Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 3400558, 16 pages
https://doi.org/10.1155/2021/3400558

Research Article

Secure Message Transmission for V2V Based on Mutual Authentication for VANETs

Jabar Mahmood,[1] **Zongtao Duan**,[1] **Heng Xue**,[1] **Yun Yang**,[1] **Michael Abebe Berwo**,[1] **Sajjad Ahmad Khan**,[2] **and Abd al Kader Ahmed Yassin**[3]

[1]*School of Information and Engineering, Chang'an University, Xi'an 710064, China*
[2]*Department of Computer Engineering, Istanbul Gelisim University (IGU), 34310 Istanbul, Turkey*
[3]*Hatay Mustafa Kemal University (MKU) Turkish-Hatay/Hassa-MYO Girne, 79. Sk., 31700, Turkey*

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

Received 25 September 2021; Revised 22 October 2021; Accepted 27 October 2021; Published 23 November 2021

Academic Editor: Muhammad Asghar Khan

Copyright © 2021 Jabar Mahmood 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.

The advancements in Vehicular Ad Hoc Networks (VANETs) require more intelligent security protocols that ultimately provide unbreakable security to vehicles and other components of VANETs. VANETs face various types of security pitfalls due to the openness characteristics of the VANET communication infrastructure. Researchers have recently proposed different mutual authentication schemes that address security and privacy issues in vehicle-to-vehicle (V2V) communication. However, some V2V security schemes suffer from inadequate design and are hard to implement practically. In addition, some schemes face vehicle traceability and lack anonymity. Hence, this paper's primary goal is to enhance privacy preservation through mutual authentication and to achieve better security and performance. Therefore, this article first describes the vulnerabilities of a very recent authentication scheme presented by Vasudev et al. Our analysis proves that the design of Vasudev et al.'s scheme is incorrect, and resultantly, the scheme does not provide mutual authentication between a vehicle and vehicle server when multiple vehicles are registered with the vehicle sever. Furthermore, this paper proposes a secure message transmission scheme for V2V in VANETs. The proposed scheme fulfills the security and performance requirements of VANETs. The security analysis of the proposed scheme using formal BAN and informal discussion on security features confirm that the proposed scheme fulfills the security requirements, and the performance comparisons show that the proposed scheme copes with the lightweightness requirements of VANETs.

1. Introduction

Recently, the use of transportation has increased in every aspect of our lives. Vehicles are used not only for traveling but also in various smart city applications (such as traffic lights, cameras, and street lights) [1]. Urban transportation faces various challenges such as traffic issues, parking challenges, poor connectivity, inefficient road safety, and traffic jamming [2]. Intelligent Transportation System (ITS) [3, 4] provides solutions to previously mentioned challenges in urban transportation [5].

Vehicular Ad Hoc Networks (VANETs) [6–9] play a vital role in the urban transportation system; they help to improve road safety and traffic management. VANETs communicate with various elements such as vehicles, Roadside Units (RSUs) [10–12], Onboard Wireless Units (OBUs), internet/network, and vehicle servers/vehicle authentication servers. Based on these elements, communication is divided into two categories, V2V and Vehicle to RSUs (V2R/V2I). V2V communicate through the Dedicated Short-Range Communication (DSRC) protocol [13], which is included in IEEE 802.11p [14, 15]. Figure 1 shows the VANET architecture.

The OBU is fixed inside the vehicle and integrated with a Global Positioning System (GPS), ITS-G5 IEEE 802.11p protocol, and various sensors [13]. The OBU function stores information such as vehicle location, speed, and traffic flow on the road during driving and permits disseminating the information to RSUs or other vehicles on the road. The RSUs are fixed on the road edges; RSUs collect all

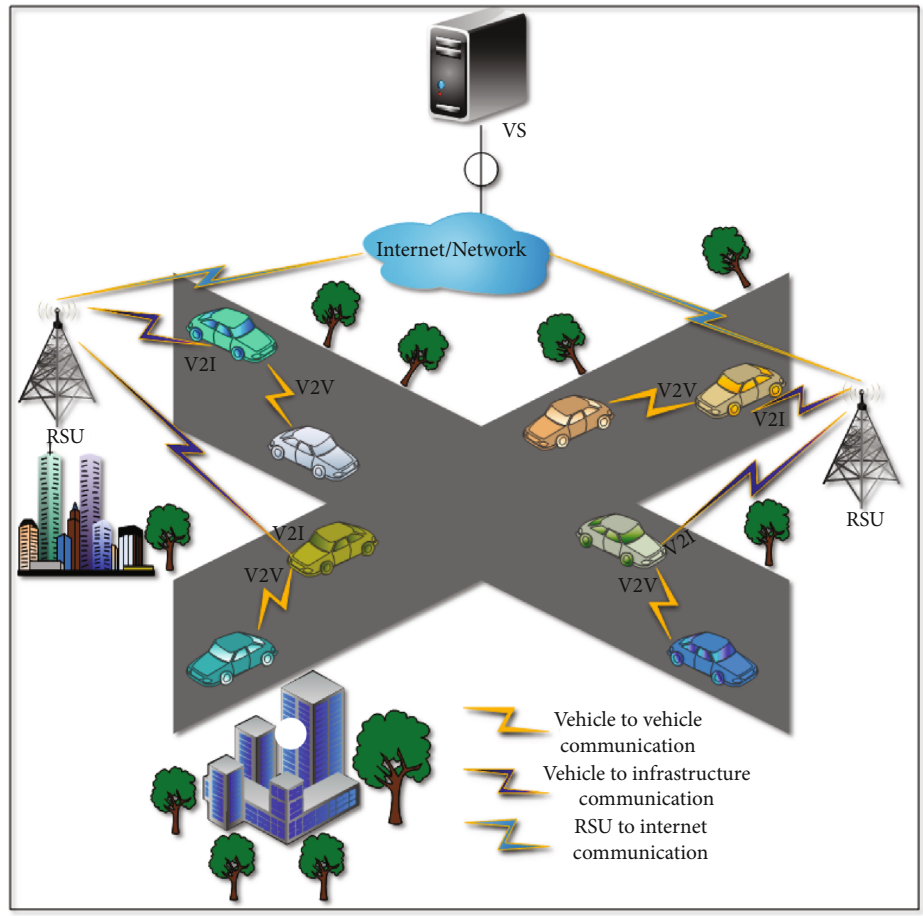

Figure 1: Structure of VANETs.

information from the vehicles/OBUs, save it, forward it to vehicles, and connect other RSUs for the network's security. That information is passed through a reliable communication channel from RSUs to OBUs and RSUs to RSUs. A vehicle server or vehicle authentication server ensures that all vehicles are trusted in-network and checks the vehicle ID and password when entering the network. If the vehicle fails to prove identity, an alert message is sent in the network through RSUs about a fake vehicle. Figure 2 provides complete details about V2V communication in VANETs. Usually, vehicles communicate with other vehicles, share information/data about the vehicle's current position, and share the keys. These data are confidential and sent through a secure communication channel with trusted vehicles part of the network. If confidential information is available, the adversary can use it in a way that is dangerous to vehicles and humans. In such a case, the adversary/attacker quickly gets a transmitted message and uses its advantages, such as altering the message and changing it according to its benefits or delaying the transmitted message making it unavailable to the original vehicle or devices within a specific time limit [16].

1.1. Motivation and Contributions. We observed that VANETs face various threats during communication, such as internal and external threats, as discussed previously. Every attacker hits the data packets, aiming to disturb the network and use its benefits. Due to these situations, we need a suitable protocol that provides strong user authentication and secures the data packet from attackers in V2V. This paper is aimed at analyzing the recent scheme, "A Lightweight Mutual Authentication Protocol V2V Communication on Internet of Vehicles," proposed by Vasudev et al. to present vital design faults. Specifically, LAMP-V2VCIoV cannot work when more than one registered vehicles are in the system. The working of LAMP-V2VCIoV can only be apprehended when there is only one vehicle registered. Moreover, this paper introduces a mutual authentication protocol for V2V communication in the VANETs (MAP-V2VCV). MAP-V2VCV is designed vigilantly to prevent any such incorrectness and provide an enhanced and secure message exchange.

The structure of the paper is organized as follows. The system model of the proposed scheme is presented in Section 2. The related works that have been done in recent years are presented in Section 3. In Section 4, we review Vasudev et al.'s authentication scheme. Section 5 points out the weakness of existing security scheme vulnerabilities. We propose a new and improved scheme in Section 6, while Section 7 describes the security analysis of the new scheme. Section 8 presents the security and performance analysis. At last, in Section 9, we provide the conclusion of the paper.

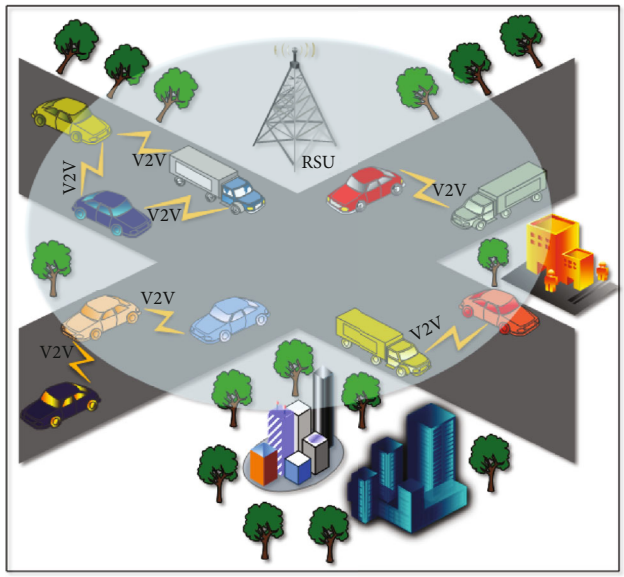

Figure 2: Typical structure of V2V communication.

2. System Models

This section presents the network and attack models and describes the working of both models on the contributed scheme.

2.1. Network Model. The network model is based on five entities, the vehicle/OBU, the RSU, registration authority (*RA*), trusted authority (*TA*), and vehicle server (*VS*); as shown in Figure 3, we describe each entity in detail.

The vehicle/OBU: an OBU installed inside each vehicle that receives messages from other vehicles/RSU/sensor verifies these messages and transmits them to other vehicles through the DSRC protocol. The secret information related to the message is kept secret in a tamper-proof device (TPD) inside the OBU. Every OBU in VANETs has a clock synchronized with the RSU communication range, also equipped with GPS and GUI interface that provide services such as the vehicle's location, the interaction of drivers to each other, and traffic information. Its computational power and storage capacity are more petite than RSU.

The RSU: the RSU is fixed on roadsides that acts as an intermediate entity between vehicles, *RA*, *TA*, and *VS*. The RSU is responsible for sharing traffic congestion, speed limits, and any threat information on the road. The RSU receives messages from the vehicle or RSUs, authenticates these messages, and then broadcasts these messages to other entities such as *VS*, via the secure communication channel.

Registration authority: in VANETs, *RA* is a trusted point to perform the registration procedure of every vehicle; this process is mandatory for each vehicle before moving to the communication phase. Generally, at the time of manufacture, the manufacturing company does this process; during the registration phase, vehicle users select required credentials, generate a key, and send some other information to *R A* for the registration. In the end, *RA*installs the OBU with the necessary parameters into the vehicle.

Trusted authority: *TA* is responsible for an authentication process that makes sure that the vehicle is trusted or authenticated and already registered with *RA*. *TA* first registers RSU and after that the vehicle and then generates anonymous identities to secure the privacy of the vehicle. *TA* also has the authority to identify the misbehaved vehicle's original identity and block it in the VANET network and inform other vehicles about that vehicle.

Vehicle server: the *VS* stores real-time information if any vehicle is requested to *VS* for the information that *VS* provides. When the vehicle wants that information, it first needs to register itself with the*TA*. If *TA* ensures the given vehicle is trusted, then credentials are sent to*VS*; after receiving this information from the trusted authority, the*VS*verifies that information again, and to ensure such information from*TA*,*VS*send some messages to*TA*; the purpose of this process is only for authenticity. After*TA*and*VS*, communication starts.

2.2. Attack Model. We choose the well-known Dolev-Yao threat model [17] for the security analysis of the proposed model. The Dolev-Yao threat model assumes and ensures a public channel for communication between vehicle to vehicle. A variety of proposals have been employed [18–21]; important points regarding the adopted attack model are given as follows:

(1) The attacker (*E*) properly controls the public channel. *E* is considered competent enough to listen, modify, delete, or jam any transmitted message between entities such as V_i, *TA*, and *VS*

(2) *E* can extract and analyze the parameter stored in a stolen smart card or capture the card's memory

(3) The vehicle and other entity are not trusted, which means any communicating authority or entity can try to impersonate on behalf of the other

(4) All parameters such as identities and the public keys of all the entities, including *TA*, are easily accessible to other systems and unauthorized users

(5) Private key (*PK*) of the participating entities, including *TA*, are secure and safe; no *E* is powerful enough to reveal the *PK* of any system entity

3. Related Work

The nature of VANETs is dynamic due to the Wireless Medium (WM) because of data transmission through WM to V2V, RSUs2V. Therefore, the chances of an attack are possible in the network every time. When attackers attack in the network during data transmission, stop, or delays, the original message can be tampered or discarded during this period [22]. A tampered or wrong message in VANETs becomes the reason for accidents or jamming of traffic. Xu et al. [22] proposed a security scheme to reduce the computation and storage cost and provide authentication to dense environments where vehicles receive multiple messages simultaneously, as well as to resist against the various attacks

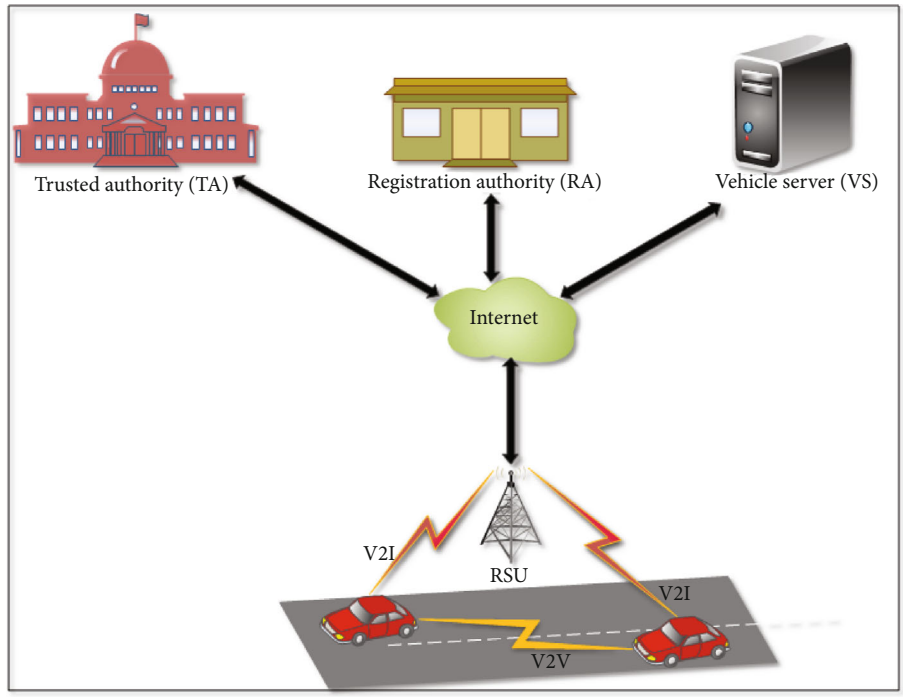

Figure 3: Network model of VANETs.

such as impersonation, modification, and replay attacks; however, the security analysis is not provided against remaining internal and external assaults [22].

VANET message transmissions from V2V or V2RSUs have many security threats. Vijayakumar et al. [23] proposed a dual authentication (DA) scheme that provides a high level of security to the vehicle inside the network and does not allow the entrance of any unauthorized vehicle in VANETS. It also provides a dual key management (DKM) security scheme for the user when joining or leaving which must be updated in the group. Nevertheless, the privacy of the vehicle's location is not provided in this scheme.

VANETs face various challenges due to dynamic topological conditions owing to speedily moving vehicles. Transmission of messages is in a limited area in VANETs, but security threats exist. Check of the authenticity of the message origin to the receiver in this environment is a big challenge. Chuang and Lee proposed a V2V communication security scheme called trust-extended authentication mechanism (TEAM) [24]. During analysis, Kumari et al. [25] find that TEAM is vulnerable to inside attacks, privacy breaches, impersonation attacks, and other challenges. Kumari et al. [25] proposed an enhanced trust extended authentication (ETEA) scheme for VANETs. ETEA proves that the analysis is better than TEAM and protects it from inside attacks. Also, computation load was reduced as compared to TEAM. Nevertheless, computational and storage cost is not discussed.

Various security protocols have been proposed for road safety applications in vehicle-to-everything (V2X) communication. These security protocols did not meet the lightweight (LW) preliminary requirements and fast processing integral parts of V2X; Hakeem et al. [26] proposed an LW authentication protocol for the privacy and protection of V2X. The protocol integrates with two hardware devices, biometrics devices and temper proof devices installed inside the vehicle. The proposed protocol is responsible for providing driver identity and private key security management. Decentralized certificateless authority generates a pseudoidentity of the driver, private key, secure privacy, and authentication V2V communication. They have also proposed an authentication signature protocol using the notation hash function. In [26], the scheme satisfies the security requirements and also reduces the message communication cost and computation time. Protection is provided against DoS, man-in-the-middle, modification, and replay assaults. However, storage cost was missing.

Chaudhry [27] states that the Internet of Vehicles (IoV) has become an integral part of our lives due to technological enhancement. Information is relevant to vehicles, including the position of the vehicle, information on the road, and the vehicle speed. This information is vital for selecting routes; without security, disseminating information between IoV entities is impossible. Many researchers proposed authentication schemes, but most security schemes did not perform as per claimed or communication cost or computation cost is very high. The authors in [27] proposed a secure message authentication protocol (SMEP-IoV); this protocol uses the symmetric lightweight hash function and encryption operation and provides a lightweight authentication process in 0.198 ms. SMEP-IoV resists various attacks such as stolen verifier, denial of service, replay, RSU impersonation, mutual authentication, and session key security. However, storage cost of the proposed is missing in their paper.

Recently, data transmission and protection of the user from various security attacks, the user authentication

protocol plays an integral role in ensuring security. Wang et al. [28] discovered two authentication security schemes that are not fully claimed and fail to provide secure communication, such as password guessing, session key disclosure, impersonation assaults, and user anonymity. In [28] eliminated the security threats from the existing scheme. The proposed improved authentication scheme based on the elliptic curve cryptosystem, performing analysis, proves that security scheme in [28] was better than existing schemes in terms of security, computation cost, and communication cost. However, storage cost was missing; also DoS and Sybil assaults were missing in the formal analysis.

In VANET, secure communication among neighbors, authentication, and trust establishment is an essential requirement of VANET. Many researchers proposed cryptography schemes that are claimed to overcome the inside assaults. However, they do not perform as per expectations. To reduce the inside attacks, researcher proposed a trust management scheme. Tangade and Manvi [29] proposed a neighbor trust management scheme (NTMS) for secure communication in VANET. NTMS employs an ID-based signature and HMAC [30]. NTMS provides various types of security during communication detection of malicious vehicles, the integrity of the message, and the level of trust among communication vehicles. However, formal security analysis was not provided, and also, computation cost and communication cost were missing.

Currently, the advancement of technologies has become a digital world, sharing information is not an issue. Hence, information must be secured; otherwise, the attacker may attack the information and use it for their own benefits and purposes. VANETs have become a more popular industry because vehicles share information among other vehicles speedily on the road. Limbasiya and Das [16] proposed a secure message exchange protocol using a public private key encryption and decryption approach in the computation of messages. In [16], the algorithm fulfills all security requirements on confidentiality, authenticity, and availability. This protocol also sends the current position of the vehicle to other vehicles within the network area. However, neither is formal security analysis provided nor are computation and communication costs discussed.

Vehicular sensor networks (VSNs) play a vital role in ITS and provide good driving experience, due to characteristics of VANETs facing different security threats. Researchers have proposed various authentication security schemes inappropriate to VSN applications due to high communication costs and high computation. Zhou et al. [30] improved the Chuang and Lee security scheme and eliminated the weakness of TEAM [24]. In [30], analysis was performed through the random oracle model and proved that this scheme was better than TEAM. Wu et al. [31] prove that Zhou et al. fail to provide identity guessing, impersonation assaults, and user anonymity and do not discuss DoS and Sybil attacks. Also, storage cost was missing.

For the last two decades, the mobile auto industry has been booming due to ITS, particularly the development of VANETs. It provides safety to the driver and passenger and a good experience. In VANETs, the mobility of vehicles is fast; due to this reason, privacy and security were a significant threat. Researchers have proposed an identity-based security scheme to overcome this issue but failed to provide the claimed solution. Wu et al. [31] improved Zhou et al.'s [30] scheme that failed to prove identity guessing and impersonation attack using elliptic curve encryption technology. Wu et al. [31] have proposed a new security scheme, V2V secure communication. However, computation cost and storage cost are missing. Table 1 provides the bird's eye view of the previous related works such as cryptography techniques, and their advantages and disadvantages/weaknesses are listed.

4. Summary of Vasudev et al.'s Authentication Scheme

This section provides a brief review of the scheme of Vasudev et al. [2]. The scheme is divided into four phases, and four entities are involved in these phases. First of all, we explain the entities and then the phases. The first entity vehicle V_i acts as a vehicle/user or node that wants to communicate with other vehicles or RSUs. Secondly, the registration authority (RA) is responsible for registering all vehicles; without RA registration, the vehicle cannot participate in VANET communication. The third entity is the trusted authority (TA), responsible for authentication between vehicle to vehicle and vehicle to a server. The fourth entity is the vehicle server (VS) that stores information about the network, such as vehicle position, weather condition, and congestion control. These four entities performed activity in four phases such as (1) registration, (2) login, (3) authentication, and (4) communication phases. For better understanding, the notations are given in Table 2.

4.1. Vehicle Registration. The vehicle driver/host (D_i) selects a vehicle ID and password (ID_i, PW_i) with random nonce Y_i. The V_i computes a cloaked ID and password such as $DVID_i = h(VID_i \| Y_i)$, $DPW_i = hh(PW_i \| Y_i)$ and sends to the registration authority through a secure channel. A secure channel means that the channel must ensure the integrity and confidentiality of information transferred via the channel. A secure channel is created using various cryptography security protocols such as SSH or TLS, or data or information is shared with the trusted user.

After receiving the data from a vehicle, RA calculates two parameters a_1 and b_1, which are unique for every vehicle or user. The value of a_1 is calculated such as $a_1 = h(DVID_i \| K_s)$, K_s is a private key that is shared by TA, and $b_1 = a_1 \oplus h(DVID_i \| DPW_i)$. The registration authority stores a_1 and b_1 parameters in SC and forwards to TA immediately. After receiving SC, it is sent to the driver/user via a secure channel.

After receiving the SC, $D_i$again computes the parameter C_i such as $C_i = VID_i \oplus PW_i \oplus Y_i$. Then, D_i stores the C_i and SC parameters for future communication.

4.2. Vasudev et al.'s Login, Authentication, and Communication. When a vehicle/user is registered successfully at RA, it must be logged in and authenticate itself with a trusted authority if D_i gets some information from the

Table 1: Summary of previous authentication schemes.

Paper	Cryptography technique	Advantage	Disadvantage
Xu et al. [22]	One-way hash function h(.) XOR (MD5)	Achieve lightweight certification; reduce storage and computation cost; less storage space; resist against impersonation, modification, and replay assaults	Does not resist reaming internal and external assaults such as DoS and man-in-the-middle, respectively
Vijayakumar et al. [23]	Hash code Finger print	Provide security to the vehicle and preventing unauthorized users, DKM for the user; unauthorized user does not enter the network; resist against replay, masquerading, Sybil, and message alteration assaults	Does not protect the vehicle location privacy
Kumari et al. [25]	One-way hash function XOR operation	Fast authentication process; low computational load; protect against impersonation, stolen verifier, modification, replay, and insider assaults	Computation cost and storage costs are missing
Hakeem et al. [26]	Hash chain key generation Elliptic curve	Enhances security level to protect anonymous identities; 20% ~ 85% communication overhead is compared to previous protocols; reduces the message communication cost and computation time; protects DoS, man-in-the-middle, modification, and replay assaults	Storage cost is missing
Chaudhry [27]	Symmetric lightweight hash functions and encryption	Provides sufficient security; provide SEMP-IoV best security requirement of the fast mobility vehicle IoV scenario; protects stolen verifier, denial of services, replay, RSU impersonation, mutual authentication, and session key security; authentication process takes 0.198 ms	Storage cost is missing
Wang et al. [28]	Elliptic curve cryptosystem	Protects session key exposure, forward scary assaults; low computation cost	Storage cost is missing; DoS and Sybil assaults were missing in formal analysis
Tangade and Manvi [29]	ID-based signatures HMAC techniques	Detection of malicious nodes; the integrity of the message is maintained; the proposed protocol fulfills the security requirements such as confidentiality, authenticity, and availability	Does not provide formal security analysis and lacks explanation of computation and communication costs
Limbasiya and Das [16]	One-way hash functions Bitwise XOR operation Low-cost cryptographic functions	Protects various assaults such as modification assault, man-in-the-middle assault, impersonation assault, concatenation, replay assault, stolen OBU, and password guessing assault	Formal security analysis is missing; computation cost and communication costs are missing
Zhou et al. [30]	Elliptic curve discrete logarithm problem	Resists internal assaults; low computation cost; secures the identity of driver and location privacy, and only authentication users get it	Storage cost is missing; does not discuss DoS and Sybil attacks
Wu et al. [31]	Hash functions XOR operation Elliptic curve encryption	Improves weaknesses of Zhou et al.'s security scheme such as guessing assaults and impersonation assaults	Computation and storages cost are missing

vehicle server. The purpose of authentication is to ensure D_i validity and protect impersonation assault from third-party vehicles or devices. The authentication process is also mandatory to verify that VS is not impersonated and that the vehicle gets accurate information. For normal execution of this phase, Figure 4 explains the process of login, authentication, and communication. The processes are described as follows.

4.2.1. Step VA1: $V_i \longrightarrow TA : \{MSG_1, X_1, T_u, SID\}$. Two parameters are required for login. The first one is the vehicle's identification number, and the second one is the password. It is not possible to login without these parameters. The vehicle computes the value of b_1, which is received from RA to cross-verify VID_i and PW_i. The vehicles (V_i) produce a nonce N_u and current timestamp T_u. Next, the vehicle computes three parameters such as MSG_1, Z_1, and X_1 for the communication with TA, $MSG_1 = h(a_1 \| T_u \| DPW_i \| N_u)$, $Z_1 = h(b_1 \| DPW_i)$, and $X_1 = N_u \oplus Z_1$, which are used for authentication of D_i. After that, the (MSG_1, X_1, T_u, SID) are sent to TA through an insecure channel.

4.2.2. Step VA2: $TA \longrightarrow VS : \{MSG_2, X_2, T_c, DCID\}$. When TA receives a message from the vehicle, the (MSG_1, X_1, T_u, SID) calculates the Z_1 and X_1 such as $Z_1^* = h(b_1 \| DPW_i)$ and $N_u^* = X_1 \oplus Z_1$. Also, it computes MSG_1

Table 2: Notation guide.

Notation symbols	Detail of notations
VS, D_i	Vehicle server, vehicle/host
VID_i	Identification number of the i^{th} vehicle
PW_i	The password of i^{th} vehicle
RA, TA	Registration authority, trusted authority
CID	The identification number of TA
SID_k	The identification number of $k^{th} VS$
Y_i	Random number (RN) generate vehicle
K_s	Secret key shared between VS and TA
N_{u_i}	Nonce produced by VID_i
N_{s_k}	Nonce produced by SID_k
N_s	Nonce produced by VS
Y_{ta}	Random number produced by RA
T_u, T_c, T_s	Timestamp of V_i, TA, VS
$EVID_i$	Pseudo identity of vehicle
E_{k_s}	Encryption using K_s
D_{k_s}	Decryption using K_s
$h(.)$	One-way cryptography hash function
$\oplus$	XOR operation
$\|\|$	Concatenation operation

$=^{?} h(a_1 \| T_u \| DPW_i \| N_u^*)$ to verify the same message which is received through an insecure channel from the vehicle. After calculation, the received information also ensures the integrity of the received message. The TA calculates $DCID$ such as $DCID = h(DVID_i \| CID \| SID)$. After that, it computes MSG_2 and X_2 as $MSG_2 = h(DCID \| K_s \| T_c \| N_u)$ and $X_2 = N_u \oplus h(K_s)$, respectively. T_c represents the timestamp that generated TAat the time when the message was computed. Finally, the $(MSG_2, X_2, T_c, DCID)$ is sent to the vehicle sever.

4.2.3. Step VA3: $VS \longrightarrow TA : \{MSG_3, X_3, T_s\}$. After receiving the information fromTA, $(MSG_2, X_2, T_c, DCID)$ calculates the information to verify whether it is correct or not, such as$N_u^* = X_2 \oplus h(K_s)$,$MSG_2 =^{?} h(DCID \| K_s \| T_c \| N_u^*)$. The VS produces random nonce N_s and timestamp T_s. The VS also generates secret key S_k, $S_k = h(DCID \| N_s \| N_u)$, that is shared with the vehicle for future communication. The VS also computes $X_3 = h(N_u \| N_s \| T_s \| K_s)$ and $MSG_3 = N_s \oplus N_u$; these parameters are $(MSG3, X_3, T_s)$ sent back to TA.

4.2.4. Step VA4: $TA \longrightarrow V_i : \{X_4, W\}$. At this phase, the trusted authority calculates the MSG_3 and X_3 as $N_s^* = MSG_3 \oplus N_u$, $X_3 =^{?} h(N_u \| N_s^* \| T_s \| K_s)$. After verification of information, TA computes $W = N_s \oplus DPW_i$, $X_4 = h(N_u \| N_s \| DPW_i)$ and sends (X_4, w) to the vehicle/user. The vehicle computes W and X_4 such as $N_s^* = W \oplus DWP_i$, $X_4 =^{?} h(N_u \| N_s^* \| DPW_i)$; after that, the secret key $S_k = h(DCID \| N_s \| N_u)$ is calculated.

4.2.5. Step VA5: Communication. The secret key S_k is used for V2V communication in the future. The vehicle server stores the vehicle/host identity and key after this communication. If vehicle A wants to communicate with other vehicles or devices, the message is encrypted with the help of a key and sent. After receiving a message from vehicle A, vehicle B sends it to VS to check the identity of vehicle A. The VS checks the legitimacy of vehicle B and vehicle A. If VS ensures that both are authorized vehicles, then the keys are sent to vehicle A and vehicle B through a secure channel. Then, vehicle B decrypts the request using this key that is received from VS.

5. Weaknesses of Vasudev et al.'s Scheme

This section highlights the weaknesses of Vasudev et al.'s scheme. The following subsections present the security scheme proposed in [2]. The scheme has some flaws and does not provide anonymity. The authenticated vehicle sends a request to TA for login approval through an insecure channel and also sends parameters $\{MSG_1, X_1, T_u, SID\}$. The TA does not recognize the specific identity of the vehicle where further communication is not possible between vehicles, TA and VS. To better understand Vasudev et al.'s scheme on that basis, the details of the scheme's incorrectness are mentioned below.

(1) V_i calculates following parameters after completing the login phase:

$$\begin{aligned} MSG_1 &= h(a_1 \| T_u \| DPW_i \| N_u), \\ Z_1 &= h(b_1 \| DPW_i), \\ X_1 &= N_u \oplus Z_1. \end{aligned} \tag{1}$$

V_i send $\{MSG_1, X_1, T_u, SID\}$

(2) After verifying the correctness of T_u, TA calculates the following:

$$Z_1^* = h(b_1 \| DPW_i), \tag{2}$$

$$N_u^* = X_1 \oplus Z_1^*, \tag{3}$$

$$MSG_1 \stackrel{?}{=} h(a_1 \| T_u \| DPW_i \| N_u^*). \tag{4}$$

(3) TA calculates Z_1 through Equation (2), where TA requires $h(b_1 \| DPW_i)$. TA receives the T_u and maintains the database that contains the records in the form of tuple$\{a_1, b_1\}$. Therefore, to extract $h(b_1 \| DPW_i)$, TA needs to know the $DVID_i$. Nevertheless, TA does not know about the identity of the vehicle. Moreover, to calculate N_u^* through Equation (3), it needs the value of Z_1^*; that is not possible because several vehicles send requests to TA at the same time where every vehicle has its own parameter values such as a_1, b_1, Z_i.

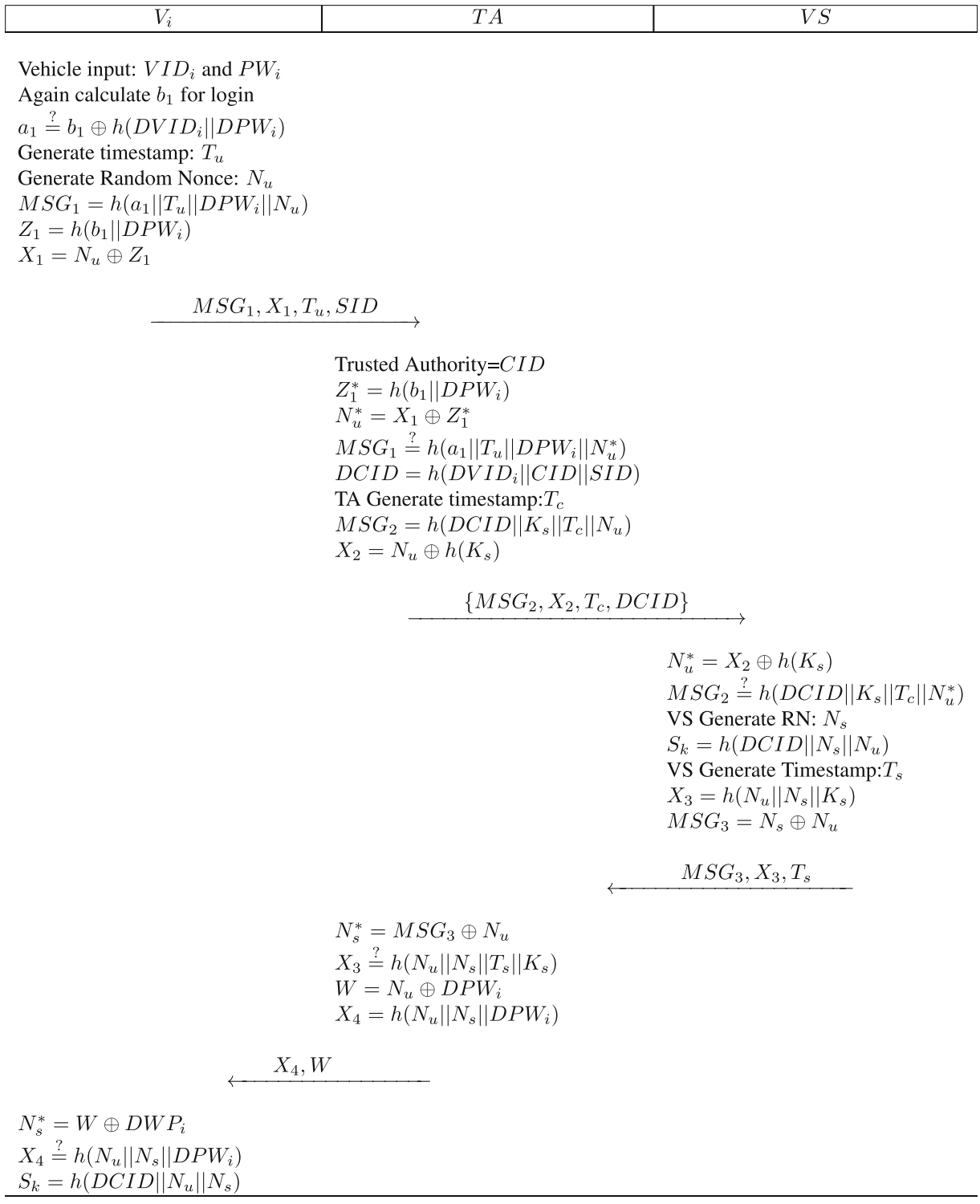

FIGURE 4: Vasudev et al.'s scheme.

Therefore, it is not possible for TA to identify the vehicle identity because TA does not know about Z_i. Similarly, in order to compute the originality of the message, Equation (4) needs the value of Z_1^*. So, TA does not calculate any parameters, and the authentication process may be suspended, irrespectively

(4) Similarly, the reply message from TA sends $\{X_4, W\}$ to the requesting vehicleV_i, without recognizing $V_i$as the information of the requesting vehicle is unknown for TA. Moreover, the message $\{MSG_2, X_2, T_c, DCID\}$ from TA to VS has not carried information about V_i; rather, TA itself is not able to recognize the

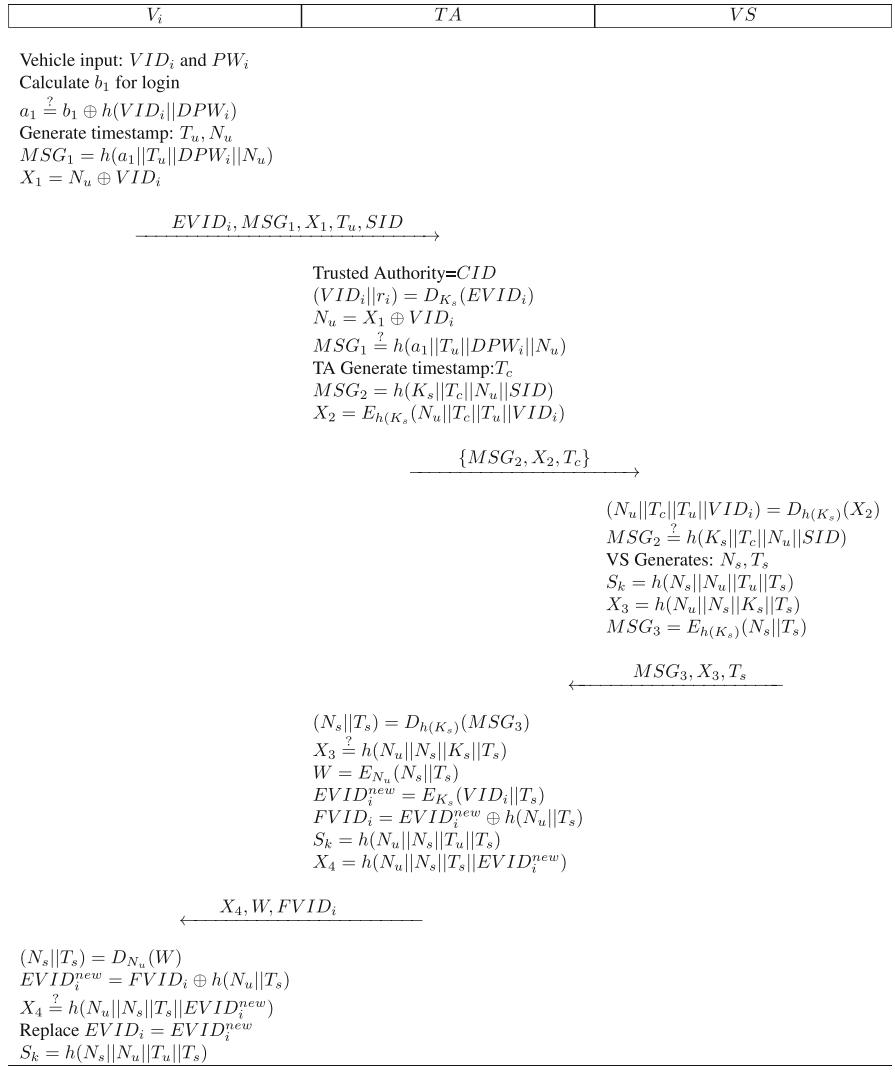

Figure 5: Proposed scheme.

identity of specific vehicles. Hence, TA does not send any message to V_i. Thus, this scheme is incorrect.

6. Proposed Scheme

In the following subsections, the main phases of the proposed scheme are explained:

6.1. Vehicle Registration. The driver of the vehicle/host (D_i) selects a vehicle ID and password (VID_i, PW_i) with random nonce Y_i. The V_i computes $DPW_i = h(PW_i \| Y_i)$ and sends $\{VID_i, DPW_i\}$ to the registration authority through a secure channel. After receiving data from the vehicle, RA generates $Y_{ta} \in Z_p^*$ and calculates the following parameters: a_1, b_1, and $EVID_i$, which are unique for every vehicle or user, where $a_1 = h(VID_i \| K_s)$, $b_1 = a_1 \oplus h(VID_i \| DPW_i)$, and $EVID_i = E_{K_s}(VID_i \| Y_{ta})$. The registration authority stores a_1, b_1, and $EVID_i$ in SC and immediately forwards to TA. After receiving SC, the information is sent to the driver/user via a secure channel.

When the SC information is received, D_i computes the parameter C_i as $C_i = VID_i \oplus PW_i \oplus Y_i$. Then, D_i stores C_i and SC parameters for future communication.

6.2. Proposed Login, Authentication, and Communication. When vehicles successfully register to the registration authority, they must be logged in and prove their authentication with a TA if the vehicle wants to obtain data from VS. The whole process is aimed at ensuring D_i validity and protecting against impersonation assaults from an intruder or third-party vehicle/device.

The authentication processes can also be done by the vehicle server to verify the impersonation of VS and send accurate information to the vehicle. Figure 5 describes the whole process of login, authentication, and communication. The explanation is given as follows.

6.2.1. Step PA1: $V_i \longrightarrow TA : \{EVID_i, MSG_1, X_1, T_u, SID\}$. Two parameters are required for the login process, i.e., the vehicle's identification number and the password. Login is not possible without these two parameters. After login, the

vehicle computes the value of b_1 which is received from RA to cross-verify VID_i and PW_i. The vehicle (V_i) produces a nonce N_u and current timestamp T_u. Then, the vehicle computes the other two parameters MSG_1 and X_1 for the communication with TA, $MSG_1 = h(a_1 \| T_u \| DPW_i \| N_u)$ and $X_1 = N_u \oplus VID_i$, respectively, which are used for authentication of D_i. After that, $(EVID_i, MSG_1, X_1, T_u, SID)$ sends the information to the TAthrough an insecure channel.

6.2.2. Step PA2: $TA \longrightarrow VS : \{MSG_2, X_2, T_c\}$. When TA receives a message from vehicle $(EVID_i, MSG_1, X_1, T_u, SID)$ to calculate the $EVID_i$, MSG_1, and X_1 such as $(VID_i \| r_i) = D_{K_s}(EVID_i)$, $MSG_1 = ^{?} h(a_1 \| T_u \| DPW_i \| N_u)$ also computes $N_u = X_1 \oplus VID_i$ to confirm the same message received on the channel from the vehicle. The above calculation ensures the integrity of the received message. The TA calculates MSG_2 and X_2 as $MSG_2 = h(K_s \| T_c \| N_u \| SID)$ and $X_2 = E_{h(K_s}(N_u \| T_c \| T_u \| VID_i)$, respectively. T_c represents the timestamp that is generated from T_A at the time when the message was computed. Finally, (MSG_2, X_2, T_c) is sent to the vehicle sever.

6.2.3. Step PA3: $VS \longrightarrow TA : \{MSG_3, X_3, T_s\}$. After receiving the information from TA in which (MSG_2, X_2, T_c), VS calculates the information to verify whether it is correct or not, such as $(N_u \| T_c \| T_u \| VID_i) = D_{h(K_s)}(X_2)$ and $MSG_2 = ^{?} h(K_s \| T_c \| N_u \| SID)$. The VS produces random nonce N_s and timestamp T_s. The VS also generates a secret key S_k, $S_k = h(N_s \| N_u \| T_u \| T_s)$, that is shared with the vehicle for future communication. The VS also computes $X_3 = h(N_u \| N_s \| K_s \| T_s)$ and $MSG_3 = E_{h(K_s)}(N_s \| T_s)$; these parameters $(MSG3, X_3, T_s)$ are sent back to TA.

6.2.4. Step PA4: $TA \longrightarrow V_i : \{X_4, W, FVID_i\}$. The trusted authority calculated MSG_3 and X_3 such as $(N_s \| T_s) = D_{h(K_s)}(MSG_3)$ and $X_3 = ^{?} h(N_u \| N_s \| K_s \| T_s)$. After verification of information, TA computes $W = E_{N_u}(N_s \| T_s)$, $EVID_i^{\text{new}} = E_{K_s}(VID_i \| T_s)$, $FVID_i = EVID_i^{\text{new}} \oplus h(N_u \| T_s)$, $S_k = h(N_u \| N_s \| T_u \| T_s)$, and $X_4 = h(N_u \| N_s \| T_s \| EVID_i^{\text{new}})$ to the vehicle/user.

The vehicle again computes W, X_4, and $FVID_i$ such as $(N_s \| T_s) = D_{N_u}(W)$, $EVID_i^{\text{new}} = FVID_i \oplus h(N_u \| T_s)$, and $X_4 = ^{?} h(N_u \| N_s \| T_s \| EVID_i^{\text{new}})$; after that, the $EVID_i$ is replaced with $EVID_i^{\text{new}}$ and the secret key $S_k = h(N_s \| N_u \| T_u \| T_s)$ is calculated.

6.2.5. Step PA5: Communication. The secret key S_k is used for V2V communication in the future. The vehicle server stores the vehicle/host identity and key after this communication. If vehicle A wants to communicate with other vehicles or devices, the message is encrypted with the help of a key and sent. After receiving a message from vehicle A, vehicle B sends it to VS to check the identity of vehicle A. The VS checks the legitimacy of vehicle B and vehicle A. If VS ensures that both are authorized vehicles, then a key is sent to vehicle A and vehicle B through a secure channel. Then, the vehicle B decrypts the request using this key which is received from VS.

7. Security Analysis

This section performs formal security analysis through the BAN-logic method and discusses how the proposed scheme protects it from various security attacks.

7.1. Formal Security Analysis through BAN-Logic. In this subsection, the detailed security analysis is provided of the proposed scheme using BAN-logic [35]. Firstly, some basic notations are presented that are used to analyze the proposed scheme. Here, the L and M are used as participators, and X is used as a formula.

(i) $(\#X)$: X is fresh

(ii) $L \mid \equiv X$: L believes the trustworthiness of X

(iii) $L \mid \sim X$: L once said X

(iv) $L \triangleleft X$: L sees X

(v) $L \mid X$: L has jurisdiction over X

(vi) $L \leftrightarrow^{K} M$: between L and M, K is shared key

(vii) $\{X, Y\}_k$: X and Y are encrypted with the help of K

(viii) $(X)_Y$:X combined with Y

The following BAN-logic rules are used to verify the security features:

(i) Rule 1: message meaning rule

If L sees a statement X encrypted with key K and L believes K is a shared secret key between L and M, then L believes M once said X.

$$\frac{L \mid \equiv \overset{K}{\leftrightarrow} M, L \triangleleft \{X\}_K}{L \mid \equiv M \mid \sim X}. \tag{5}$$

(ii) Rule 2: nonce verification rule

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

$$\frac{L \mid \equiv \#X, L \mid \equiv M \mid \sim X}{L \mid \equiv M \mid \equiv X}. \tag{6}$$

(iii) Rule 3: jurisdiction rule

If L believes M has jurisdiction over the statement X and L believes M is the statement X, then L believes the statement of X.

$$\frac{L \mid \equiv M \Rightarrow X, L \mid \equiv M \mid \equiv X}{L \mid \equiv X}. \tag{7}$$

(iv) Rule 4: freshness rule

If L believes that the part of the statement X is updated, then L believes that the statement $\{X, Y\}$ is updated.

$$\frac{L|\equiv\#(X)}{L|\equiv\#(X,Y)}. \tag{8}$$

(v) Rule 5: belief rule

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

$$\frac{L|\equiv M|\equiv\{X,Y\}}{L|\equiv M|\equiv X}. \tag{9}$$

The main goals of the proposed security scheme are proven under the BAN-logic analytic procedure:

(i) $G1: V_i \mid \equiv V_i \leftrightarrow^{S_K} TA$

(ii) $G2: V_i \mid \equiv TA \mid \equiv V_i \leftrightarrow^{S_K} TA$

(iii) $G3: TA \mid \equiv V_i \leftrightarrow^{S_K} TA$

(iv) $G4: TA \mid \equiv V_i \mid \equiv V_i \leftrightarrow^{S_K} TA$

(v) $G5: VS \mid \equiv VS \leftrightarrow^{S_K} TA$

(vi) $G6: VS|\equiv TA| \equiv VS \leftrightarrow^{S_K} TA$

(vii) $G7: TA \mid \equiv VS \leftrightarrow^{S_K} TA$

(viii) $G8: TA|\equiv VS| \equiv VS \leftrightarrow^{S_K} TA$

In the proposed scheme, when a message is sent over an unsafe communication channel, the details of the message are mentioned below:

(i) $M1: V_i \longrightarrow TA: EVID_i, MSG_1X_1, T_u, SID : \{N_u, EVID_i\}_{VID_i}$

(ii) $M2: TA \longrightarrow VS: MSG_2, X_2, T_c : \{h(K_s\|T_c\|N_u\|SID), N_u\}_{K_s}$

(iii) $M3: VS \longrightarrow TA: MSG_3, X_3, T_s : \{N_s\}_{k_s}$

(iv) $M4: TA \longrightarrow V_i: X_4, W, FVID_i : \{N_u, N_s\}_{VID_i}$

Furthermore, the following assumptions are given as proof of the proposed security scheme:

(i) $A1: TA \mid \equiv\#(N_u)$

(ii) $A2: TA \mid \equiv\#(N_s)$

(iii) $A3: VS \mid \equiv\#h(K_s\|T_c\|N_u\|SID)$

(iv) $A4: V_i \mid \equiv\#(N_u)$

(v) $A5: V_i \mid \equiv TA(V_i \leftrightarrow^{S_k} TA)$

(vi) $A6: TA \mid \equiv V_i(V_i \leftrightarrow^{S_k} TA)$

(vii) $A7: VS \mid \equiv TA(VS \leftrightarrow^{S_k} TA)$

(viii) $A8: TA \mid \equiv VS \mid (VS \leftrightarrow^{S_k} TA)$

(ix) $A9: V_i \mid \equiv V_i \leftrightarrow^{VID_i} TA$

(x) $A10: TA \mid \equiv V_i \leftrightarrow^{VID_i} TA$

(xi) $A11: VS \mid \equiv VS \leftrightarrow^{S_k} TA$

(xii) $A12: TA \mid \equiv VS \leftrightarrow^{S_k} TA$

(xiii) $A13: VS \mid \equiv TA \mid \sim h(K_s\|T_c\|N_u\|SID), N_u$

7.1.1. BAN-Logic Proof. The BAN-logic is conducted to analyze the proposed scheme:

Step 1. S_1 can be acquired from M_1.

$$S_1: TA \triangleleft \left\{N_u, EVID_{iVID_i}\right\}. \tag{10}$$

Step 2. S_2 can be persuaded by applying rule 1, using S_1 and A_{10}.

$$S_2: TA|\equiv V_i| \sim (N_u, EVID_i). \tag{11}$$

Step 3. S_3 can be persuaded by applying rule 4, using S_2 and A_1.

$$S_3: TA| \equiv \#(N_u, EVID_i). \tag{12}$$

Step 4. S_4 can be persuaded by applying rule 2, using S_2 and S_3.

$$S_4: TA|\equiv V_i| \equiv (N_u, EVID_i). \tag{13}$$

Step 5. S_5 can be persuaded by S_4 and applying rule 5

$$S_5: TA|\equiv V_i| \equiv (N_u). \tag{14}$$

Step 6. S_6 obtained from M_2.

$$S_6: VS \triangleleft \left\{h(K_s||T_c||N_u||SID)_{K_s}\right\}. \tag{15}$$

Step 7. S_7 can be persuaded by applying rule 1, using S_6 and A_{13}.

$$S_7: VS|\equiv TA| \sim h(K_s||T_c||N_u||SID). \tag{16}$$

Step 8. S_8 can be persuaded by applying rule 5, using S_7 and A_3.

$$S_8: VS| \equiv \#h(K_s||T_c||N_u||SID), N_u. \tag{17}$$

Step 9. S_9 can be persuaded by applying rule 2, using S_7 and S_8.

$$S_9: VS|\equiv TA| \equiv h(K_s||T_c||N_u||SID), N_u. \tag{18}$$

Step 10. S_{10} obtained from M_3.

$$S_1 0 : TA \triangleleft \{N_U\}_{S_k}. \tag{19}$$

Step 11. $S_1 1$ can be persuaded by applying rule 1, using A_5 and S_8.

$$S_{11} : TA| \equiv VS| \sim (N_s). \tag{20}$$

Step 12. S_{12} can be persuaded by applying rule 2, using S_9 and S_{10}.

$$S_{12} : TA| \equiv VS| \equiv (N_s). \tag{21}$$

Step 13. S_{13} can be persuaded by S_9 and S_{12}, VS. TA can be calculated by session key $S_k = h(N_s \| N_u \| T_u \| T_s)$.

$$\begin{aligned} S_{13} : TA| \equiv VS| &\equiv \left(VS \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G8), \\ S_{14} : VS| \equiv TA| &\equiv \left(VS \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G6). \end{aligned} \tag{22}$$

Step 14. S_{15} and S_{16} can be persuaded by applying rule 3, using S_{13} and A_8 and S_{14} and A_7.

$$\begin{aligned} S_{15} : TA| &\equiv \left(VS \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G7), \\ S_{16} : VS| &\equiv \left(VS \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G5). \end{aligned} \tag{23}$$

Step 15. S_{17} obtained from M_4.

$$S_{17} : V_i \triangleleft \{N_s, N_U\}_{VID_i}. \tag{24}$$

Step 16. S_{18} can be persuaded by applying rule 1, using A_9 and S_{17}.

$$S_{18} : V_i| \equiv TA| \sim (N_u, N_s). \tag{25}$$

Step 17. S_{19} can be persuaded by applying rule 5, using S_{18} and A_4.

$$S_{19} : V_i| \equiv \#(N_u, N_s). \tag{26}$$

Step 18. S_{20} can be persuaded by applying rule 2, using S_{16} and S_{17}.

$$S_{20} : V_i| \equiv TA| \equiv (N_u, N_s). \tag{27}$$

Step 19. S_{21} and S_{22} can be persuaded by S_5, S_{18}, and V_i. TA can be calculated by session key $S_k = h(N_s \| N_u \| T_u \| T_s)$.

$$\begin{aligned} S_{21} : V_i| \equiv TA| &\equiv \left(V_i \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G2), \\ S_{22} : TA| \equiv V_i| &\equiv \left(V_i \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G4). \end{aligned} \tag{28}$$

Step 20. S_{23} and S_{24} can be persuaded by applying rule 3, using S_{21}, A_5, S_{22}, and A_6.

$$\begin{aligned} S_{23} : V_i| &\equiv \left(V_i \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G1), \\ S_{24} : TA| &\equiv \left(V_i \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G3). \end{aligned} \tag{29}$$

7.2. Security Discussion. This subsection explains how the proposed security scheme can resist against various security attacks; details are given as follows.

7.2.1. Correctness. The proposed scheme completes the authentication process correctly between V_i and VS with the help of TA. The proposed scheme is designed and provides intuition to the common mistakes. It also provides supports for correctness issues in the future work. In the vehicle registration phase of the proposed scheme, a random and dynamic identity $EVID_i$ is generated by the RA and is stored in the memory of vehicle SC. This identity is used in the process of the login and authentication request on both SC in possession of the vehicle and TA. Furthermore, every vehicle has a different random number and unique identity. Thus, TA easily identifies the vehicle identity at the time of authentication when the vehicle requests TA for login. Therefore, the proposed scheme eliminates the correctness issues.

7.2.2. Impersonation Attack. Here, the defense of the proposed security scheme against the vehicle such as TA, and the VS impersonation assault are described.

(1) *Vehicle impersonation attack*: if E tries to launch the impersonation assault on the behalf of the vehicle, it needs to construct an original login request message M_1' such as $M_1' = MSG_1', EVID_i', T_u', X_1', SID'$, where $MSG_1' = h(a_1 \| T_u \| DPW_i \| N_u)$, $X_1' = N_u \oplus VID_i$, $EVID_i' = E_{K_s}(VID_i \| Y_{ta})$ with updated nonce N_u' and timestamp T_u'. However, it is seen at the start that it is very difficult to recover T_u, VID_i, and DWP_i for constructing $M' = MSG_1', EVID_i', T_u', X_1', SID'$. Thus, the proposed protocol provides security against the vehicle impersonation assault.

(2) *TA impersonation attack*: similarly, an E tries to instigate a forgery toward VS on the behalf of TA. For this purpose, E needs to construct the M_2' such as $M_2' = MSG_2, X_2$ with updated nonce N_u' and timestamp T_c' and also requires some confidential parameters such as T_c, N_u, T_u, and K_s secret keys. It is a computationally hard problem to compute these parameters from previously intercepted message MSG_2 and X_2. Thus, the proposed protocol also provides security against TA impersonation assault.

(3) *VS impersonation attack*: in the case of VS impersonation assault, when E launches an assault on VS toward TA, it also needs to design the message M_3'

with an updated nonce N_u' and new timestamp T_c', where $M_3' = MSG_3', X_3', T_s'$, $MSG_3' = E_h(N_s \| T_s)$, and $X_3' = h(N_u' \| N_s' \| K_s' \| T_s')$. However, the attacker may not be able to construct the valid message parameters in M_3', until granted the valid secret key K_s. Thus, E cannot impersonate the VS, and the proposed scheme provides security to VS impersonation assault.

7.2.3. Stolen SC Attack. Suppose if E steals the smart card and obtains all confidential credentials $\{a_1, b_1, EVID_i\}$ using a power analysis attack (PWA) [33]. E tries to compute MSG_1, X_1, and $EVID_i$. However, E requires the knowledge of $DPW_i = h(PW_i \| Y_i)$, whereas the E does not hold a hash function, which is not convertible. Thus, E cannot recover the password, and the stolen smart card cannot be accessible.

7.2.4. Session Key Security. The trusted authority and vehicle server both verify the value of nonce N_s, T_u, T_s, and N_u that are used to compute the secret key value $S_k = h(N_s \| N_u \| T_u \| T_s)$. This process ensures the originality of the session key. Thus, session key security is ensured.

7.2.5. Anonymity and Untraceability. In the phase of mutual authentication, the proposed security scheme utilizes random nonce N_u, r_i, and T_u, as well as timestamp T_u, T_c, and T_s in communication messages MSG_1–MSG_3. In the communication scenario, E may not differentiate among the messages of the different sessions, which publicly render the proposed scheme untraceable. At the same time, the E may not identify the vehicle identity, since the messages employ pseudoidentities, i.e., $EVID_i$, $EVID_i^{\text{new}}$, and $FVID_i$ and again replace $EVID_i^{\text{new}}$ into $EVID_i$ in the messages instead of original identities, that are enclosed under the rigidity of a one-way hash function-bearing collision resistance characteristic. Thus, the proposed scheme maintains the untraceability and anonymity characteristics.

7.2.6. Man-in-the-Middle Attack. If E want to launch the man-in-the-middle assault, it is required to build the message M' i.e., $M_1' = MSG_1, EVID_i, T_u, X_1, SID$ where $MSG_1 = h(a_1 \| T_u \| DPW_i \| N_u)$, $X_1 = N_u \oplus VID_i$, and $EVID_i = E_{K_s}(VID_i \| Y_{ta})$. However, to meet the goal, the attacker needs to build those message parameters with updated nonce N_u and timestamp T_u, which are not possible until E has access to K_s, $EVID_i$, and DPW_i. Likewise, E is not able to rebuild other messages such as MSG_1–MSG_3 in the protocol with updated nonce and timestamp without having access to important parameters in possession with those participating entities. Therefore, the proposed scheme provides security against the man-in-the-middle assault.

7.2.7. Off-Line Password Guessing Attack. It is proven that the proposed scheme is infeasible for E to get the identity of D_i, even after extracting the parameters. Suppose if E has access to a smart card, which contains $\{EVID_i, a_1, b_1, h(.), Y_i\}$, the parameters can be obtained by using the PWA [33]. However, assaults cannot compute the K_s and, ultimately, PW_i from DWP_i. The E has only one way to acquire the PW_i from MSG_1 without breaching the noninvertible characteristics of the cryptography hash function.

7.2.8. Replay Attack. In the proposed security scheme, various entities such as V_i, TA, and VS exchange the messages from MSG_1 to MSG_3 and utilize the timestamp T_u, T_c, and T_s to encounter the possible replay assault. At the same time, mutual authentication is required for communication. The messages need to be replied to in a short period of timestamp T to abolish the possibility of E manipulating the messages and initiating replay assault. Without updating the parameters MSG_1, X_1, $EVID_i$, MSG_2, X_2, MSG_3, X_3, W, X_4, and $FVID_i$, the updated timestamp cannot be utilized. At the same time, the parameters need to be updated with the new timestamp, whereas the E requires access to VID_i identity and password, and other shared parameters between V_i, TA, and VS. Thus, the replay assault does not happen in the proposed scheme.

7.2.9. Denial of Service (DoS) Attack. The proposed scheme provides security against DoS assault as the SC in the start authenticate V_i such as $EVID_i = H(VID_i \| Y_{ta})$. This condition will only be legal if V_i enters the correct identity VID_i and password DPW_i; after the insertion of the valid identity and password, the parameters are computed in SC $(VID_i \| Y_{ta}) = E_{ks}(EVID_i)$. The authentication of V_i is done locally at the vehicle's side. After that, a request is sent to TA for authentication. The same process is followed in the password and update phases to protect the incorrect modification of these parameters. Thus, the scheme prevents DoS assault.

8. Security and Performance Analysis

Under this section, the security features, computation cost, and communication cost of the proposed scheme with relation to other schemes are described [2, 25, 30, 34].

8.1. Security Features. Table 3 provides a detailed overview of security comparisons of our proposed scheme in relation to other schemes [2, 25, 30, 34]. In Table 3, the proposed scheme acquires the required attributes associated with pragmatic security under the DY model described in Section 2.2. At the same time, Vasudev et al.'s scheme [2] is incorrect and cannot fulfill the authentication as evinced in Section 5. In Vasudev et al.'s scheme [2], TA cannot identify the vehicle identity if more than one vehicle communicates to TA. This scheme also only works when one registered vehicle is in the system. Vasudev et al.'s scheme [2] is insecure against the man-in-the-middle attack. Additionally, the scheme of Mohit et al. [34] also failed to provide security against man-in-the-middle and DoS attacks. Kumari et al.'s scheme [25] is also insecure against the man-in-the-middle, offline password guessing, and DoS attacks. Zhou et al.'s scheme [30] failed to provide security against the impersonation attack such as (V_i, TA, VS) and is also insecure against the man-in-the-middle, offline password guessing, replay, and DoS attacks.

Table 3: Security analysis.

Schemes	Ours	[2]	[34]	[25]	[30]
Correctness	✓	✗	✓	✓	✓
Vehicle impersonation attack	✓	✓	✓	✓	✗
Trusted authority impersonation attack	✓	✓	✓	✓	✗
Vehicle server impersonation attack	✓	✓	✓	✓	✗
Stolen SC attack	✓	✓	✓	✓	✓
Anonymity attack	✓	✓	✓	✓	✓
Untraceability attack	✓	✓	✓	✓	✓
Man-in-the-middle attack	✓	✗	✗	✗	✗
Off-line password guessing attack	✓	✓	✓	✗	✗
Replay attack	✓	✓	✓	✓	✗
Mutual authentication	✓	✓	✓	✓	✓
DoS attack	✓	✓	✗	✗	✗

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

Table 4: Performance comparisons.

Scheme	Computation cost	RT (ms)	ME	BE	SC
Ours	$14T_h + 14T_{be}$	0.266	4	1824	512
Vasudev et al. [2]	$16T_h$	0.096	4	1696	384
Mohit et al. [34]	$19T_h$	0.114	4	1760	864
Kumari et al. [25]	$12T_h$	0.072	3	1056	608
Zhou et al. [30]	$16T_h$	0.096	3	1604	544

Note: RT: running time; ME: no. of message exchanges; BE: bit exchange: SC: storage cost in bits.

8.2. Computation Cost. We adopted the running times computed in [35] over a Pi-3:B+64-bit-Cortes A5-3:ARM-v8, SoC:1.4 GHz processor, and 1 GB LPDDR2-SDRAM. We denote T_{be}, T_h, and $T_\oplus$ as the symbols representing symmetric block encryption, hash, and exclusive or operations, respectively. Implying the experiment conducted in [35], the T_{be} furnishes in 0.013 ms, the running time of T_h is 0.006, while $T_\oplus$ takes negligible time to complete its execution, and therefore, $T_\oplus$ is being ignored in the comparisons. We used AES-128-bit block for encryption, and each identity and random numbers are of 64-bit size. Therefore, an encryption block can convert two parameters (identity/random number) into cipher text. The proposed scheme executes $\{14T_h + 14T_{be}\}$ operations with a running time of 0.266 ms. Table 4 shows the computation cost comparisons of the proposed and related schemes [2, 25, 30, 34]. The proposed scheme has a slight extra computation cost as compared with the other schemes [2, 25, 30, 34].

8.3. Communication Cost. To calculate the fair and pragmatic communication cost comparisons of the proposed scheme with related other schemes, we adopted 160-bit SHA-1, timestamps, random numbers, and identities which are considered to be 64 bits of length. We simulated the AES block cipher with 128-bit output. Thus, in the proposed scheme, communication cost is computed following the previously mentioned parameter values. The authentication cycle of the proposed scheme finishes through the exchange of four messages. In message 1, $\{EVID_i, MSG_1, X_1, T_u, SID\} = \{128 + 160 + 160 + 64 + 64\} = 576$ bits are sent from V_i to TA. In message 2, $\{MSG_2, X_2, T_c\} = \{160 + 160 + 64\} = 384$ bits sent from TA to VS.

In message 3, $\{MSG_3, X_3, T_s\} = \{160 + 160 + 64\} = 384$ bits are directed from VS to TA, and the transmission of message 4 $\{X_4, W, FVID_i\}$ requires transmission of $\{160 + 160 + 160\} = 480$ bits from TA to V_i. Thus, total communication cost of the authentication phase of the proposed scheme is $\{576 + 384 + 384 + 480\} = 1824$ bits. Referring to Table 4, the communication cost of the proposed scheme is higher than other schemes [2, 25, 30, 34]; however, other scheme do not provide one or more security features.

8.4. Storage Cost. To calculate the storage cost of the proposed scheme, we took into account the parameters stored in the memory of the vehicle. The three parameters stored are the hash output, random numbers, and block-based symmetric encryption. Due to usage of SHA-1, the hash output value is 160 bits, the size of the random nonce is 64 bits, and the size of AES-128 encryption is 128 bits. Thus, the storage cost of the proposed scheme is $\{a_1 + b_1 + EVID_i + C_i\} = \{160 + 160 + 128 + 64\} = 512$ bits. Table 4 shows the storage cost of the proposed scheme and other schemes [2, 25, 30, 34]. The storage cost of the proposed scheme is lower than the schemes in [25, 30, 34]; however, the storage cost of the proposed scheme is a bit higher than the scheme in [2], and we proved that Vasudev et al.'s scheme design is incorrect and cannot work in practical environments.

9. Conclusion

Primarily, this study reviewed some of the recent V2V authentication schemes. The paper is aimed at openly discussing the faulty design of the V2V mutual authentication scheme of Vasudev et al. We proved that the design of the scheme of Vasudev et al. is incorrect, and it cannot work practically. Moreover, we introduced an improvement over the scheme of Vasudev et al. The robustness of the proposed

scheme is formally proven through BAN-logic. The proposed security scheme provides mutual authentication between a vehicle and the vehicle server through intermediation of a trusted authority. We also provided security discussion and proved that the proposed scheme provides resistance against various security assaults and provides essential security features. The execution time of a cycle of authentication of the proposed scheme is slightly over the execution time of Vasudev et al.'s scheme. The comparisons with some of the related and recently proposed schemes also show that the proposed scheme provides known security features and resistance to known attacks, while the compared schemes lack one or more security features.

Data Availability

The data used to support this study are already inside the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Conceptualization was handled by J.M. and Y.Y.; investigation was handled by J.M., Y.Y., and A.K.Y; original draft preparation was handled by J.M., M.A.B., and H.X.; review and editing were handled by Y.Y., J.M., S.A.K., and M.A.B.; supervision was handled by Z.D.; and funding acquisition was handled by Z.D. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

This work was supported by funds for the Key Research and Development Plan Project of Shaanxi Province, China, under grant nos. 2019ZDLGY17-08, 2019ZDLGY03-09-01, and 2020ZDLGY09-02; Funds for Science and Technology Innovation Leading Talent of Shaanxi Province, China, under grant no. TZ0336; and Key Research Item for the Industry of Shaanxi Province under grant no. 2018GY-136.

References

[1] T. Limbasiya and D. Das, "Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication," *IEEE Systems Journal*, vol. 14, no. 1, pp. 520–529, 2019.

[2] 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.

[3] I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, "An efficient and provably secure ecc-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1278–1291, 2021.

[4] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: a survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 1, pp. 383–398, 2019.

[5] Y. Zhang, G. Zhang, R. Fierro, and Y. Yang, "Force-driven traffic simulation for a future connected autonomous vehicle-enabled smart transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2221–2233, 2018.

[6] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, "Security in vehicular ad hoc networks: challenges and countermeasures," *Security and Communication Networks*, vol. 2021, Article ID 9997771, 20 pages, 2021.

[7] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314–54344, 2020.

[8] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal, "A comprehensive review of authentication schemes in vehicular ad-hoc network," *IEEE Access*, vol. 9, pp. 31309–31321, 2021.

[9] O. S. al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020.

[10] D. Kim, Y. Velasco, W. Wang, R. N. Uma, R. Hussain, and S. Lee, "A new comprehensive RSU installation strategy for cost-efficient VANET deployment," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4200–4211, 2017.

[11] Z. Gao, D. Chen, S. Cai, and H.-C. Wu, "Optimal and greedy algorithms for the one-dimensional RSU deployment problem with new model," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7643–7657, 2018.

[12] H. Tan and I. Chung, "Secure authentication and key management with blockchain in VANETs," *IEEE Access*, vol. 8, pp. 2482–2498, 2020.

[13] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[14] C.-Y. Chang, H.-C. Yen, and D.-J. Deng, "V2V QoS guaranteed channel access in IEEE 802.11p VANETs," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 5–17, 2015.

[15] F. Arena, G. Pau, and A. Severino, "A review on IEEE 802.11p for intelligent transportation systems," *Journal of Sensor and Actuator Networks*, vol. 9, no. 2, p. 22, 2020.

[16] T. Limbasiya and D. Das, "Secure message transmission algorithm for vehicle to vehicle (V2V) communication," in *2016 IEEE Region 10 Conference (TENCON)*, pp. 2507–2512, Singapore, November 2016.

[17] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[18] K. Mahmood, X. Li, S. A. Chaudhry et al., "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Generation Computer Systems*, vol. 88, pp. 491–500, 2018.

[19] A. Irshad, S. A. Chaudhry, O. A. Alomari, K. Yahya, and N. Kumar, "A novel pairing-free lightweight authentication protocol for mobile cloud computing framework," *IEEE Systems Journal*, vol. 15, no. 3, pp. 3664–3672, 2020.

[20] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in internet of vehicles with

blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11815–11829, 2020.

[21] M. N. Aman, M. H. Basheer, S. Dash et al., "Hatt: hybrid remote attestation for the internet of things with high availability," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7220–7233, 2020.

[22] H. Xu, M. Zeng, W. Hu, and J. Wang, "Authentication-based vehicle-to-vehicle secure communication for VANETs," *Mobile Information Systems*, vol. 2019, Article ID 7016460, 9 pages, 2019.

[23] P. Vijayakumar, M. Azees, A. Kannan, and L. J. 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.

[24] M.-C. Chuang and J.-F. Lee, "TEAM: trust-extended authentication mechanism for vehicular ad hoc networks," in *2011 International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 1758–1761, Xianning, China, April 2011.

[25] S. Kumari, M. Karuppiah, X. Li, F. Wu, A. K. Das, and V. Odelu, "An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks," *Security and Communication Networks*, vol. 9, no. 17, 4271 pages, 2016.

[26] S. A. Abdel Hakeem, M. A. Abd el-Gawad, and H. W. Kim, "A decentralized lightweight authentication and privacy protocol for vehicular networks," *IEEE Access*, vol. 7, pp. 119689–119705, 2019.

[27] S. A. Chaudhry, "Designing an efficient and secure message exchange protocol for internet of vehicles," *Security and Communication Networks*, vol. 2021, Article ID 5554318, 9 pages, 2021.

[28] F. Wang, G. Xu, and L. Gu, "A secure and efficient ECC-based anonymous authentication protocol," *Security and Communication Networks*, vol. 2019, Article ID 4656281, 13 pages, 2019.

[29] S. Tangade and S. S. Manvi, "Trust management scheme in VANET: neighbour communication based approach," in *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, pp. 741–744, Bengaluru, India, August 2017.

[30] 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.

[31] 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.

[32] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

[33] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[34] P. Mohit, R. Amin, and G. P. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Vehicular Communications*, vol. 9, pp. 64–71, 2017.

[35] S. A. Chaudhry, J. Nebhen, K. Yahya, and F. al-Turjman, "A privacy enhanced authentication scheme for securing smart grid infrastructure," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.