $A_{j_2}' = T_{s_{TA}}(A_{j_1})$, $(VID_j \| y_j \| MAC_j) = H_1(A_{j_2}' \| T_j \| PID_j) \oplus A_{j_3}$ to get VID_j, y_j, MAC_j, and then 5GC looks for the database to find the VID_j. If it finds the VID_j, then proceed to the next steps; otherwise, the authentication is terminated. 5GC calculates $MAC_j' = H_2(VID_j \| A_{j_2}' \| A_{j_1} \| PID_j \| T_j)$, and verifies whether MAC_j' and MAC_j are equal. If they are equal, the validity of the vehicle is verified, and the certification continues. 5GC reselects $n_j^{new}, e_i^{new} \in Z_q^*$, calculates $PID_j^{new} = H_1(VID_j \| s_{TA} \| n_j^{new})$ and updates database $\{EID_i, e_i^{new}\}$. 5GC selects current timestamp T_{TA} and the random values $g_j, v_i \in Z_q^*$, and calculates $F_{j_1} = T_{g_j}(x)$, $F_{j_2} = T_{g_j}(A_{j_1}), F_{j_3} = PID_j^{new} \oplus H_1(F_{j_2} \| VID_j \| T_{TA})$, $F_{i_1} = T_{e_i}(x), F_{i_2} = T_{v_i}(x)$, $F_{i_3} = T_{v_i}(F_{i_1}), F_{i_4} = e_i^{new} \oplus H_1(F_{i_3} \| e_i \| T_{TA})$, $F_{i_5} = H_1(GID_i \| e_i \| e_i^{new} \| F_{i_3} \| EID_i \| T_{TA})$. 5GC selects group key $MK \in Z_q^*$ for vehicle group and a random number $R \in Z_q^*$, calculates $MAC_{TA} = H_1(PID_j \| PID_j^{new} \| A_{j_2}' \| VID_j \| F_{j_2} \| T_{TA}), P_j = (MK \| MAC_{TA}) \oplus H_1(A_{j_2}' \| VID_j \| T_{TA})$, $Y = \prod_{j=1}^{n} y_j, Y_j = Y/y_j, Y_j t_j \equiv 1 (\mod y_j)$, and obtains $S = \sum_{j=1}^{n} P_j t_j Y_j \bmod Y$ through Chinese remainder theorem. Finally, 5GC calculates the certification confirmation value $CCV_j = H_2(VID_j \| MK)$ and gets the group authentication confirmation value $CCVS = \oplus_{j=1}^{n} CCV_j$, and hashes it to get $HCCVS = H_1(CCVS \| R)$. Then, 5GC sends the message

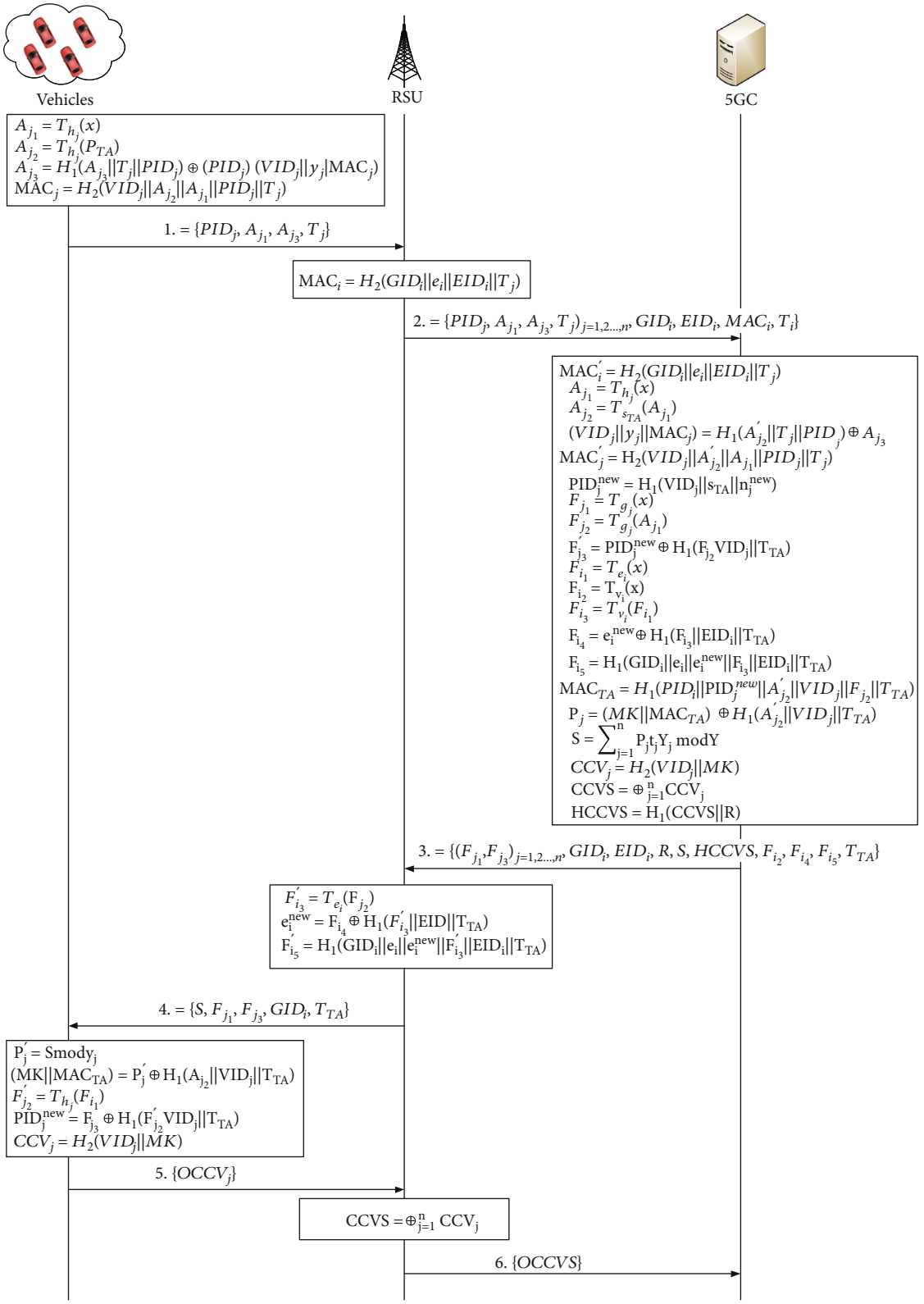

Figure 2: Authentication process of the proposed protocol.

$\{-(F_{j_1}, F_{j_3})_{j=1,2\cdots,n}, \mathrm{GID}_i, \mathrm{EID}_i, R, S, \mathrm{HCCVS}, F_{i_2}, F_{i_4}, F_{i_5}, T_{TA}\}$.

(5) After receiving the message sent by 5GC, RSU_i first verifies whether the timestamp T_{TA} is within the legal range. If the timestamp is valid, RSU_i calculates $F'_{i_3} = T_{e_i}(F_{i_2})$, gets $e_i^{\mathrm{new}} = F_{i_4} \oplus H_1(F'_{i_3} \| e_i \| T_{TA})$, and calculates $F'_{i_5} = H_1(\mathrm{GID}_i \| e_i \| e_i^{\mathrm{new}} \| F'_{i_3} \| \mathrm{EID}_i \| T_{TA})$. Then, it verifies whether F'_{i_5} and F_{i_5} are equal. If they are equal, it uses e_i^{new} to update the secret value e_i. At the same time, RSU_i extracts the HCCVS, R and saves them to the database. Finally, the message $\{\mathrm{GID}_i, S, F_{j_1}, F_{j_3}, T_{TA}\}$ is forwarded to the corresponding vehicle

(6) When the corresponding message is received in the group vehicles, the OBU_j first verifies whether the timestamp T_{TA} is the legal. If the timestamp is valid, it calculates $P'_j = S \bmod y_j$, $(MK \| \mathrm{MAC}_{TA}) = P'_j \oplus H_1(A_{j_2} \| \mathrm{VID}_j \| T_{TA})$ and obtains the vehicle group key MK and MAC_{TA}.Then, OBU_j calculates $F'_{j_2} = T_{h_j}(\mathrm{F}_{i_1})$, $\mathrm{PID}_j^{\mathrm{new}} = F_{j_3} \oplus H_1(F'_{j_2} \| \mathrm{VID}_j \| T_{TA})$, $\mathrm{MAC}'_{TA} = H_1(\mathrm{PID}_j \| \mathrm{PID}_j^{\mathrm{new}} \| A_{j_2} \| \mathrm{VID}_j \| F'_{j_2} \| T_{TA})$. OBU_j verifies whether MAC'_{TA} and MAC_{TA} are equal. If they are equal, OBU_j certifies 5GC. At this time, it can know that OBU_j gets the group key MK and updates $\mathrm{PID}_j^{\mathrm{new}}$. OBU_j calculates $\mathrm{OCCV}_j = H_2(\mathrm{VID}_j \| MK)$ and sends the message $\{\mathrm{OCCV}_j\}$ to RSU_i

(7) When RSU_i receives the messages from the group vehicles, it calculates $\mathrm{OCCVS} = \oplus_{j=1}^{n} \mathrm{OCCV}_j$, $\mathrm{HCCVS} = H_1(\mathrm{OCCVS} \| R)$. And it verifies whether it is equal to the stored value HCCVS. If they are equal, it means that the group vehicles have been approved. Then, RSU sends OCCVS to 5GC and at the same time sends a successful authentication notification message to vehicular members

(8) After 5GC receives the sent message, it verifies whether OCCVS and CCVS are equal. If they are equal, the group members are successfully authenticated

5. Security Evaluation

5.1. Formal Verification with Scyther Tool. Here, we use the Scyther tool to verify our protocol, which is a formal verification tool for security protocols [52]. There are many models in the Scyther, such as standard Dolev-Yao model, CK model, and eCK model. By using the Scyther to model our protocol, the Scyther can effectively discover potential security issues. The tool evaluates the confidentiality and authenticity of protocol information by writing protocol roles. Moreover, the tool provides a friendly graphical user interface, which is convenient to analyze and verify the complex attack scenarios on the target protocol. Authentication statement in Scyther is as follows: Alive, Weakagree, Niagre, and Nisynch are used to detect malicious attacks such as replay attacks, reflection attacks, and man-in-the-middle attacks [53].

In this scheme, there are four roles: GV, RSU, 5GC, and TA. Since the protocol proposed in this paper is secure in the registration phase, we only consider the security in the access authentication phase. In the process of verification, we choose Dolev–Yao model to test, because attackers can carry out related attacks by controlling the network in this model. The simulation results based on Scyther are shown in Figure 3. It can be concluded from the results that our scheme successfully meets all the requirements of the Scyther confidentiality and authentication and resists attacks.

5.2. Security Analysis. According to the safety requirements given in the previous chapter, the following safety analysis is given.

(1) Anonymity: this is an important aspect of vehicle privacy protection. In our proposed scheme, vehicles have communicated through the use of pseudonym $\mathrm{PID}_j = H_1(\mathrm{VID}_j \| s_{TA} \| n_j)$. And in the communication process, we hide the real identity in $A_{j_3} = H_1(A_{j_2} \| T_j \| \mathrm{PID}_j) \oplus (\mathrm{VID}_j \| y_j \| \mathrm{MAC}_j)$, and only by using the secret value s_{TA} can restore the real identity of the vehicle. Therefore, the anonymity of the vehicle can be guaranteed

(2) Message authentication and integrity: the communication entities in the scheme verify each other's legitimacy by verifying the message authentication code, so the scheme can provide message authentication. Since the generation of the message authentication code is based on the extended Chebyshev polynomial DH problem, the message authentication code is secure. Therefore, the integrity of the message can be verified

(3) Traceability: once a message is disputed, according to the report message sent by the malicious vehicle and the pseudoidentity, TA can trace back the true identity of the malicious vehicle by calculating $(\mathrm{VID}_j \| y_j \| \mathrm{MAC}_j) = H_1(\mathrm{A}'_{j_2} \| T_j \| \mathrm{PID}_j) \oplus A_{j_3}$

(4) Unlinkability: because the scheme uses random numbers and timestamps, the messages transmitted over the network are different. In addition, since the pseudoidentity of the vehicle is dynamically updated, the attacker cannot confirm that they are from the same sender.

(5) Resistance to common attacks: the proposed scheme should be able to resist the following common types of attacks:

(a) Resistance replay attack: since a timestamp is attached to the message, by checking the validity

Figure 3: Scyther result.

Table 2: Security features comparison.

Functionality	[24]	[29]	[13]	[30]	[35]	[36]	[31]	Our scheme
Anonymous	Yes	No	No	Yes	Yes	Yes	Yes	Yes
Mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Traceability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Unlinkability	Yes	Yes	No	No	Yes	Yes	No	Yes
Replay attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Man-in-the-middle attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Counterfeit attack	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Batch certification	No	Yes	Yes	Yes	No	No	No	Yes

of the timestamp, the entities participating in the authentication can find out whether message replay has occurred

(b) Resistance modification attack: in our proposed scheme, the message authentication code is calculated by the secret value held by the corresponding entity. And the secret value is updated dynamically. Therefore, the entity can verify whether the message has been modified

(c) Resistance man-in-the-middle attack: according to the analysis of the previous message authentication and modification attacks, once an attacker intercepts and maliciously changes the message in transmission, the entity verifies that the message authentication code in the message cannot be passed. This can be quickly found that the transmission content has been changed

(d) Resist counterfeit attacks: in order to disguise a legitimate vehicle to send a request message, the adversary needs to send correct $A_{j_3} = H_1($ $A_{j_2} \| T_j \| \mathrm{PID}_j) \oplus (\mathrm{VID}_j \| y_j \| \mathrm{MAC}_j)$ and $\mathrm{MAC}_j = H_2(\mathrm{VID}_j \| A_{j_2} \| A_{j_1} \| \mathrm{PID}_j \| T_j)$. As analyzed above, it is impossible to extract the true identity of the vehicle from the intercepted

Table 3: Computation overhead.

Protocol	Total computation overhead	Total execution time
[33]	$8nT_{ECC} + 25nT_H + 2nT_{DE}$	$0.546093n$
[13]	$12nT_{CCM} + 14nT_H + 2nT_{DE}$	$0.28025n$
[30]	$9nT_{ECC} + 13nT_H + 4T_{ECC} + 7T_H$	$0.582657n + 0.259571$
[31]	$4nT_{ECC} + 14nT_H$	$0.263078n$
Our scheme	$6nT_{CCM} + 13nT_H + 4T_{CCM} + 8T_H$	$0.132411n + 0.08794$

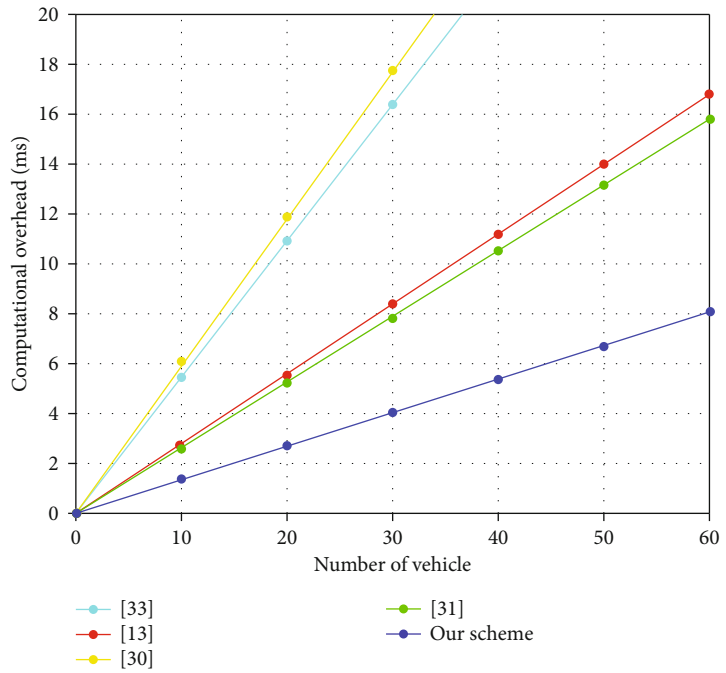

Figure 4: Computation overhead between different protocols.

Table 4: Communication overhead.

Protocol	Communication overhead
[33]	$2176n$
[13]	$2688n$
[30]	$2272n + 704$
[31]	$2816n + 1024$
Our scheme	$1760n + 1472$

message. Therefore, the scheme in this article can resist this type of attack

5.3. Security Comparison. Through the previous safety analysis, we show the comparison results with other schemes in Table 2. Comparison of the results in the table show that our scheme has better security performance.

6. Performance Analysis

By computation overhead and communication overhead, we evaluate the performance of the scheme. Here, we will mainly compare the performance of some schemes similar to our proposed scheme, so our main comparison schemes are [13, 30, 31, 33]. Here, n represents the number of vehicles in the group.

6.1. Computation Overhead. In terms of computation overhead, we evaluated the proposed scheme on a laptop. We tested the calculation time of ECC-based scalar multiplication T_{ECC}, hash operation T_H, and Chebyshev mapping operation T_{CCM}, as well as calculation time based on symmetric encryption and decryption T_{DE}. Here, we only calculate some important operations and no longer calculate negligible operations, such as XOR operations. The results of our test are $T_{ECC} = 0.064016$ ms, $T_H = 0.000501$ ms, $T_{CCM} = 0.020983$ ms, $T_{DE} = 0.01072$ ms. As shown in Table 3, we have calculated the computation cost of the related schemes.

As can be seen from Figure 4, compared with other schemes, our scheme has the least computation overhead. When the number of vehicles are increasing, the advantage will be more obvious.

6.2. Communication Overhead. Before analyzing related protocols, we first define the size of relevant parameter in the

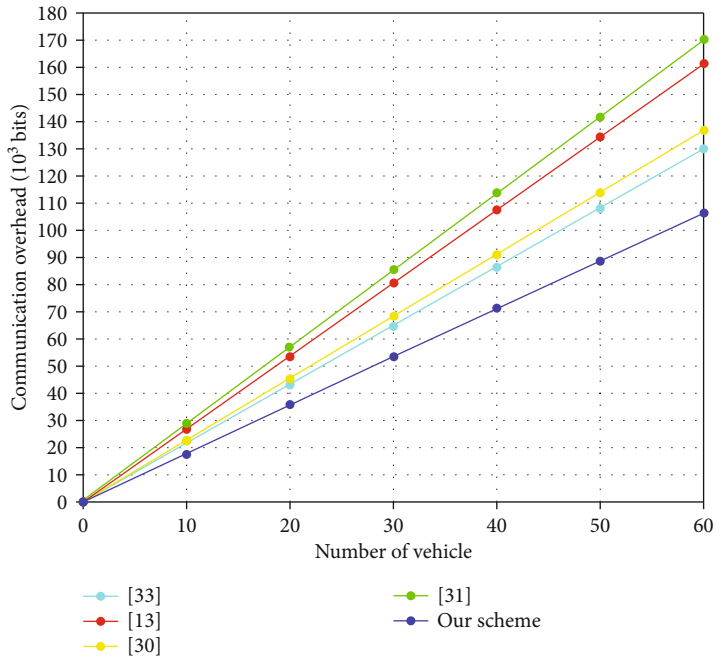

Figure 5: Communication overhead between different protocols.

protocol. Assume that the key size based on the ECC algorithm is 256 bits, the size of Chebyshev chaotic map is 128 bits, the size of hash value is 128 bits, the size of identity information is 128 bits, the size of timestamp is 32 bits, and the size of random number is 128 bits [54]. Calculation of the communication overhead for the above schemes is shown in Table 4.

As can be seen from Figure 5, our scheme has obvious advantages in communication overhead by comparing with other schemes [30].

7. Conclusion

As the communication among vehicle groups involves the problems of low delay, safety, and efficiency in the 5G-enabled vehicular networks, we propose a lightweight and secure vehicle group authentication protocol. The scheme is based on the extended chaotic mapping algorithm to achieve authentication, and the group key is distributed through the Chinese remainder theorem, so that the vehicle groups will communicate through the group key. In order to protect the security of RSU, the shared key will be updated. In addition, the security of the scheme is verified by the Scyther tool, and the verification results show that the security of the protocol can be guaranteed. And through the security analysis, the scheme can not only effectively resist all kinds of attacks but also ensure the anonymity, unlinkability, and other security requirements. Finally, by comparing the computation overhead and communication overhead with related schemes, our scheme has less overhead. In the future research work, we will start to study the group management scheme based on aggregation authentication. With the development of 5G communication technology, an efficient scheme is designed to meet the needs of security and privacy.

Data Availability

The data used to support the findings of this study are included within this article.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the 2020 Industrial Technology Foundation Public Service Platform Project (grant number 2020-0105-2-1).

References

[1] G. Dimitrakopoulos and P. Demestichas, "Intelligent transportation systems," *IEEE Vehicular Technology Magazine*, vol. 5, no. 1, pp. 77–84, 2010.

[2] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (V2X) testing," *Sensors*, vol. 19, no. 2, p. 334, 2019.

[3] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[4] S. Zhang, N. Zhang, X. Fang, P. Yang, and X. S. Shen, "Self-sustaining caching stations: Toward cost-effective 5g-enabled vehicular networks," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 202–208, 2017.

[5] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: the next generation of mobile communication," *Physical Communication*, vol. 18, pp. 64–84, 2016.

[6] A. Osseiran, F. Boccardi, V. Braun et al., "Scenarios for 5G mobile and wireless communications: the vision of the METIS project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, 2014.

[7] J. Saqlain, *IoT and 5G: History Evolution and Its Architecture Their Compatibility and Future, [Ph.D. Thesis]*, Subtitle Metropolia University of Applied Sciences, 2018.

[8] S. A. Abdel Hakeem, A. A. Hady, and H. W. Kim, "5G-V2X: standardization, architecture, use cases, network-slicing, and edge-computing," *Wireless Networks*, vol. 26, no. 8, pp. 6015–6041, 2020.

[9] Z. Lin, X. Du, H. H. Chen, B. Ai, Z. Chen, and D. Wu, "Millimeter-wave propagation modeling and measurements for 5G mobile networks," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 72–77, 2019.

[10] I. Rasheed, F. Hu, Y. K. Hong, and B. Balasubramanian, "Intelligent vehicle network routing with adaptive 3D beam alignment for mmwave 5G-based V2X communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 2706–2718, 2021.

[11] N. Zhang, S. Zhang, P. Yang, O. Alhussein, W. Zhuang, and X. S. Shen, "Software defined space-air-ground integrated vehicular networks: challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 7, pp. 101–109, 2017.

[12] O. Yilmaz and N. Johansson, "5G radio access for ultra-reliable and low-latency communications," *Ericsson Research Blog*, vol. 1, pp. 1184–1189, 2015.

[13] 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 Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8914–8924, 2020.

[14] C. Wang, D. Wang, G. Xu, and D. He, *Efficient Privacy-Preserving User Authentication Scheme with Forward Secrecy for Industry 4.0*, Science China: Information Sciences, 2020.

[15] Z. Li, D. Wang, and E. Morais, "Quantum-safe round-optimal password authentication for mobile devices," *IEEE Transactions on Dependable and Secure Computing*, 2020.

[16] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, 2019.

[17] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2020.

[18] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 248–262, 2011.

[19] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: a secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10283–10295, 2017.

[20] P. Vijayakumar, V. Chang, L. Jegatha Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generations Computer Systems*, vol. 78, Part 3, pp. 943–955, 2018.

[21] M. Han, L. Hua, and S. Ma, "A self-authentication and deniable efficient group key agreement protocol for VANET," *Ksii Transactions on Internet & Information Systems*, vol. 11, no. 7, pp. 3678–3698, 2016.

[22] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2016.

[23] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Computing*, vol. 20, no. 3, pp. 2439–2450, 2017.

[24] J. Cui, X. Tao, J. Zhang, Y. Xu, and H. Zhong, "HCPA-GKA: a hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs," *Vehicular Communications*, vol. 14, pp. 15–25, 2018.

[25] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2021.

[26] C. Lai, D. Zheng, Q. Zhao, and X. Jiang, "SEGM: a secure group management framework in integrated VANET-cellular networks," *Vehicular Communications*, vol. 11, pp. 33–45, 2018.

[27] Q. Zhang, X. Wang, J. Yuan et al., "A hierarchical group key agreement protocol using orientable attributes for cloud computing," *Information Sciences*, vol. 480, pp. 55–69, 2019.

[28] A. Shi, B. Mso, C. Pv et al., "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.

[29] I. Gharsallah, S. Smaoui, and F. Zarai, "An efficient authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks," *IET Information Security*, vol. 14, no. 1, pp. 21–29, 2020.

[30] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, "Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7940–7954, 2020.

[31] M. Ouaissa, M. Houmer, and M. Ouaissa, "An enhanced authentication protocol based group for vehicular communications over 5G networks," in *2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*, pp. 1–8, Marrakech, Morocco, 2020.

[32] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[33] J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "SMAKA: secure many-to-many authentication and key agreement scheme for vehicular networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1810–1824, 2021.

[34] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "RSMA: reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6417–6428, 2019.

[35] J. Huang, Y. Qian, and R. Q. Hu, "Secure and efficient privacy-preserving authentication scheme for 5G software defined vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8542–8554, 2020.

[36] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for VANETs," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, 2020.

[37] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar, "A novel lightweight authentication protocol for emergency vehicle avoidance in VANETs," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[38] 3rd Generation Partnership Project and Technical Specification Group Services and System Aspects, "System Architecture for the 5G System (Release 16)," in *3GPP Standard TS 33.501,V16.4.0*, pp. 18–46, 3rd Generation Partnership Project (3GPP), 2020.

[39] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.

[40] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, "Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11309–11322, 2019.

[41] O. Mir, T. Weide, and C. C. Lee, "A secure user anonymity and authentication scheme using AVISPA for telecare medical information systems," *Journal of Medical Systems*, vol. 39, no. 9, p. 265, 2015.

[42] C. T. Li, C. C. Lee, C. Y. Weng, and S. J. Chen, "A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems," *Journal of Medical Systems*, vol. 40, no. 11, article 233, 2016.

[43] M. S. Hwang, C. C. Lee, and Y. C. Lai, "Traceability on low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E85-A, no. 5, pp. 1181-1182, 2002.

[44] H.-A. Wen, K.-C. Lee, S.-Y. Hwang, and T. Hwang, "On the traceability on RSA-based partially signature with low computation," *Applied Mathematics and Computation*, vol. 162, no. 1, pp. 421–425, 2005.

[45] C. C. Lee, M. S. Hwang, and W. P. Yang, "A new blind signature based on the discrete logarithm problem for untraceability," *Applied Mathematics & Computation*, vol. 164, no. 3, pp. 837–841, 2005.

[46] P. Bergamo, P. D'Arco, A. de Santis, and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 52, no. 7, pp. 1382–1393, 2005.

[47] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos, Solitons &Fractals*, vol. 37, no. 3, pp. 669–674, 2008.

[48] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2020.

[49] T. T. K. Hue, T. M. Hoang, and A. Braeken, "Lightweight signcryption scheme based on discrete Chebyshev maps," in *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 43–47, Cambridge, UK, 2017.

[50] Y. Ren, V. Oleshchuk, and F. Y. Li, "An efficient Chinese remainder theorem based node capture resilience scheme for mobile WSNs," in *2010 IEEE International Conference on Information Theory and Information Security*, pp. 689–692, Beijing, China, 2010.

[51] P. Vijayakumar, S. Bose, and A. Kannan, "Chinese remainder theorem based centralised group key management for secure multicast communication," *Information Security*, vol. 8, no. 3, pp. 179–187, 2014.

[52] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu, and H. Li, "LSAA: a lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5329–5344, 2020.

[53] C. Cremers, *The Scyther Tool*, CISPA Helmholtz Center for Information Security, 2020, https://people.cispa.io/cas.cremers/scyther/.

[54] Y. Sun, J. Cao, M. Ma et al., "EAP-DDBA: efficient anonymity proximity device discovery and batch authentication mechanism for massive D2D communication devices in 3GPP 5G HetNet," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2020.