








Research Article

TFPPASV: A Three-Factor Privacy Preserving Authentication Scheme for VANETs

Zongtao Duan ¹, Jabar Mahmood ¹, Yun Yang ¹, Michael Abebe Berwo ¹,
Abd al Kader Ahmed Yassin ², Muhammad Nasir Mumtaz Bhutta ³,
and Shehzad Ashraf Chaudhry ^{3,4}

¹School of Information and Engineering, Chang'an University, Xi'an 710064, China

²Hatay Mustafa Kemal University (MKU) Turkish-Hatay/Hassa-MYO Girne, 79 Sokak, Hassa 31700, Turkey

³Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, UAE

⁴Department of Computer Engineering, Faculty of Engineering and Architecture, Nisantasi University, Istanbul 34398, Turkey

Correspondence should be addressed to Yun Yang; yangyun@chd.edu.cn

Received 25 May 2022; Revised 6 August 2022; Accepted 12 August 2022; Published 30 September 2022

Academic Editor: AnMin Fu

Copyright © 2022 Zongtao Duan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

A vehicular ad hoc network (VANET) is essential for the autonomous vehicle industry, and with the advancement in VANET technology, security threats are increasing rapidly. Mitigation of these threats needs an intelligent security protocol that provides unbreakable security. In recent times, various three-factor authentication solutions for VANET were introduced that adopt the centralized Trusted Authority (TA), which is responsible for assigning authentication parameters during vehicle registration, and the authentication process depends on these parameters. This article first explains the vulnerabilities of the recent three-factor (3F) authentication scheme presented by Xu et al. Our analysis proves that if an RSU is dishonest, it can easily bypass the TA and can create a session with OBU. Furthermore, this paper puts forward a new scheme that provides the 3F authentication for VANETs (TFPPASV) to resist RSU from bypassing the TA and to offer user privacy. The proposed scheme fulfills the security and performance requirements of the VANET. We use BAN-Logic analysis to perform a formal security analysis of the proposed scheme, in addition to the informal security feature discussion. Finally, we compare the security and performance of the proposed TFPPASV with some recent and related schemes.

1. Introduction

Due to its dynamic structure and related advantages including the realization of autonomous cars, increased road safety, congestion avoidance, and so on, the vehicular ad hoc networks (VANETs) are getting more popularity and are being considered as the only vehicular network structure of the future. In recent years, the road travel safety is also being considered as most important factor for transportation industry and accordingly several technologies are being developed. A general model of vehicular ad hoc network (VANET) [1–3] is given in Figure 1. VANET is a subbranch of MANETs; intelligent transportation system (ITS) [4] provides support to manage transportation efficiently on

roads. VANET consists of three parts [5]. (i) On-board unit (OBU) [6]: OBU is installed inside the vehicle at the time of manufacture from the company side. The OBU stores the information related to vehicle identity, vehicle password, and other parameters necessary for registration and communication; without this confidential information, the vehicle cannot communicate to other OBUs or road side unit (RSU) [2]. OBU communicates to other OBUs or RSUs on the road using the dedicated short range communication (DSRC) protocol [7–9]. (ii) RSU is fixed alongside the road; RSU has more computational and communication power than OBU. RSU provides the facilities to OBUs to communicate with other OBUs or to communicate with RSU via DSRC. In addition, OBU wants to communicate with

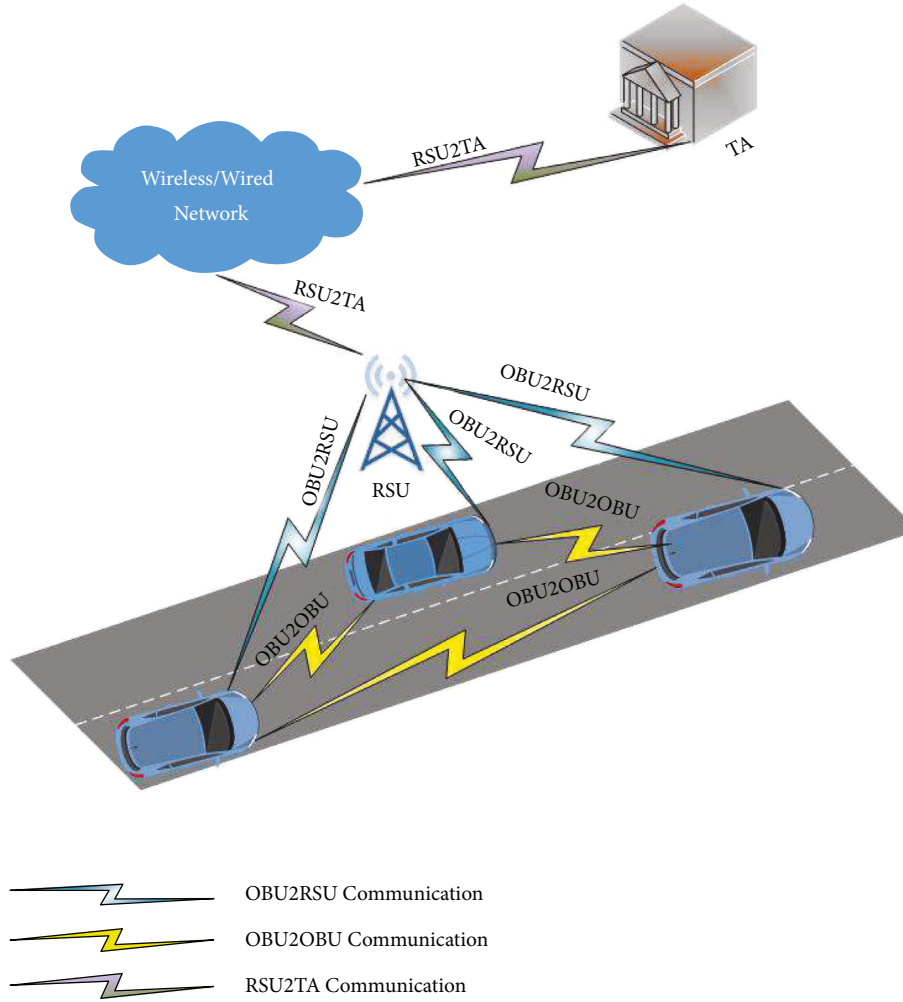


FIGURE 1: General model of VANETs.

Trusted Authority (TA) [2]. RSU acts as a mediator between OBU and TA , where the communication among RSU and TA is carried over some wired or wireless channel. (iii) TA provides authentication parameters to facilitate communication among various entities in a VANET. TA is responsible for completing all node authentication. VANETs provide more comfortable and reliable facilities to passengers and drivers on the road, such as infotainment, weather conditions, location information, traffic congestion, and so on. These services aim to provide a safe drive and secure human life on the road and proper energy resource utilization. Due to VANET's openness characteristics, many security threats are faced during communication. Avoiding these security threats needs a secure authentication scheme that provides resilience against all such threats.

1.1. Motivation. In recent past, many researchers proposed various authentication schemes for VANETs, but many of these schemes do not fulfill the security requirements and are having insecurities against various threats. In addition, some of these schemes have high computational and communication costs. Due to these limitations, we propose a

three-factor authentication scheme and key agreement for VANETs. In our scheme, RSU and TA perform authentication processes. RSU reduces the TA computational and communication cost and performs the authentication. In the proposed scheme, TA hands over a smart card (SC) to each registering vehicle. Inside the SC, TA stores confidential information such as the biological information of the vehicle to provide better security. The proposed scheme provides the facilities to identify malicious vehicle in a multi-drive environment.

1.2. Contributions. The contributions of this study are as follows:

- (1) Firstly, we reviewed and revealed that Xu et al.'s authentication scheme for IoV is insecure against TA bypassing attack. Additionally, an improved scheme titled "TFPPASV: A Three-Factor Privacy Preserving Authentication Scheme for VANETs" is proposed.
- (2) Secondly, the security of the proposed TFPPASV scheme is proved using BAN-Logic in addition to the

informal discussion on critical security feature provision of the proposed TFPPASV scheme.

- (3) We also provided a comparative security and performance analysis of the proposed TFPPASV with some related and recent authentication schemes.

1.3. Organization. The remaining structure of the paper is organized as follows. Section 2 describes the preliminaries such as elliptic curve cryptography, fuzzy extractor, network model, and attack model. Section 3 provides the summary of the related work, and Section 4 details the previously published Xu et al.'s scheme [10]. Section 5 summarizes the weaknesses of Xu et al.'s scheme. In Section 6, the proposed TFPPASV is explained briefly. Section 7 analyzes the BAN-Logic-based security proof of the proposed TFPPASV, in addition to the security feature discussion under various attacks. In Section 8, we conduct security and performance comparisons with related schemes. Finally, a conclusion is provided in Section 9.

2. Preliminaries

This section describes the elliptic curve cryptography (ECC), fuzzy extraction, network model, and attack model used in the proposed TFPPASV. Moreover, Table 1 provides the notation used in this paper.

2.1. Elliptic Curve Cryptography. The concept of elliptic curve cryptography (ECC) was presented by Miller and Koblitz in 1985 [11]. ECC is an asymmetric cryptography technique and the following are details related to ECC.

Characteristics of ECC:

- (i) In ECC, the key generation time is faster than other cryptographic techniques.
- (ii) The size of the ECC key is small and provides the same security, for example, RSA key size is 1024-bit and ECC key size is 160-bit.

Currently, ECC is used in various authentication schemes, devices, and applications such as VANETs, wireless sensor networks, mobiles, RFID devices, bitcoin, and safe web browsers through SSL/TLS due to its small key size. In this paper, we also used the ECC for a secure scheme. Here, we describe the basics of ECC.

The ECC equation $E: y^2 = x^3 + ix + j \pmod{p}$ is used to describe the mathematical operations, where $i, j \in \mathbb{Z}_p^*$ and $4i^3 + 27j^2 \pmod{p} \neq 0$ such that p is a large prime number ($|P| \geq 2^{160}$). Here, we discuss two computationally intensive problems along with a trapdoor function (TF) role in ECC.

- (i) TF is defined as a function that is a one-way function easy to compute in one direction but if computing in the reverse direction is computationally difficult, every public key cryptography has its TF.
- (ii) Elliptic curve discrete logarithm problem (ECDLP): Let $U = kV$ and $k < n$, if V and k are known, U can be computed easily, whereas, it is computationally

difficult to compute k such that $k \in \mathbb{Z}_p^*$, if U and V are known.

- (iii) Elliptic curve computational Diffie–Hellman problem (ECCDHP): let $U = aP$ and $V = bP$ be two points on E and $\{a, b\} \in \mathbb{Z}_p^*$. It is computationally hard to calculate the $W = abP$ point, provided that a, b are unknown.

2.2. Fuzzy Extractor. Authentication through complex passwords is not a better idea for secure registration on an insecure channel. A good technique for secure registration is biometric template, for example, heartbeat, fingerprint, and iris templates are usually used for authentication.

The characteristics of the biometric key are given below:

- (i) Biometric keys are unique and these are not easy to replicate.
- (ii) No need to store or memorize because it comes from the user's body.
- (iii) No duplicate keys are generated.
- (iv) Cannot be estimated or guessed.
- (v) Challenging to reprint and distribute.

Biometrics using raw data are not safe, and thus the biometric data must be stored safely in the system. Various security methods are developed to save the biometric information, such as fuzzy extractor and bio-hash function. They mostly used the fuzzy extractor because the bio-hash function faces the denial of service attack.

The fuzzy extractor has been widely used in an authentication scheme for extracting the biometric key.

The fuzzy extractor has two processes with the following parameters (W, l, t) where W is the input string.

- (i) $\text{Gen}(\cdot)$ is a probability generation procedure. In this procedure, input W is the biometric information from the user, α is a random secret key of the length of l , and β is a public string extracted from the input W , and (1) describes the procedure of generation key.

$$\text{Gen}(W) = (\alpha, \beta). \quad (1)$$

- (ii) $\text{Rep}(\cdot)$ is the process of reproduction and in this procedure, and R can be retrieved as per biometric information W' close to W and β . (2) describes the procedure of reproduction key. For all W, W' , if $d(W, W') \geq t$, there is (2) under precondition (1), where $d(W, W') \geq t$ represent the distance between W and W' which should not be greater than l .

$$\alpha = \text{Rep}(W', \beta). \quad (2)$$

Here, we define the fuzzy extractor.

- (iii) In (3), there is a high probability that the distance between two biometric values W and W' generated from the same entity is low, which can be described as

TABLE 1: List of notations.

Notations	Description of notations
TA, OBU	Trusted authority, on-board unit
RSU	Road side unit
$V2V, V2I$	Vehicle to vehicle, vehicle to infrastructure
IoV	Internet of vehicle
x	RSU and TA private key
P_{pub}	TA public key
A	An adversary
TPD	Temper proof device
W_i	Biometric Information of U_i
α	The random biometric secret key of U_i
β	The public reproduction parameter of U_i
G	An elliptic curve cycle additive group
P	A generator of G
P	Order of G
SC	Smart card
U_i	i_i h users
t_0, t_1, t_2	Timestamp
y_i, r, k	Random number
ID_i	The identity of vehicle/user (U_i)
PW_i	The password of vehicle/user (U_i)
A_i, C_i, D_i, E_i	TA -generated U_i parameters
$h(.)$	One-way cryptography hash function
\oplus	XOR operation

$$P_r[\text{dis}(W, W') < t] \geq 1 - \epsilon_{f_n}, \quad (3)$$

where t is the predetermined tolerance threshold and “false negative” probability is ϵ_{f_n} .

- (iv) There is a high probability that the distance between two biometric values, W_1, W_2 , for two entities is high, which is described in the following equation:

$$P_r[\text{dis}(W, W') < t] \geq 1 - \epsilon_{f_n}, \quad (4)$$

where $t' < t$ and ϵ_{f_p} is the probability of “false positive.”

2.3. Network Model. The network model of the proposed security scheme is presented in Figure 2.

TA: TA is an autonomous or fully trusted entity in VANET responsible for system initialization and registration of a vehicle or a user. TA has more resources in the shape of communication and computational cost. It knows about all RSUs’ locations and identities. It issues the parameters to the nodes in VANET and transmits via a secure channel to each node.

RSU: RSU is fixed alongside the road and is equipped with temper proof device (TPD). TPD is responsible for storing data and performing encryption operations on data. RSU communicates with TA via wired or wireless channels and OBU via DSCR protocol. RSU holds information about all registered vehicles in the range of RSU. In addition, RSU shares information with authenticated vehicles via a session key created during authentication.

OBU: each vehicle has its OBU device fixed inside it and stores all confidential information integral for OBU to prove

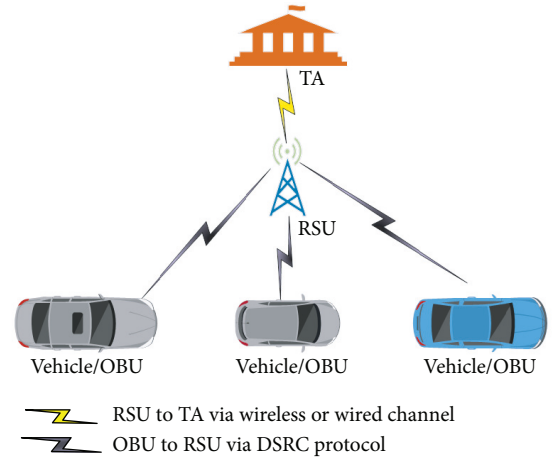


FIGURE 2: Proposed scheme network model.

its authenticity. OBU links to RSU via DSRC protocol. Before communication, OBU proves their authenticity; if OBU proves that it is authenticated, then it communicates with RSU; otherwise, it stops the session key generation.

2.4. Attack Model. In this paper, we consider the common DY adversarial model with following description:

- (1) An adversary (A) plays the role of an eavesdropper, who easily eavesdrops on the insecure communication link and can modify/change or replay the message or send a new message on the link. A can also stop/remove a message from the communication link.

- (2) If A gets the vehicle smart card (SC), he can quickly get all the confidential information stored in SC.
- (3) TA is assumed to be secure. Precisely, except the private key of the TA , rest of the parameters stored on TA could be exposed to A .
- (4) TPD is an important temper proof device because the authenticated data of RSU are stored inside the TPD. Suppose E captures the TPD; it cannot extract the data from the TPD.

3. Related Work

Due to dynamicity of VANETs environment, communication process deviates from other networks. VANET communication in smart cities faces various security threats such as eavesdropping, tracking, and positioning. Security and anonymity provisions are required to avoid these issues. Zheng et al. [12] proposed a VANETs authentication scheme for smart cities. Zhang et al.'s scheme uses certificateless group signature and the Elliptic curve scalar multiplication operations. Zheng et al. [12] proved that overhead cost of their scheme is less than Chen et al.'s [13] and Zhao et al.'s [14] schemes. However, they failed to provide the security analysis of the proposed scheme.

Two-factor security authentication protocols in VANETs are mainly accepted and used for authentication between $V2V$ and $V2I$ on the insecure communication channel. In recent years, various two-factor authentication schemes were proposed, but most of these schemes are vulnerable to one or more weaknesses including SC loss, impersonation assaults, and offline password guessing assaults. Qu and Tan. [15] proposed a password based remote user authentication with key agreement scheme using ECC. Qu and Tan [15] proved that their proposed scheme provides security against various known security threats, but they did not provide the communication cost, running time, and overhead cost of their scheme.

Nandy et al. [16] proposed an authentication scheme using ECC. Nandy et al. [16] proved through security analysis that the proposed scheme provides security against several VANET security attacks. Nevertheless, Chaudhry [17] proved that the ECC techniques used by Nandy et al. involve a faulty operation and their scheme cannot compute the private key of the vehicles. Therefore, their scheme cannot complete the authentication process in their described manner.

Chuang and Lee [18] proposed a security scheme called TEAM in 2013 for $V2V$ secure communication. In TEAM, TA is only for initialization and vehicle registration, which reduces the computational cost of TA . However, Zhou et al. [19] in 2017 highlighted the weakness of the Chuang and Lee's scheme [18] and proved that it cannot perform against inside assaults such as impersonation assaults. Thus, Zhou et al. [19] proposed an authentication scheme that removes the weakness of Chuang and Lee's scheme [18]. In 2019, Wu et al. [20] revealed the weakness of Zhou et al.'s scheme [19]

and proved that it cannot perform against impersonation assault, identity guessing assault, and vehicle anonymity. Wu et al. [20] proposed a scheme for $V2V$ secure communication through mutual authentication.

In 2020, Vasudev et al. [21] proposed a security scheme related to mutual authentication between $V2V$ of IoV and proved that it worked against various VANET attacks through informal security analysis. However, they did not provide a formal security analysis of the scheme. In 2021, Mahmood et al. [22] highlighted its weakness and proved that it does not work in dense environments if more than one vehicle is registered. Thus, Mahmood et al. [22] proposed a new scheme that removes the weakness of Vasudev et al. [21] and proved it through formal analysis and informal analysis.

The main issue faced in VANETs is the provision of security to the user on the road because the nature of VANETs is different from the other communication networks. Therefore, more focus on the secure and authentication process is mandatory to avoid the VANET threats. In 2016, Jiang et al. [23] proposed a scheme related to WSN and implemented the three-factor authentication mechanism and proved that it works better than other schemes. However, in 2017, Li et al. [24] pointed out the functional and security flaws in Jiang et al.'s [23] scheme and proposed a new scheme for WSN. Li et al. [24] removed the flaws of the Jiang et al.'s scheme and proved through formal and informal security analysis that their proposed scheme provides correctness and incurs less computation and communication cost than other schemes. However, they did not provide the running time of the proposed scheme.

Wang et al. [25] proposed a two-factor authentication scheme for vehicular ad hoc networks. The scheme aims to provide lightweight authentication and parallel security against various security threats such as denial of service attacks that cause traffic jamming. Wang et al.'s [25] scheme provides biometric security to vehicles; thus, adversaries cannot track and trace the vehicle's location and identity. However, the authors [25] did not provide a formal security analysis of the scheme.

In 2010, Paruchuri and Durresi [26] proposed a protocol called PAAVE. In that protocol, the smart card generated a key for authentication between the vehicle and RSU. Paruchuri and Durresi [26] provided security comparison but did not provide formal and informal security analysis.

In 2017, Ying and Nayak [27] proposed lightweight authentication for VANETs; the authors [27] focused on efficiency and anonymity. The proposed protocol reduces 50% computation and communication cost compared to other protocols. The scheme of Ying and Nayak [27] provides password change feature without involvement of TA . In 2019, Chen et al. [28] discovered some weaknesses in Ying and Nayak's scheme and proved that the scheme does not perform securely against location spoofing, offline identity guessing, and replay attack. In addition, it takes more time for authentication; after that, Chen et al. [28] also proposed a protocol to remove these vulnerabilities from the

TABLE 2: Summary of authentication schemes in VANETs.

Authors	Cryptography technique	Advantage	Disadvantage
Zheng et al. [12]	ECC	Less storage cost, suitable for OBU and RSU in sense of less computing and limited storage	Missing formal security analysis
Qu and Tan [15]	ECC	Provides mutual authentication and key agreement, resists against impersonation attack, stolen smart card, inside attack, and sever spoofing attack, provides user anonymity	Missing communication cost, running time, and overhead cost
Nandy et al. [16]	ECC and symmetric key operation-based authentication	Lightweight and provides vehicle to vehicle secure communication	Faulty design
Vasudev et al. [21]	XOR operation, one-way hash functions	Resists against impersonation attack, stolen smart card, offline password guessing, and man-in-the-middle attacks and provides anonymity	Missing formal security analysis
Mahmood et al. [22]	XOR operations, one-way hash functions	Proved that Vasudev et al.'s scheme [21] is incorrect and proposed new scheme for V2V secure communication. Resists against impersonation attack, stolen smart card, offline password guessing, man-in-the-middle attacks, and DOS attack and provides anonymity and untraceability.	—
Li et al. [24]	XOR operation, hash function, biometric authentication	Improves the functional and security flaws of Jiang et al.'s scheme [23], communication and computation cost is less than that of other schemes	Running time of scheme is missing
Wang et al. [25]	Using multiple hashing functions, biological password-based authentication	Reduces the communication, overhead, and computation cost	Formal security analysis is missing
Paruchuri and Durrezi [26]	Smart card-based key generation	Provides anonymous authentication, less space for key storage in smart card	Informal and formal security analysis is missing

scheme presented in [27]. Table 2 provides the bird's eye view of the previous related works such as cryptography techniques, and their advantages and disadvantages are listed in the table.

4. Summary of Xu Et Al.'s Scheme

This section provides a detailed review of Xu et al.'s scheme [10]. The scheme is divided into six phases and three entities are participating in this scheme. First of all, we explain the entities and then phases of the scheme. User U_i or OBU acts as a vehicle or node that wants to communicate with other OBUs or RSUs. The second entity is RSU which plays the role of an intermediate node between U_i and TA . U_i communicates with RSU via DSRC protocol and RSU communicates with TA via a wired or wireless channel. The last entity of this scheme is TA , and it is responsible for user authentication and making sure users have been authenticated. These three entities perform activities in six phases such as (1) system initialization, (2) registration, (3) user login, (4) user authentication, (5) malicious user tacking, and (6) password and biometric key exchange phase.

4.1. System Initialization. In system initialization phase, TA performs the following steps:

- (i) TA selects G , which is a cyclic additive group having order p and $E: y^2 = X^3 + iX + j \pmod p$ where $i, j \in_R Z_p^*$. The TA further generates x as the primary/private key and computes the $P_{pub} = x.P$ as the public key; after generation, the public key is published by

TA . Through secure channel, TA loads the private key x in the RSUs and TPD.

4.2. User Registration. Under this phase, U_i approaches the TA for the completion of the registration process. The following are the steps involved in user registration phase:

- (i) U_i puts W_i (his biometric information) on the reader to get $\{\alpha_i, \beta_i\} = \text{GEN}(W)$ via FE and provides his original identity ID_i and password PW_i to the TA . TA generates $y_i: \{i = 1, 2 \dots n\}$ randomly for each U_i . Moreover, TA computes $PID_i = h(ID_i, y_i)$, $A_i^* = h(ID_i, x) \oplus \alpha_i$, $C_i = h(ID_i, PW_i, \alpha_i) \oplus y_i$, $D_i = h(PW_i, y_i, \alpha_i)$, $E_i = PID_i \oplus A_i$. After that, TA forwards the SC to U_i with engraved information of the tuple $\langle G, p, P, \beta_i, C_i, D_i, h \rangle$ and stores the tuple $\{PID_i, \alpha_i\}$ in a verifier table.

4.3. User Login. For user login, the OBU checks and verifies the legitimacy of users via execution of the following steps:

- (i) User U_i inserts the SC into OBU and enters the ID_i^* and PW_i^* and imprints biometric information W_i^* . The SC extracts $\alpha_i^* = \text{Rep}(W^l, \beta_i)$. The SC computes $y_i^* = C_i \oplus (ID_i^*, PW_i^*, \alpha_i^*)$. The SC verifies $D_i \stackrel{?}{=} h(PW_i^*, y_i^*, \alpha_i^*)$. If the information is true, login is successful. The SC computes $A_i^* = E_i \oplus (ID_i^*, y_i^*)$; after that, user attenuation will start. Otherwise, SC terminates the registration process. If U_i repeatedly enters wrong information and exceeds the threshold value, it will not accept inputs from U_i .

4.4. User Authentication. Under this phase, OBU and RSU perform mutual authentication and produce secret key for data communication through authentication process. Figure 3 describes the whole process of user authentication of Xu et al.'s scheme, and the following steps are involved:

Step 1. OBU \rightarrow RSU : $\{DID_i, M_0, M_1, R_0, t_0\}$.

- (i) OBU generates a random number r and computes $R_0 = rP, R_1 = rP_{pub}$. After that, OBU computes the dynamic identity $DID_i = h(ID_i^*, y_i^*) \oplus h(R_1, t_0)$ and t_0 (timestamp). Now, OBU computes $M_0 = A_i^* \oplus h(R_1, t_0)$ and $M_1 = h(ID_i^*, DID_i, A_i^*, R_1, t_0)$. OBU sends $DID_i, M_0, M_1, R_0, t_0$ to RSU through insecure channel.

Step 2. RSU \rightarrow TA: $\{DID_i, AID_i, t_0\}$.

- (ii) After receiving the message from the OBU, the RSU checks the freshness of t_0 and verifies whether the message has expired or not. If $t_{r1} - t_0 \geq \Delta t$, RSU immediately stops the process; otherwise, continue. RSU computes $R_1 = xR_0$. RSU computes $PID_i^* = DID_i \oplus h(R_1, t_0)$, $A_1^* = M_0 \oplus h(R_1, t_0)$. RSU computes $AID_i = h(DID_i, x) \oplus PID_i^*$. Now, RSU sends the message $\{DID_i, AID_i, t_0\}$ to the TA.

Step 3. TA \rightarrow RSU: $\{BID_i, t_1\}$.

- (iii) When TA receives the message form the RSU, it checks the freshness of t_1 and verifies whether the message has expired or not. On success, TA computes $PID_i^* = AID_i \oplus h(DID_i, x)$. TA searches the legitimate table of U_i based on PID_i^* . If table is not found, TA stops the process; otherwise, it continues the process. TA computes $BID_i = h(DID_i, x) \oplus ID_i$. After computing BID_i , TA sends message $\{BID_i, t_1\}$ to RSU.

Step 4. RSU \rightarrow OBU: $\{M_2, R_2, t_2\}$.

- (iv) When RSU receives the message from the TA side, check the freshness of t_2 and verify whether the received message has expired. On success, the RSU computes $ID_i = BID_i \oplus h(DID_i, x)$ and verifies $M_1 = h(ID_i, DID_i, A_i^*, R_1, t_0)$; if RSU finds these parameters correct and satisfies the originality, the process continues; otherwise, it stops. After that, RSU computes $R_2 = kP, K_S = h(R_0, R_2, kR_0)$, $M_2 = h(K_S, A_i^*, R_0, R_2, t_2)$. Now RSU stores data tuple $\langle PID_i^*, A_i^*, K_S \rangle$. RSU sends the message $\{M_2, R_2, t_2\}$ to OBU.

Step 5. The OBU reacts by executing the following steps.

- (v) When the OBU receives the message from the RSU, it checks the freshness of t_3 , and on success, the SC computes $K_S = h(R_0, R_2, rR_2)$ and verifies $M_2 = h(K_S, A_i^*, R_0, R_2, t_2)$. On successful verification, the OBU considers K_S as session key and U_i as authenticated user.

4.5. Malicious User Tracking. If the malicious vehicle/node tries to authenticate itself, then the following steps will be performed to identify and track the malicious node:

- (i) When RSU gets the message from OBU and computes the $PID_i^* = DID_i \oplus h(R_1, t_0)$, $A_i^* = M_0 \oplus h(R_1, t_0)$, then RSU gets the value of A_i^* from database (stored tuple) (PID_i^*, A_i^*, K_S) . RSU computes the $MA = PID_i^* \oplus x \oplus t_3$, $M_3 = h(PID_i^*, A_i^*, MA, MP, t_3)$. After that, RSU sends message $\{MA, MP, M_3, t_3\}$ to trusted authority. When TA receives a message from the RSU, TA checks and verifies the freshness of message and stops the process if freshness is not validated. The TA computes the $PID_i^* = MA \oplus x \oplus t_3$ and $A_i^* = MP \oplus PID_i^* \oplus t_3$. The TA checks and verifies the $M_3 = h(PID_i^*, A_i^*, MA, MP, t_3)$. If it holds, the process continues.
- (ii) The TA searches the verifier table; if the table contains $(ID_i, PID_i^*, \alpha_i)$, the process continues. The TA checks and verifies $A_i^* = h(ID_i, x) \oplus \alpha_i$; if this parameter holds, the process continues. After the confirmation of the malicious vehicle, TA computes the $MN = ID_i \oplus x \oplus t_4$, $M_4 = h(ID_i, MN, t_4)$ and sends a message to RSU $\{MN, M_4, t_4\}$. RSU deletes the entry from the legal user table and declares that malicious user is not a legitimate user. After receiving the message from TA, the RSU computes the message again and checks its originality such as $ID_i = MN \oplus x \oplus t_4$, $M_4 = h(ID_i, MN, t_4)$. Now, RSU broadcasts the malicious node identity (ID_i, PID_i^*) to inform other nodes or vehicles.

4.6. Password and Biometric Change. Under this phase, the user changes his password or gives the vehicle to another user. The user changes his biometric key using the following step:

- (i) The U_i inserts SC into OBU and enters the identity ID_i^* and password PW_i^* and imprints the biometric information W_i' . The FE extracts $\alpha_i^* = \text{Rep}(W_i', \beta_i)$. The SC computes $y_i^* = C_i \oplus h(ID_i^*, PW_i^*, \alpha_i^*)$. The SC checks and verifies $D_i = h(PW_i^*, y_i^*, \alpha_i^*)$; if equation carries these parameters, U_i is granted permission to change his/her password and biometric key; otherwise, it stops the process. In case U_i wants to change his/her password, the SC computes the $C_{i_{New}} = h(ID_i^*, PW_{i_{New}}^*, \alpha_i^*) \oplus y_i$, $D_{i_{New}} = h(PW_{i_{New}}^*, y_i^*, \alpha_i^*)$. The SC replaces the values of C_i, D_i with $C_{i_{New}}, D_{i_{New}}$ and stores these into memory.
- (ii) If U_i wants to hand over the vehicle temporarily to another user, he/she must change biometric key. $U_{i_{New}}$ puts his own biometric information $W_{i_{New}}$ in the special device to get $\text{Gen}(W_{i_{New}}) = (\alpha_{i_{New}}, \beta_{i_{New}})$ via fuzzy extractor. SC computes the

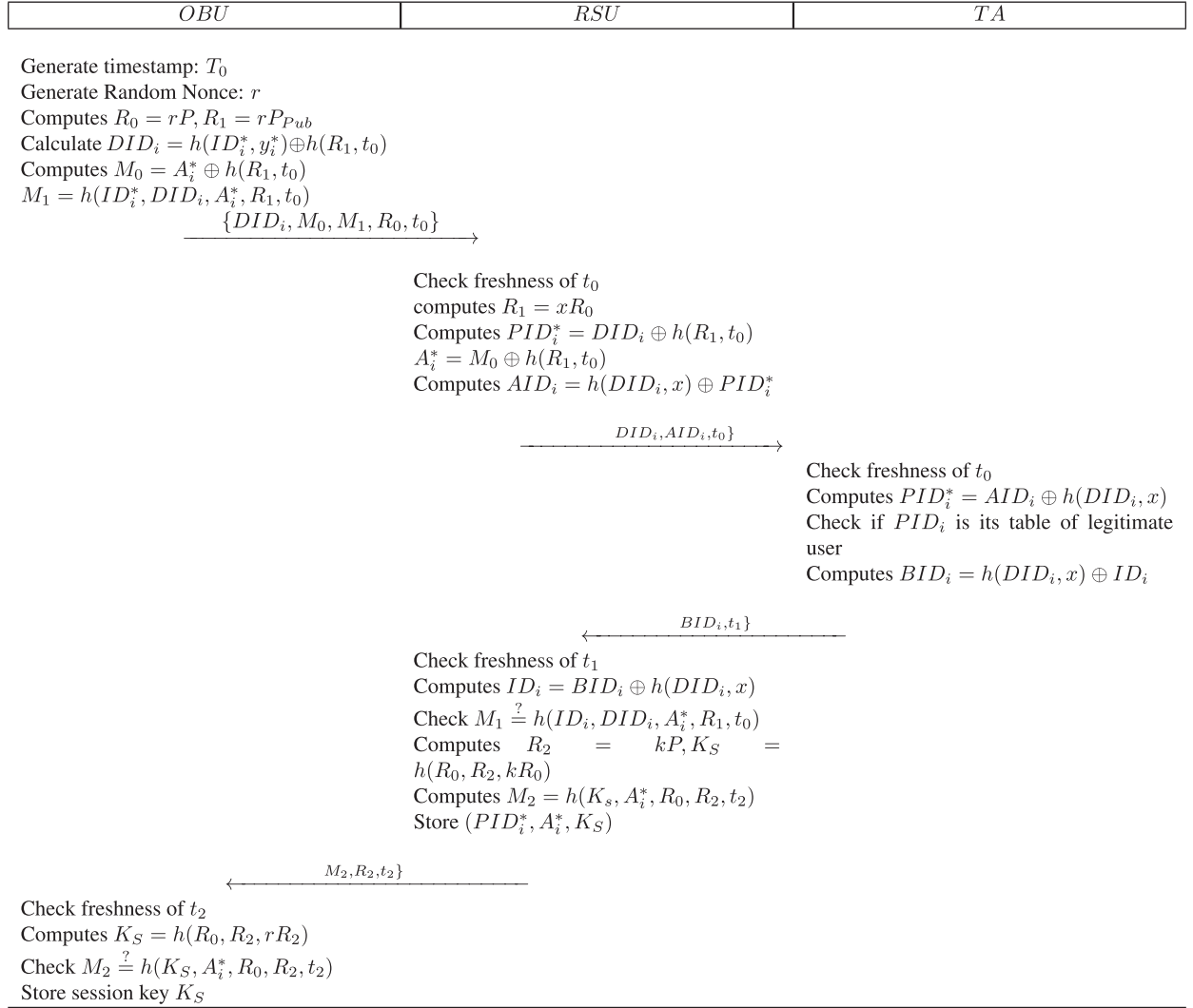


FIGURE 3: User authentication phase of Xu et al.'s scheme.

$C_{i_{New}} = h(ID_i^*, PW_i^*, \alpha_i) \oplus y_i^*$ and $D_{i_{New}} = h(PW_i^*, y_i^*, \alpha_{i_{New}})$. SC computes $A_i^* = E_i h(ID_i^*, y_i^*)$, $h(ID_i^*, x) = A_i^* \oplus \alpha_i$ and $E_{i_{New}} = h(ID_i^*, x) \oplus \alpha_{i_{New}} \oplus h(ID_i^*, y_i^*)$. SC replaces (β_i, C_i, D_i, E_i) in memory with $(\beta_{i_{New}}, C_{i_{New}}, D_{i_{New}}, E_{i_{New}})$ to complete the process of biometric key exchange.

5. Weaknesses of Xu Et Al.'s Scheme

This section describes the ability of a dishonest RSU to bypass TA and construct a session key with requesting OBU.

5.1. TA Bypassing. If an RSU is dishonest, it can easily by pass TA and create a session key directly with OBU, and for this, RSU can skip sending message (DID_i, AID_i, t_0) . In this case, the RSU will calculate $R_1 = xR_0$, $PID_i^* = DID_i \oplus h(R_1, t_0)$, and $A_i^* = M_0 \oplus h(R_1, t_0)$. Now RSU just skips some of the remaining steps and goes directly on the step which computes $R_2 = kP, K_S = h(R_0, R_2, kR_0)$ and $M_2 = h(K_S, A_i^*, R_0, R_2, t_2)$ and sends PID_i^*, A_i^*, K_S to OBU. The OBU checks validity of t_2 and then computes

$K_S = h(R_0, R_2, rR_2)$. Finally, the OBU checks $M_2 = h(K_S, A_i^*, R_0, R_2, t_2)$. As the computation of K_S involves R_0, R_2 , and $rR_2 = kR_0$ and the RSU has access to all these parameters, it does not require any information from the TA. Therefore, it can easily compute K_S without any verification by the TA. Hence, in the scheme of Xu et al. [10], a dishonest RSU can bypass the TA.

6. Proposed Scheme

The following subsections explain the main phases of the proposed scheme.

6.1. System Initialization. Under this phase, TA performs the following steps for registration:

- (i) TA selects the cyclic additive group G with order of p and a generator P .
- (ii) TA selects an ECE : $y^2 = X^3 + iX + j \pmod{P}$ where $\{i, j\} \in \{-RZ_p^*\}$.

- (iii) TA generates a primary key x as a random number and then computes the $P_{\text{pub}} = x.P$ as the public key.
- (iv) Through secure channel, TA uploads the primary key x into RSUs and TPD.

6.2. User Registration. Under this phase, user and TA interact through following steps for the completion of registration process, where U_i approaches the TA to complete the process:

- (i) The U_i puts his biometric information on the reader to get $\{\alpha_i, \beta_i\} = \text{GEN}(W)$ via FE and provides his original identity ID_i and password PW_i to the TA .
- (ii) TA generates a random number y_i for each U_i , and TA computes $PID_i = h(ID_i, y_i)$, $A_i^* = h(ID_i, x) \oplus \alpha_i$, $C_i = h(ID_i, PW_i, \alpha_i) \oplus y_i$, $D_i = h(PW_i, y_i, \alpha_i)$, $E_i = PID_i \oplus A_i$.
- (iii) TA forwards the SC to U_i , which is engraved with the following tuple: $\langle G, p, P, \beta_i, C_i, D_i, h \rangle$. The TA now stores the tuple $\{ID_i, \alpha_i\}$ in the verification table.

6.3. User Login. Under the user login phase, OBU checks and verifies U_i 's legitimacy via the following steps:

- (i) User U_i inserts the SC into OBU and enters the ID_i^* and PW_i^* and imprints biometric information W_i^* . The FE extracts $\alpha_i^* = \text{Rep}(W_i^*, \beta_i)$.
- (ii) The SC computes $y_i^* = C_i \oplus (ID_i^*, PW_i^*, \alpha_i^*)$.
- (iii) The SC verifies $D_i \stackrel{?}{=} h(PW_i^*, y_i^*, \alpha_i^*)$. If this information is true, the user login succeeds and SC computes $A_i^* = E_i \oplus (ID_i^*, y_i^*)$. After that, user attenuation will start. Otherwise, SC terminates the registration process and SC sets an error threshold to increase the security. If U_i tries repeatedly through entering wrong information and attempts exceed the threshold value, U_i is blocked.

6.4. User Authentication. Under the user authentication phase, OBU and RSU perform mutual authentication and produce a session key for data/information communication. Figure 4 describes the complete process of user authentication phase of the proposed scheme.

Step 1. OBU \rightarrow RSU: $\{DI, D_i, M_0, M_1, R_0, t_0\}$.

- (i) The OBU generates a random number r and computes $R_0 = rP$, $R_1 = rP_{\text{pub}}$.
- (ii) The OBU computes the dynamic identity $DID_i = h(ID_i^*, y_i^*) \oplus h(R_1, t_0)$ and t_0 (timestamp).
- (iii) The OBU computes $M_0 = A_i^* \oplus h(R_1, t_0)$ and $M_1 = h(ID_i^*, DID_i, A_i^*, R_1, t_0)$.
- (iv) The OBU sends $DID_i, M_0, M_1, R_0, t_0$ to RSU through insecure channel.

Step 2. RSU \rightarrow TA: $\{DID_i, AID_i, t_0\}$.

- (v) After receiving the message from the OBU, the RUS checks the freshness of t_0 and verifies

whether the message has expired or not. If the message is fresh, the process continues; otherwise, RSU stops the process.

- (vi) The RUS computes $R_1 = xR_0$, $PID_i^* = DID_i \oplus h(R_1, t_0)$, and $A_1^* = M_0 \oplus h(R_1, t_0)$.
- (vii) The RSU computes $AID_i = h(DID_i, x) \oplus PID_i^*$.
- (viii) Now, the RSU sends the message $\{DID_i, AID_i, t_0\}$ to the TA .

Step 3. $TA \rightarrow$ RSU: $\{BID_i, t_1\}$.

- (ix) When TA receives the message form the RSU, it checks the freshness of t_1 and verifies whether message timeliness has expired or not. On successful validation of timeliness, the process continues; otherwise, the process is stopped.
- (x) Now, TA computes $PID_i^* = AID_i \oplus h(DID_i, x)$. TA searches the verifier table for PID_i^* . If corresponding entry in the table is not found, the TA stops the process; otherwise, the process continues.
- (xi) TA computes the $BID_i = h(DID_i, x) \oplus ID_i$. After computing the BID_i , TA sends message $\{BID_i, t_1\}$ to RSU.

Step 4. RSU \rightarrow OBU: $\{M_2, R_2, t_2\}$.

- (xii) When RSU receives the message from the TA side, check the freshness of t_2 and verify whether the received message has expired.
- (xiii) On successful validation of timeliness, the RSU computes $ID_i = BID_i \oplus h(DID_i, x)$.
- (xiv) RSU verifies $M_1 \stackrel{?}{=} h(ID_i, DID_i, A_i^*, R_1, t_0)$ and on success executes the next steps.
- (xv) The RSU computes $R_2 = kP$, $K_S = h(R_0, R_2, kR_0, \overline{ID_i})$, $M_2 = h(K_S, A_i^*, R_0, R_2, t_2)$.
- (xvi) The RSU stores the data tuple $\langle PID_i^*, A_i^*, K_S \rangle$.
- (xvii) The RSU sends the message $\{M_2, R_2, t_2\}$ to OBU

Step 5. The OBU performs following steps.

- (xviii) When the OBU receives the message from the RSU, it checks the freshness of t_3 .
- (xix) On successful validation of timeliness, the SC computes the $K_S = h(R_0, R_2, rR_2, \overline{ID_i})$.
- (xx) Now, SC verifies the $M_2 \stackrel{?}{=} h(K_S, A_i^*, R_0, R_2, t_2)$, and if it is proved, the process of mutual authentication is assumed to be successfully completed. Furthermore, the K_S will be kept for further use.

6.5. Malicious User Tracking. Following is the malicious user tracking phase of the proposed scheme:

- (i) RSU gets the message from OBU, computes the $PID_i^* = DID_i \oplus h(R_1, t_0)$, $A_i^* = M_0 \oplus h(R_1, t_0)$, and gets stored tuple (PID_i^*, A_i^*, K_S) . RSU computes the $MA = PID_i^* \oplus x \oplus t_3$, $MA = PID_i^* \oplus A_i^* \oplus t_3$, $M_3 = h(PID_i^*, A_i^*, MA, MP, t_3)$. After that, RSU sends

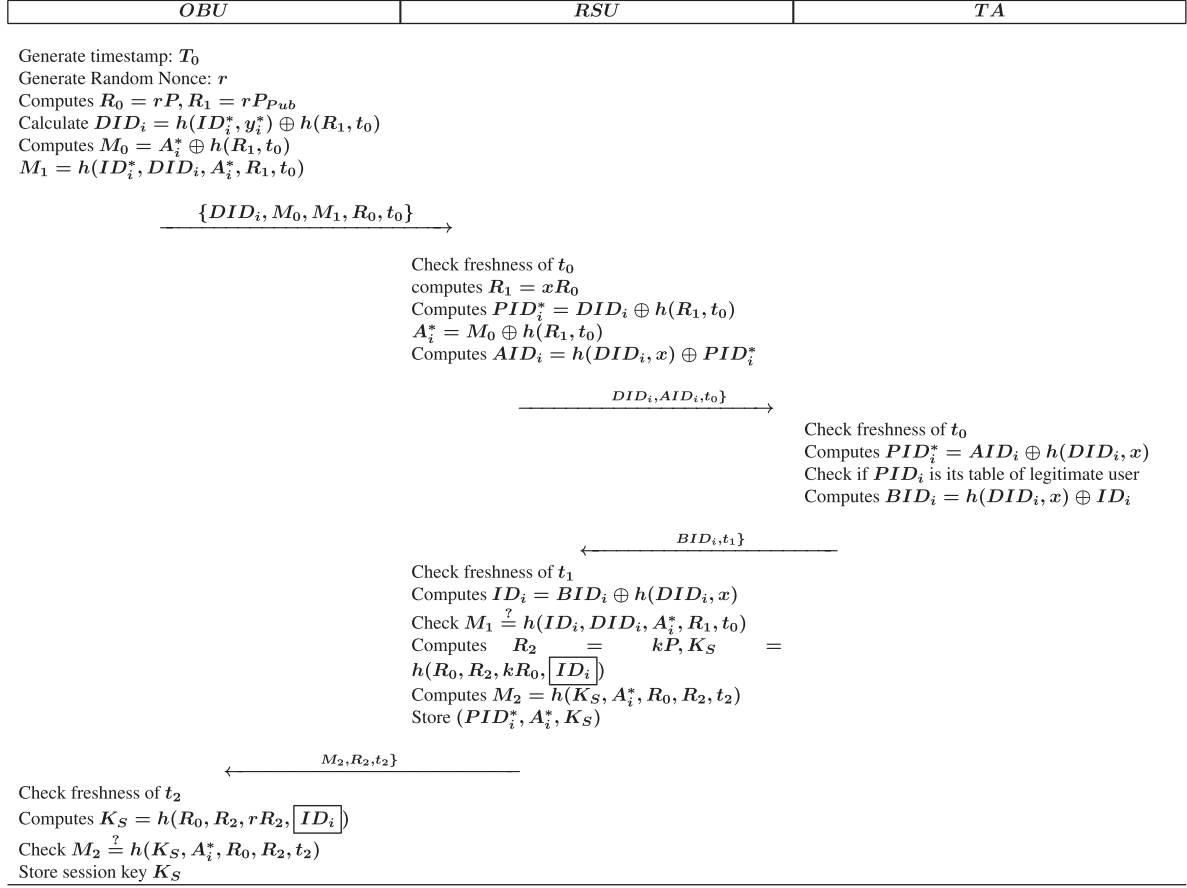


FIGURE 4: User authentication phase of the proposed scheme.

message $\{MA, MP, M_3, t_3\}$ to the trusted authority. When TA receives message from the RSU , TA checks and verifies the freshness of message. On successful validation of timeliness, the TA computes the $PID_i^* = MA \oplus x \oplus t_3, A_i^* = MP \oplus PID_i^* \oplus t_3$. The TA then checks and verifies the $M_3 = h(PID_i^*, A_i^*, MA, MP, t_3)$. On successful validation, the process continues; otherwise, the process is stopped by RSU .

- (ii) The TA searches the user verifier table for $(ID_i, PID_i^*, \alpha_i)$; if these values are found in the table, rest of the process continues; otherwise, the process is stopped. The TA checks and verifies $A_i^* = h(ID_i, x) \oplus \alpha_i$; if this equation holds, the malicious vehicle is identified. After the confirmation of the malicious vehicle, TA computes $MN = ID_i \oplus x \oplus t, M_4 = h(ID_i, MN, t_4)$ and sends a message $\{MN, M_4, t_4\}$ to RSU . The RSU selects the entry from the legal user table and declares that vehicle is malicious. After receiving the message from TA , the RSU computes the message again and checks its originality $ID_i = MN \oplus x \oplus t_4$. RSU broadcasts the malicious node identity (ID_i, PID_i^*) to inform other nodes or vehicles about the malicious node and warns RSU that malicious node is no more allowed to communicate with system entities including the $RSUs$.

6.6. *Password and Biometric Change.* Under this phase, the user changes his password or hands over his vehicle to some other user, and it needs to change his own biometric key. We consider the same process as that used by Xu et al.'s scheme. Therefore, it is not reproduced here.

7. Security Analysis

Under this section, we have performed the formal security analysis using BAN-Logic [29–31] in addition to the security discussion of the proposed scheme.

7.1. *Formal Security Analysis.* This section provides the detailed formal security analysis of the proposed security scheme using the BAN-Logic. It first describes the basic notations of BAN-Logic that are used to analyze the proposed scheme's secure authentication and correctness. Here, X is used for the formula, and N and Q are used as participants.

- (i) $(\#X)$: X is fresh.
- (ii) $N| \equiv X$: N believes that X is trustworthy.
- (iii) $N| \sim X$: N said X once.
- (iv) $N \triangleleft X$: N sees X .
- (v) $N|X$: N has jurisdiction over X .

- (vi) $N \stackrel{K_S}{\leftrightarrow} Q$: between N and Q , K_S is the shared key.
- (vii) $\{X, Y\}_K$: K is used to encrypt X and Y .
- (viii) $(X)_Y$: X and Y are combined.

Following are the rules of BAN-Logic:

Rule 1: message meaning rule.

If N sees X and believes that X is encrypted by shared key K among N and Q , then N believes Q said X once.

$$\frac{N| \equiv \stackrel{K}{\leftarrow} Q, N \triangleleft \{X\}_K}{N| \equiv Q| \sim X} \quad (5)$$

Rule 2: nonce verification rule.

If N believes that the statement X is updated and N also believes that Q once said X , then N believes Q is the statement of X .

$$\frac{N| \equiv \#X, N| \equiv Q| \sim X}{N| \equiv Q| \equiv X} \quad (6)$$

Rule 3: jurisdiction rule.

If N believes Q has jurisdiction over the statement X and N believes Q the statement X , then N believes the statement of X .

$$\frac{N| \equiv Q \Rightarrow X, N| \equiv Q| \equiv X}{N| \equiv X} \quad (7)$$

Rule 4: session key rule.

If N believes the freshness of X , N and Q believes on X , then N believes that a key is shared between N and Q .

$$\frac{N| \equiv \#(X), N| \equiv Q| \equiv X}{N| \equiv N \stackrel{K}{\leftrightarrow} Q} \quad (8)$$

Rule 5: freshness rule.

If a part of X is believed by N as updated, then $\{X, Y\}$ is also believed by N as updated.

$$\frac{N| \equiv \#(X)}{N| \equiv \#(X, Y)} \quad (9)$$

Rule 6: belief rule.

If N believes that Q believes in the statement of $\{X, Y\}$, then N believes that Q believes in the part of statement X .

$$\frac{N| \equiv Q| \equiv \{X, Y\}}{N| \equiv Q| \equiv X} \quad (10)$$

The goals of our TFPPASV protocol are proved through BAN-Logic as under:

- (i) G1: $\text{OBU} | \equiv \text{OBU} \stackrel{K_S}{\leftrightarrow} TA$
- (ii) G2: $TA | \equiv \text{OBU} \stackrel{K_S}{\leftrightarrow} TA$
- (iii) G3: $\text{RSU} | \equiv \text{OBU} \stackrel{K_S}{\leftrightarrow} TA$
- (iv) G4: $\text{OBU} | \equiv TA | \equiv \text{OBU} \stackrel{K_S}{\leftrightarrow} TA$

- (v) G5: $TA | \equiv \text{OBU} | \equiv \text{OBU} \stackrel{K_S}{\leftrightarrow} TA$
- (vi) G6: $\text{RSU} | \equiv \text{OBU} | \equiv \text{OBU} \stackrel{K_S}{\leftrightarrow} TA$
- (vii) G7: $\text{RSU} | \equiv TA | \equiv \text{OBU} \stackrel{K_S}{\leftrightarrow} TA$

In the proposed TFPPASV scheme, the messages are sent over the public channel. The details of these messages are mentioned below:

- (i) M1: $\text{OBU} \longrightarrow \text{RSU}: \text{DID}_i, M_0, M_1, R_0, t_0$
- (ii) M2: $\text{RSU} \longrightarrow TA: \text{DID}_i, \text{AID}_i, t_0$
- (iii) M3: $TA \longrightarrow \text{RSU}: \text{BID}_i, t_1$
- (iv) M4: $\text{RSU} \longrightarrow \text{OBU}: M_2, R_2, t_2$

Furthermore, the following assumptions are used for analyzing the proposed scheme using BAN-Logic.

- (i) A1: $\text{OBU} | \equiv \#(r_{\text{OBU}})$
- (ii) A2: $TA | \equiv \#(r_{\text{RSU}})$
- (iii) A3: $\text{RSU} | \equiv \#(r_{TA})$
- (iv) A4: $\text{RSU} | \equiv \text{OBU} \Rightarrow \text{DID}_i$
- (v) A5: $\text{RSU} | \equiv \text{OBU} \stackrel{A1}{\Rightarrow} TA$
- (vi) A6: $\text{RSU} | \equiv \#(r_{\text{OBU}})$
- (vii) A7: $\text{RSU} | \equiv \text{OBU} \Rightarrow r_{\text{OBU}}$
- (viii) A8: $\text{RSU} | \equiv \#(A_i^*)$
- (ix) A9: $\text{RSU} | \equiv \text{OBU} \Rightarrow (A_i^*)$
- (x) A10: $TA | \equiv \text{RSU} \Rightarrow \text{DID}_i$
- (xi) A11: $TA | \equiv \text{RSU} \Rightarrow \text{AID}_i$
- (xii) A12: $TA | \equiv \#(\text{AID}_i)$
- (xiii) A13: $TA | \equiv \#(\text{PID}_i^*)$
- (xiv) A14: $TA | \equiv \text{RSU} \Rightarrow \text{PID}_i^*$
- (xv) A15: $TA | \equiv \#(r_{\text{OBU}})$
- (xvi) A16: $\text{RSU} | \equiv TA \stackrel{R_1, t_0}{\Rightarrow} TA$
- (xvii) A17: $\text{RSU} | \equiv \#(r_{TA})$
- (xviii) A18: $\text{RSU} | \equiv TA | \Rightarrow r_{TA}$
- (xix) A19: $\text{OBU} | \equiv \text{RSU} | \equiv A_1$
- (xx) A20: $\text{OBU} | \equiv \#(A_1)$
- (xxi) A21: $\text{OBU} | \equiv \#(r_{TA})$
- (xxii) A22: $\text{OBU} | \equiv \text{RSU} | \Rightarrow r_{TA}$
- (xxiii) A23: $\text{OBU} | \equiv \text{OBU} \stackrel{R_1, t_0}{\Rightarrow} TA$
- (xxiv) A24: $\text{OBU} | \equiv (r_{\text{RSU}})$
- (xxv) A25: $\text{OBU} | \equiv TA | \Rightarrow r_{\text{RSU}}$
- (xxvi) A26: $\text{RSU} | \equiv \text{RSU} | \equiv r_{\text{OBU}}$

7.1.1. BAN-Logic Proof. The proof of proposed scheme through BAN-Logic analysis is as follows.

S_1 can be acquired from M_1 .

$S_1: \text{RSU} \triangleleft \{\text{DID}_i, M_0, M_1, R_0, t_0\}$.

$S_2: \text{RSU} | \equiv \text{OBU} | \equiv \text{DID}_i$. Based on A_4, S_2 , and rule 3, we can obtain $S_3: \text{RSU} | \equiv \text{DI } D_i$. According to S_1 , it implies that $S_4: \text{RSU} \triangleleft r_{\text{OBU}}, \text{DID}_{iA1}$. By A_5, S_4 , and rule 1, it implies that $S_5: \text{RSU} | \equiv \text{OBU} | \sim (r_{\text{OBU}}, \text{DID}_i)$. By A_6, S_5 , and rule 2,

we can obtain $S_6: \text{RSU} \equiv \text{OBU} \equiv r_{\text{OBU}}$. According to A_7, S_6 , and rule 3, it implies that $S_7: \text{RSU} \equiv r_{\text{OBU}}$. According to S_1 , we have acquired $S_8: \text{RSU} \triangleleft \text{AID}_i$. By A_5, S_8 , and rule 1, it implies that $S_9: \text{RSU} \equiv \text{OBU} \sim \text{AID}_i$. By A_8, S_9 , and rule 2, we can obtain $S_{10}: \text{RSU} \equiv \text{OBU} \equiv \text{AID}_i$. According to A_9, S_{10} , and rule 3, it implies that $S_{11}: \text{RSU} \equiv \text{AID}_i$.

By M_2 , we can obtain $S_{12}: \text{TA} \triangleleft \text{DID}_i, \text{AID}_i, t_0$ and further $S_{13}: \text{TA} \equiv \text{RSU} \equiv \text{DID}_i$. Based on A_{10}, S_{13} , and rule 3, we can obtain $S_{14}: \text{TA} \equiv \text{DID}_i$. By A_{11}, A_{12} , and rule 4, it implies that $S_{15}: \text{TA} \equiv \xrightarrow{A_1} \text{RSU}$. According to S_{12} , we have $S_{16}: \text{TA} \triangleleft \text{PID}_i^* \text{RSU}$. Based on S_{15}, S_{16} , and rule 1, it implies that $S_{17}: \text{TA} \equiv \text{RSU} \sim r_{\text{RSU}}$. By A_{13}, S_{17} , and rule 2, we can obtain $S_{18}: \text{TA} \equiv \text{RSU} \equiv r_{\text{RSU}}$. According to A_{14}, S_{18} , and rule 3, it implies that $S_{19}: \text{TA} \equiv r_{\text{RSU}}$. Based on A_{11}, A_{12} , and rule 4, we have $S_{20}: \text{TA} \equiv \text{TA} \xrightarrow{\text{PID}_i^*} \text{RSU}$. According to S_{12} , we have $S_{21}: \text{TA} \triangleleft r_{\text{OBU}}$. By S_{20}, S_{21} , and rule 1, it implies that $S_{22}: \text{TA} \equiv \text{RSU} \sim r_{\text{OBU}}$. By A_{15}, S_{22} , and rule 2, we can obtain $S_{23}: \text{TA} \equiv \text{RSU} \equiv r_{\text{OBU}}$. Based on A_{26}, S_{23} , and rule 3, it implies that $S_{24}: \text{TA} \equiv r_{\text{OBU}}$. $K_S = h(R_0, R_2, kR_0, ID_i)$.

$S_{25}: \text{TA} \equiv \text{OBU} \xleftrightarrow{K_S} \text{TA}$ is obtained. (G2). According to A_2, S_{25} , and rule 4, we can obtain $S_{26}: \text{RSU} \equiv \text{OBU} \xrightarrow{A_1} \text{RSU}$. (G5).

By M_3 , we have $S_{27}: \text{RSU} \triangleleft \text{BID}_i, t_1$ and further $S_{28}: \text{RSU} \triangleleft ID_i = \text{BID}_i \oplus h(\text{DID}_i, x)$. Based on A_{16}, S_{28} , and rule 1, we can obtain $S_{29}: \text{RSU} \equiv \text{TA} \equiv r_{\text{TA}}$. By A_{17}, S_{29} , and rule 2, it implies that $S_{30}: \text{RSU} \equiv \text{TA} \equiv r_{\text{TA}}$. Based on A_{18}, S_{30} , and rule 3, we can obtain $S_{31}: \text{RSU} \equiv r_{\text{TA}}$. According to S_{27}, S_{31} , and S_{31} , it implies that $S_{32}: \text{RSU} \equiv \text{OBU} \xleftrightarrow{K_S} \text{TA}$. (G3). Based on A_{16}, S_{32} , and rule 4, we can obtain $S_{33}: \text{RSU} \equiv \text{OBU} \equiv \xleftrightarrow{K_S} \text{TA}$. (G6). According to A_{12}, S_{32} , and rule 4, it implies that $S_{34}: \text{RSU} \equiv \text{TA} \equiv \text{OBU} \xleftrightarrow{K_S} \text{TA}$. (G7).

By M_4 , we have $S_{35}: \text{OBU} \triangleleft M_2, R_2, t_2$. Based on A_{19}, A_{20} , and rule 4, we can obtain $S_{36}: \text{OBU} \equiv \text{OBU} \xrightarrow{h(R_0, R_2, kR_0, ID_i)} \text{RSU}$. According to S_{35} , we have $S_{37}: \text{OBU} \triangleleft r_{(\text{RSU}), h(R_0, R_2, kR_0, ID_i)}$. Based on S_{36}, S_{37} , and rule 1, it implies that $S_{38}: \text{OBU} \equiv \text{RSU} \sim r_{\text{RSU}}$. By A_{21}, S_{38} , and rule 2, we can obtain $S_{39}: \text{OBU} \equiv \text{RSU} \equiv r_{\text{RSU}}$. According to A_{22}, S_{39} , and rule 3, it implies that $S_{40}: \text{OBU} \equiv r_{\text{RSU}}$.

We have $S_{41}: \text{OBU} \triangleleft r_{\text{TA}}, h(\text{OBU} \| r_{(\text{RSU})})$. Based on A_{23}, S_{41} , and rule 1, it implies that $S_{42}: \text{OBU} \equiv \text{TA} \sim r_{\text{TA}}$. By A_{24}, S_{42} , and rule 2, we can obtain $S_{43}: \text{OBU} \equiv \text{TA} | r_{\text{TA}}$. Based on A_{25}, S_{43} , and rule 3, it implies that $S_{44}: \text{OBU} \equiv r_{\text{TA}}$. According to S_{40} and S_{44} , we can obtain $S_{45}: \text{OBU} \equiv \text{OBU} \xleftrightarrow{K_S} \text{TA}$. (G1). According to A_{24} and S_{45} , we can obtain $S_{46}: \text{OBU} \equiv \text{TA} \equiv \text{OBU} \xleftrightarrow{K_S} \text{TA}$. (G4).

7.2. Security Discussion. The security feature provision and resistance of the proposed scheme against various attacks are explained in the following subsection.

7.2.1. Anonymity and Untraceability. In the proposed TFPPASV protocol, the identity ID_i of the user is secure, because in TFPPASV, the vehicle sends a pseudo identity $\text{DID}_i = h(ID_i^*, y_i^*) \oplus h(R_1, t_0)$ instead of its original identity

ID_i over the communication channel. The attacker can intercept DID_i , but it cannot extract ID_i because it is concealed in a oneway hash function along with a random number and other parameters. The only method to get the identity is to break the hash function and get knowledge of random numbers involved in the computation of DID_i . Thus, the protocol provides user anonymity. In addition, the proposed protocol provides untraceability for the user because when the message is transmitted on a communication channel, it uses a random number during the authentication process. Thus, the attacker is not able to track the user.

7.2.2. Perfect Forward Secrecy. The proposed TFPPASV protocol provides ultimate forward secrecy because it uses various random numbers during the message transmission. Three parameters $R_O = rP, R_2 = kP$ and kR_0 are used to construct the session key $K_S = h(R_0, R_2, kR_0, \text{DID}_i)$. If an attacker wants to launch an attack on the basis of a compromised session key, the attacker is not able to obtain the previous and subsequent session keys. Thus, the proposed protocol provides forward secrecy.

7.2.3. Replay Attack. The proposed TFPPASV protocol provides resistance against the replay attack. Three entities (OBU, RSU, and TA) are involved in the authentication phase of the proposed TFPPASV protocol. These entities send the messages to each other such as $(\text{DID}_i, M_0, M_1, R_0, t_0)$, $(\text{DID}_i, \text{AID}_i, t_0)$, (BID_i, t_1) , and (M_2, R_2, t_2) . In each of these messages, random numbers and timestamps are used and these are session specific. If an attacker wants to launch a replay attack, the replayed message cannot pass the verification process and the recipient can easily identify the replay attack.

7.2.4. Offline Password Guessing Attack. Our TFPPASV protocol provides resistance against offline password guessing attack. During registration phase, some parameters are stored into SC such as $C_i = h(ID_i, PW_i, \alpha_i) \oplus y_i$, $D_i = h(PW_i, y_i, \alpha_i)$. The PW_i is masked with y_i generated randomly and the biometric key α_i . Thus, attacker is not able to guess the password.

7.2.5. Impersonation Attack. Our TFPPASV protocol provides resistance against impersonation assaults such as OBU impersonation assault, RSU impersonation assault, and TA impersonation assault.

OBU impersonation attack: if an attacker tries to impersonate the OBU, it requires to construct the original login request message: $(\text{DID}'_i, M'_0, M'_1, R'_0, t'_0)$ $\text{DID}'_i = h(ID_i^*, y_i^*) \oplus h(R_1, t_0)$, $M'_0 = A_i^* \oplus (R_1, t_0)$, $M'_1 = h(ID_i^*, \text{DID}_i, A_i^*, R_1, t_0)$, and $R'_0 = rP$ with updated random number r and timestamp t_0 . However, it is computationally difficult to recover t_0, DID_i , and R_1 for constructing $(\text{DID}'_i, M'_0, M'_1, R'_0, t'_0)$. Thus, the proposed protocol provides security against OBU impersonation.

RSU impersonation attack: for the execution of a RSU impersonation attack, the attacker tries to instigate a forgery

to TA on behalf of the RSU. The attacker needs to construct the (DID'_i, AID'_i, t'_0) with updated timestamp. In addition, it requires more confidential parameters such as (x, R_0) and R_1 . It is computationally hard to calculate these parameters from $(DID_i, M_0, M_1, R_0, t_0)$. Thus, the proposed TFPPASV scheme provides security against RSU impersonation.

TA impersonation attack: in the case of TA impersonation, the attacker needs to construct BID'_i, t_1 with an updated timestamp, and in addition, it requires the private key x , where $BID'_i = (DID_i, x) \oplus ID_i$. However, the attacker is not able to form the message until it gets the private key x and DID_i . Thus, the attacker is not able to launch TA impersonation attack.

7.2.6. Smart Card Stolen. The proposed protocol provides security against SC stolen. If an attacker captures the SC and gets the information $(G, p, P, \beta_i, C_i, D_i, E_i, h)$ from the SC and it wants to login via SC, the attacker also needs the user ID_i, PW_i , and the biometric key α_i in polynomial time, which is not possible for the attacker. Thus, the attacker is not able to complete a successful login.

7.2.7. Man-in-the-Middle Attack. If the attackers want to launch attack as a man-in-the-middle, it needs to capture the messages $(DID_i, M_0, M_1, R_0, R_1)$, (DID_i, AID_i, t_0) , (BID_i, t_1) , and (M_2, R_2, t_2) from the public communication channel. The attacker must change or replace the message and forward it on the channel to get authenticated from both sides. However, due to the inability of construction of legal messages, the attacker may not be able to get authenticated from any side without getting ID_i and PW_i and private key x of the TA .

7.2.8. Insider Attack. The proposed TFPPASV protocol protects from insider attacks because at the time of registration, user registers itself with TA on a secure channel. In addition, stored user passwords are in the ciphertext. It is computationally difficult for any dishonest insider to get information related to passwords and keys.

8. Security and Performance Analysis

This section describes the security features and computational and communication cost of the proposed TFPPASV scheme in relation to other schemes [10, 32–34].

8.1. Security Feature. Table 3 provides the complete bird's eye view of the security feature comparison of our TFPPASV scheme with related schemes [10, 32–34]. Through BAN-Logic analysis, we prove that our proposed scheme is correct. Section 5.1 discusses Xu et al.'s scheme [10] which has TA bypassing issue, and if RSU is dishonest, it can easily bypass the TA and establish a connection directly with OBU. Ma et al.'s [32] scheme does not provide security against malicious user tracking, offline password attack, and smart card stolen attack. Cui et al.'s [33] scheme is also insecure against the man-in-the-middle attack, offline password, and

TABLE 3: Security feature performance analysis.

Schemes	Ours	[10]	[32]	[33]	[34]
Correctness	✓	✓	✓	✓	✓
Vehicle impersonation attack	✓	✓	✓	✓	✓
Trusted authority impersonation attack	✓	✓	✓	✓	✓
Vehicle server impersonation attack	✓	✓	✓	✓	✓
Stolen SC attack	✓	✓	✗	✗	✗
Anonymity attack	✓	✓	✓	✓	✓
Untraceability attack	✓	✓	✓	✓	✓
Man-in-the-middle attack	✓	✓	✗	✗	✗
Offline password guessing attack	✓	✓	✗	✗	✗
Replay attack	✓	✓	✓	✓	✓
Mutual authentication	✓	✓	✓	✓	✓
Malicious user tracing	✓	✓	✓	✗	✗
TA bypassing	✓	✗	✓	✓	✓

Note. ✓: provides or resists; ✗: does not provide or does not resist.

smart card stolen attacks. Zhong et al.'s [34] scheme failed to provide security against the man-in-the-middle attack, offline password attack, and smart card stolen attack. The proposed scheme provides better security features compared to other related schemes [10, 32–34].

8.2. Computational Cost. In this section, we calculate the computational cost (CC) of the proposed TFPPASV scheme and compare it with the related schemes. Before calculating CC, we denote some symbols as follows: xor operation is denoted by T_{\oplus} , the execution time for scale multiplication on ECC is denoted by T_{sm} , and the execution time for hash function is represented by T_h . For calculating the CC, the real-time hardware platform with the following specifications: CPU: Intel I7-6700, with 4.00 GHz RAM 16 GB OS windows 10th, is adopted from [35]. T_{sm} furnishes in 0.442 ms, and the running time of T_h is 0.0001, while T_{\oplus} takes negligible time to complete the execution. Thus, T_{\oplus} is being ignored in the comparisons. We used SHA256 with 256 bit hash digest and the size of identity and random numbers are fixed at 64 bits. The proposed scheme executes $\{6T_{sm} + 15T_h + 8T_{\oplus}\}$ operations with the running time of 2.6535 ms. Referring to Table 4, computational cost of the proposed TFPPASV scheme is low as compared to Ma et al.'s scheme [32] and a bit high as compared to Cui et al. and Zhong et al.'s schemes [33, 34], respectively. However, the proposed TFPPASV scheme offers more security features as compared with related schemes.

8.3. Communication Cost. To calculate the communication cost of the proposed TFPPASV scheme and to compare it with related schemes, we adopted SHA-256 with 256 bit size. We also adopted 256 bit ECC parameters. In addition, identities and timestamps are taken as 64 bit length. In the proposed TFPPASV scheme, total four messages are exchanged for a successful authentication process completion. In message 1, $\{DID_i, M_0, M_1, R_0, t_0\} = \{256 + 256 + 256 + 256 + 64\} = 1088$ bits are sent from OBU to RSU. In message 2, $\{DID_i, AID_i, t_0\} = \{256 + 256 + 64\} = 576$ bits are sent from

TABLE 4: Performance comparisons.

Scheme	Computation cost	RT (ms)	ME	BE	SO
Ours	$6T_{sm}^* + 15T_h^* + 8T_{\oplus}^*$	2.6535	4	2560	1024
Xu et al. [10]	$6T_{sm}^* + 15T_h^* + 8T_{\oplus}^*$	2.6535	4	2560	1024
Ma et al. [32]	$17T_{sm}^* + 19T_h^* + 3T_{\oplus}^*$	7.5159	4	4992	832
Cui et al. [33]	$6T_{sm}^* + 3T_h^*$	2.6523	3	3840	512
Zhong et al. [34]	$1T_{sm}^* + 6T_h^*$	0.4426	3	4648	320

Note. RT: running time; ME: no. of message exchanges; BE: bit exchange; SO: storage overhead.

RSU to TA . In message 3, $\{BID_i, t_1\} = \{256 + 64\} = 320$ bits are sent from TA to RSU. In message 4, $\{M_2, R_2, t_2\} = \{256 + 256 + 64\} = 576$ bits are sent from RSU to OBU. Total communication cost of the proposed TFPPASV scheme is $= \{1088 + 576 + 320 + 576\} = 2560$ bits. Referring to Table 2, the TFPPASV scheme has low communication as compared to other related schemes [32–34].

8.4. Storage Cost. The proposed TFPPASV stores four authentication related parameters $\{P, \beta_i, C_i, D_i\}$ in addition to h function and system parameters $\{G, p\}$. The system parameters and functions take marginal memory and are stored in the smart card in all competing authentication schemes. Therefore, for analysis and comparison purposes, we focus on the authentication related parameters. The storage cost of the proposed TFPPASV $\{P, \beta_i, C_i, D_i\} = \{256 + 256 + 256 + 256\} = 1024$ bits. The storage cost of Xu et al.'s scheme is also same (i.e., 1024 bits). The storage cost of Ma et al. [32], Cui et al. [33], and Zhong et al. [34] is 832, 512, and 320, respectively.

9. Conclusion

In this study, we analyzed a recent authentication scheme and proved that the scheme of Xu et al. can become a victim of TA bypassing attack by a dishonest RSU. We then introduced an improved and bypassing free authentication scheme (TFPPASV) for VANETs. We used the lightweight ECC and symmetric key based functions to design our proposed TFPPASV scheme. In addition to a comprehensive discussion on the security feature provision of TFPPASV, we utilized the BAN-Logic analysis to prove the formal security of the TFPPASV. We also compared the security and performance of the TFPPASV with related schemes and showed that the proposed TFPPASV offers a good trade-off between the security and performance criterion. Therefore, it can be concluded that the TFPPASV is best suitable in practical VANET scenarios.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

J.M. and Z.D. were responsible for conceptualization. Y.Y., M.N.M.B., and M.A.B. were responsible for investigation. J.M. and Z.D. were responsible for original draft preparation. J.M., Y.Y., A.K.A.Y., and S.A.C. were responsible for review and editing. Z.D. and S.A.C. were responsible for supervision. Z.D. was responsible for funding acquisition. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

This study was supported by funds for Key Research and Development Plan Project of Shaanxi Province, China (grant nos. 2019ZDLGY17-08, 2019ZDLGY03-09-01, 2020ZDLGY09-02, and 2020GY-013), and funds for Science and Technology Innovation Leading Talent of Shaanxi Province, China (grant no. TZ0336).

References

- [1] Y. Wang, H. Zhong, Y. Xu, J. Cui, and G. Wu, "Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for vanets," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5373–5383, 2020.
- [2] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. Mumtaz Bhutta, "Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures," *Security and Communication Networks*, vol. 2021, no. 3, pp. 1–20, 2021.
- [3] F. Ahmed, L. Wei, Y. Niu et al., "Toward fine-grained access control and privacy protection for video sharing in media convergence environment," *International Journal of Intelligent Systems*, vol. 37, no. 5, pp. 3025–3049, 2022.
- [4] F.-Y. Wang, D. Zeng, and L. Yang, "Smart cars on smart roads: an IEEE intelligent transportation systems society update," *IEEE Pervasive Computing*, vol. 5, no. 4, pp. 68–69, 2006.
- [5] Y. Ming and X. Shen, "Pcpa: a practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks," *Sensors*, vol. 18, no. 5, p. 1573, 2018.
- [6] J. J. Cheng, J. L. Cheng, M. C. Zhou, F. Q. Liu, S. C. Gao, and C. Liu, "Routing in internet of vehicles: a review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.
- [7] S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, and A. Lei, "A lightweight authentication and privacy-preserving scheme for vanets using tesla and bloom filters," *ICT Express*, vol. 4, no. 4, pp. 221–227, 2018.
- [8] H. Oh, C. Yae, D. Ahn, and H. Cho, "5.8 ghz dsrc packet communication system for its services," *Gateway to 21st Century Communications Village. VTC 1999-Fall. IEEE VTS 50th Vehicular Technology Conference (Cat. No. 99CH36324)*, vol. 4, pp. 2223–2227, 1999.
- [9] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.
- [10] T. Xu, C. Xu, and Z. Xu, "An efficient three-factor privacy-preserving authentication and key agreement protocol for

- vehicular ad-hoc network,” *China Communications*, vol. 18, no. 12, pp. 315–331, 2021.
- [11] V. S. Miller, “Use of elliptic curves in cryptography,” in *Conference on the Theory and Application of Cryptographic Techniques*, vol. 218, pp. 417–426, Springer, Berlin, Heidelberg, 1985.
- [12] Y. Zheng, G. Chen, and L. Guo, “An anonymous authentication scheme in vanets of smart city based on certificateless group signature,” *Complexity*, vol. 2020, pp. 1–7, 2020.
- [13] Y. Chen, X. Cheng, S. Wang, and M. Gao, “Research on certificateless group signature scheme based on bilinear pairings,” *Netinfo Security*, vol. 3, pp. 53–58, 2017.
- [14] N. Zhao, G. Zhang, and X. Gu, “Certificateless aggregate signature scheme for privacy protection in vanet,” *Computer Engineering*, vol. 46, no. 1, pp. 114–128, 2020.
- [15] J. Qu and X.-L. Tan, “Two-factor user authentication with key agreement scheme based on elliptic curve cryptosystem,” *Journal of Electrical and Computer Engineering*, vol. 2014, pp. 1–6, 2014.
- [16] T. Nandy, M. Y. I. Idris, R. M. Noor et al., “A secure, privacy-preserving, and lightweight authentication scheme for vanets,” *IEEE Sensors Journal*, vol. 21, no. 18, pp. 20998–21011, 2021.
- [17] S. A. Chaudhry, “Comments on ”a secure, privacy-preserving, and lightweight authentication scheme for vanets,” *IEEE Sensors Journal*, vol. 22, no. 13, pp. 13763–13766, 2022.
- [18] M.-C. Chuang and J. F. Lee, “Team: Trust-extended authentication mechanism for vehicular ad hoc networks,” *IEEE Systems Journal*, vol. 8, no. 3, pp. 749–758, 2013.
- [19] Y. Zhou, X. Zhao, Y. Jiang, F. Shang, S. Deng, and X. Wang, “An enhanced privacy-preserving authentication scheme for vehicle sensor networks,” *Sensors*, vol. 17, no. 12, p. 2854, 2017.
- [20] L. Wu, Q. Sun, X. Wang et al., “An efficient privacy-preserving mutual authentication scheme for secure v2v communication in vehicular ad hoc network,” *IEEE Access*, vol. 7, pp. 55050–55063, 2019.
- [21] H. Vasudev, V. Deshpande, D. Das, and S. K. Das, “A lightweight mutual authentication protocol for v2v communication in internet of vehicles,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6709–6717, 2020.
- [22] J. Mahmood, Z. Duan, H. Xue et al., “Secure message transmission for v2v based on mutual authentication for vanets,” *Wireless Communications and Mobile Computing*, vol. 2021, pp. 2021–2116, 2021.
- [23] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, “An untraceable temporal-credential-based two-factor authentication scheme using ecc for wireless sensor networks,” *Journal of Network and Computer Applications*, vol. 76, pp. 37–48, 2016.
- [24] X. Li, J. Niu, S. Kumari et al., “A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments,” *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.
- [25] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, “2flip: a two-factor lightweight privacy-preserving authentication scheme for vanet,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896–911, 2016.
- [26] V. Paruchuri and A. Durrezi, “Paave: protocol for anonymous authentication in vehicular networks using smart cards,” in *Proceedings of the 2010 IEEE global telecommunications conference GLOBECOM 2010*, pp. 1–5, IEEE, Manhattan, New York, USA, 2010.
- [27] B. Ying and A. Nayak, “Anonymous and lightweight authentication for secure vehicular networks,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10626–10636, 2017.
- [28] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, “A secure authentication protocol for internet of vehicles,” *IEEE Access*, vol. 7, pp. 12047–12057, 2019.
- [29] A. C. Shehzad, “Designing an Efficient and Secure Message Exchange Protocol for Internet of Vehicles,” *Security and Communication Networks*, vol. 2021, pp. 1–9, 2021.
- [30] T. Maitra, M. S. Obaidat, R. Amin, S. K. H. Islam, S. A. Chaudhry, and D. Giri, “A robust elgamal-based password-authentication protocol using smart card for client-server communication,” *International Journal of Communication Systems*, vol. 30, no. 11, Article ID e3242, 2017.
- [31] T.-Y. Wu, L. Yang, Z. Lee, S.-C. Chu, S. Kumari, and S. Kumar, “A provably secure three-factor authentication protocol for wireless sensor networks,” *Wireless Communications and Mobile Computing*, vol. 202115 pages, 2021.
- [32] M. Ma, D. He, H. Wang, N. Kumar, K. K. R. Choo, and R. C. Kwang, “An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8065–8075, 2019.
- [33] 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.
- [34] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, “Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks,” *IEEE Access*, vol. 6, pp. 2241–2250, 2018.
- [35] D. He, S. Zeadally, B. Xu, and X. Huang, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.