sensors

MDPI

Article

SELWAK: A Secure and Efficient Lightweight and Anonymous Authentication and Key Establishment Scheme for IoT Based Vehicular Ad hoc Networks

Sagheer Ahmed Jan [1], Noor Ul Amin [1], Junaid Shuja [2], Assad Abbas [3], Mohammed Maray [4] and Mazhar Ali [2,]*

[1] Department of Computer Science and Information Technology, Hazara University, Mansehra 21300, Pakistan; saghir30232@gmail.com (S.A.J.); namin@hu.edu.pk (N.U.A.)
[2] Department of Computer Science, Abbottabad Campus, COMSATS University Islamabad, Abbottabad 22060, Pakistan; junaidshuja@cuiatd.edu.pk
[3] Department of Computer Science, Islamabad Campus, COMSATS University Islamabad, Islamabad 44000, Pakistan; assadabbas@comsats.edu.pk
[4] College of Computer Science and Information Systems, King Khalid University, Abha 62529, Saudi Arabia; mmarey@kku.edu.sa
* Correspondence: mazhar@cuiatd.edu.pk

Abstract: In recent decades, Vehicular Ad Hoc Networks (VANET) have emerged as a promising field that provides real-time communication between vehicles for comfortable driving and human safety. However, the Internet of Vehicles (IoV) platform faces some serious problems in the deployment of robust authentication mechanisms in resource-constrained environments and directly affects the efficiency of existing VANET schemes. Moreover, the security of the information becomes a critical issue over an open wireless access medium. In this paper, an efficient and secure lightweight anonymous mutual authentication and key establishment (SELWAK) for IoT-based VANETs is proposed. The proposed scheme requires two types of mutual authentication: V2V and V2R. In addition, SELWAK maintains secret keys for secure communication between Roadside Units (RSU_s). The performance evaluation of SELWAK affirms that it is lightweight in terms of computational cost and communication overhead because SELWAK uses a bitwise Exclusive-OR operation and one-way hash functions. The formal and informal security analysis of SELWAK shows that it is robust against man-in-the-middle attacks, replay attacks, stolen verifier attacks, stolen OBU attacks, untraceability, impersonation attacks, and anonymity. Moreover, a formal security analysis is presented using the Real-or-Random (RoR) model.

Keywords: authentication; internet of things; vehicular and wireless technologies; privacy; computational efficiency

check for updates

Citation: Jan, S.A.; Amin, N.U.; Shuja, J.; Abbas, A.; Maray, M.; Ali, M. SELWAK: A Secure and Efficient Lightweight and Anonymous Authentication and Key Establishment Scheme for IoT Based Vehicular Ad hoc Networks. *Sensors* **2022**, *22*, 4019. https://doi.org/10.3390/s22114019

Academic Editors: Robertas Damaševičius, M. Poongodi, Hafiz Tayyab Rauf and Hasan Ali Khattak

Received: 5 April 2022
Accepted: 16 May 2022
Published: 26 May 2022

1. Introduction

The past decade has witnessed colossal advancements in Information and Communication technologies (ICT) resulting in a number of concepts appearing on technological horizons. In practice, ICT has become an integral part of every field of human life. The concept of "smart and autonomous environment" is the result of emerging ICT models that can benefit human society at large. The Internet of Things enables the autonomous and smart society to connect billions of smart devices to inter- and intra-communication to achieve its goals [1–3]. These intelligent sensing and interconnected devices depict a tremendous capacity for replicating the physical environment into corresponding digital environments. IoT-based smart environments can assist society in a broad spectrum, such as e-health care, business, e-commerce, logistics, education, agriculture, defense, and many more.

VANETs are a crucial component of a smart and autonomous environment with an aim to deliver Intelligent Transport System [4] where vehicles communicate with each other, roadside infrastructure, and/or other network services. ITS aims to provide controlled traffic flows, co-operative traffic monitoring, collision prevention, detour route computation, and internet connectivity to moving vehicles. Therefore, VANETS became a combination of wireless ad hoc networks and IoT-based devices for the provision of services. There are three main components of ITS: (a) vehicle, (b) Trust Authority (TA), and (c) Road-Side Unit (RSU), as shown in Figure 1. Vehicular communication takes place in two ways: (a) Vehicle to Vehicle (V2V) and (b) Vehicle to RSU (V2R). Each vehicle is equipped with an onboard unit (OBU) that receives and processes traffic-related data. The OBU also transmits information related to neighboring vehicles and RSU_s using Dedicated Short Range Communication (DSRC) protocols [5]. The RSU is deployed beside the road as a base station and acts as a connecting node between OBU_s and the Trusted Authority (TA). The RSU performs various authentication operations. The TA's responsibilities are to register the OBU_s and RSU_s, perform maintenance, and conduct the entire vehicular system.

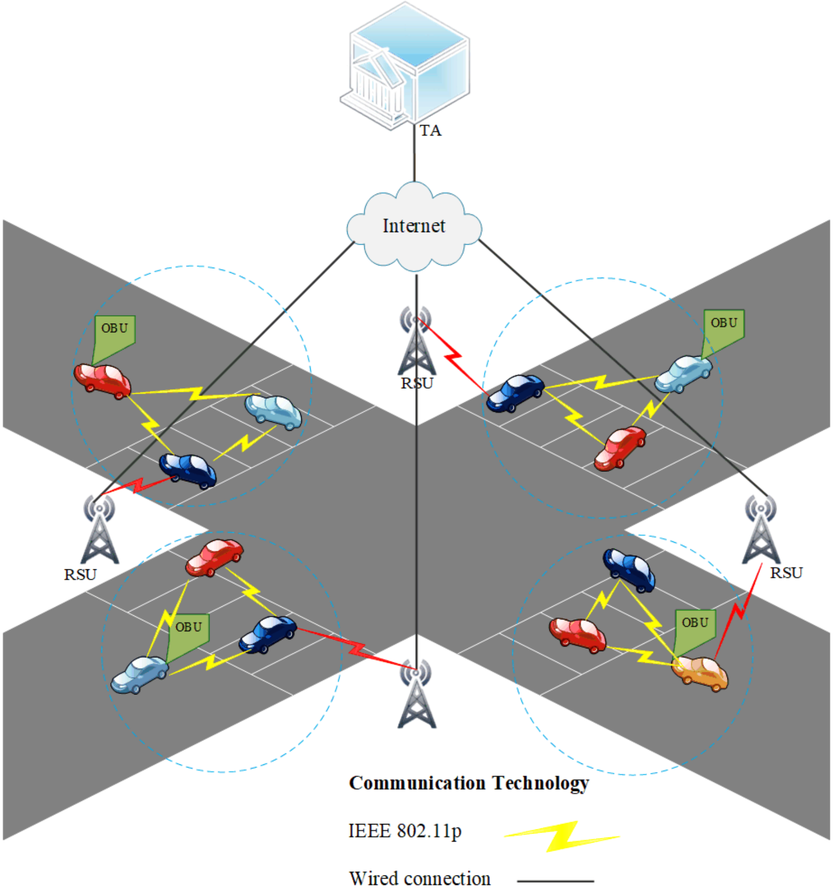


Figure 1. A Typical VANET Scenario.

Moving vehicles with varying accelerations make VANETs different from traditional ad hoc networks, thereby featuring specific network challenges in the case of VANETs. Resource-constrained IoT devices and the wireless nature of communication in VANETs make security a concern of prime focus [6]. Insecure communication may result in the transfer of life-critical information to an adversary. Unauthentic information may lead a passenger to a path of adversary's choice, thus, putting life in danger [7]. Acceptance of a malicious message may cause malfunctioning of the vehicle system. Therefore, security gains prime importance in the case of VANETs, as unwanted situations may cause privacy breaches to one extent and prove to be fatal to the other.

A Secure and Efficient Lightweight Anonymous Mutual Authentication and Key establishment scheme for IoT-based vehicular ad hoc networks (SELWAK) is proposed in this paper. The proposed scheme uses a simple XOR operation and a one-way hash function, making it light in terms of resource usage. Various authentication and key establishment schemes have been discussed in the literature. Moreover, resource-constrained devices do not support traditional cryptographic operations due to low memory and computational power, and therefore demand lightweight cryptographic preemptive. Ensuring the privacy of vehicles is a challenging issue because an adversary can trace the traveling routes of vehicles and identify vehicles that may cause serious danger. To overcome privacy issues, the proposed scheme uses mask identities to ensure anonymity and privacy preservation. In addition to this, an attacker cannot relate driver's multiple mask identities to reveal his/her real identity. The proposed scheme provides better security services in a cost-effective manner compared to existing schemes. The SELWAK consists of four phases: (i) Registration, (ii) authentication and key agreement, (iii) RSU-to-RSU key establishment, and (iv) password change.

In the registration phase, vehicles and roadside units register with the TA. The driver of the vehicle chooses various credentials and sends them to the TA in a secure way. Then, the vehicle is deployed on the VANETs. Before deployment of a vehicle in VANETs, TA sends the information to vehicle V_i in a secure way, and OBU_i stores that information for future use. In the RSU registration phase, the TA generates credentials for every RSU that is deployed in VANETs. The second phase consists of two sub phases, such as (i): V2V authentication key agreement phase and (ii) the V2RSU authentication key agreement phase. In each sub phase, after successful mutual authentication, a session key is established between two entities, and this key is later used for authentication purposes. In the key establishment phase of RSU-to-RSU, a session key is established between those RSU_s on the basis of their preloaded credentials. For secure communication, it is necessary that the driver of the vehicle change the password periodically. There is an option available for drivers to change passwords locally without interacting with the TA. Formal security analysis of the SELWAK was done using the Real-or-Random (RoR) model. SELWAK provides better security services and effectively reduces computational cost and communication overhead, as indicated by the derived results. The following are the main contributions of this paper.

- In this paper, a novel lightweight anonymous authentication and key establishment scheme for VANETs is proposed that uses one-way cryptographic hash functions and simple XOR operations.
- We ensure the privacy of vehicles so that an adversary cannot trace the real identity and travel routes of vehicles.
- SELWAK is secure against replay attacks, impersonation attacks, man-in-the-middle attacks, stolen verifier attacks, stolen OBU attacks, untraceability, and anonymity.
- Formal security proof of establishing a secure session key is provided using the RoR model.

The remainder of the paper is organized as follows. Section 2 discusses related work, whereas Section 3 presents systems models. In Section 4, the proposed SELWAK is described, while Section 5 presents the security analysis. In Section 6, we evaluate the performance of the proposed scheme, and Section 7 concludes the paper.

2. Related Work

Numerous studies exist on authentication, key establishment, and privacy preservation in VANETs. Below, we present a brief discussion of the few existing techniques. Wang et al. [8] proposed an authentication scheme for VANET using a group signature. According to the authors, when vehicles apply for group membership, membership validity is checked to determine whether the vehicle is still a member of the group. Batch verification of vehicles can also be done in the proposed scheme. The authors in [9] proposed a password based novel group key agreement protocol. Their scheme provides batter privacy services in the field of VANET. The proposed scheme uses a hash function for authentication and integrity. According to the authors, their scheme has less computational cost as well as communication overhead as compared to certificate-based public key cryptography and identity-based public key cryptography but is vulnerable to denial-of-service attacks. In a novel secure and efficient anonymous authentication scheme with a privacy preserving scheme (EAAP) [10], RSU_s and OBU_s use digital signatures to sign each message. The EAAP scheme uses a bilinear-pairing technique to conform to the integrity and authentication of messages. Bilinear pairing has a high computational cost compared to the cryptographic general hash function [11]. A discrete event-based threat-driven authentication scheme has been proposed to ensure secure V2I and V2V communication in [12]. To satisfy the secure communication between V2V and V2R, the proposed approach uses a session key, private key, and public key simultaneously. The authors used the Petri Nets and Veins framework for the formal analysis of their scheme. Zhang et al. [13] proposed an identity-based public key cryptographic (ID-PKC) scheme for privacy-preservation communication. The authors used bilinear pairing and ID-PKC to originate vehicular clouds and secure communication in vehicular clouds. In this scheme, a secure and anonymous dynamic vehicular cloud comes from using pseudonyms. The authors also presented a well-organized protocol that allowed cloud users to join or leave the group dynamically. Two schemes that control traffic lights intelligently using for computing were proposed in [14]. The first scheme's security is based on Computational Diffie-Hellman puzzle hardness, and the second is based on the hash collision puzzle. After a fixed interval of time, the traffic lights generate the puzzle and verify it. For VANETs, a decentralization mutual authentication and key agreement scheme were proposed in [15]. The vehicles communicate in the cluster's fashion and use the hash function and XOR operation. There are three types of authentication taking place: vehicles-to-cluster heads, between cluster heads and cluster heads, and roadside units. This scheme does not deliberate batch verification and privacy preservation of the signatures of multiple messages. Ibrahim et al. [16] proposed two schemes, epidemic-based and topology-based, in which RSU switches its authentication service to the nearest vehicle for the betterment of the authentication service. The topology-based scheme depends upon network analysis and computing node degree, but the scheme based on the epidemic level did not depend on network analysis. The authors have compared both schemes and show that topology-based schemes have better performance but more security threats than epidemic-based schemes. An authentication scheme with privacy preservation property based on identity was proposed in [17]. To reduce communication overhead, a registration list is used instead of the revocation list. The security features of VANET were not affected by malicious vehicles. Moreover, their scheme did not use bilinear pairing operations, which takes more execution time, thus dramatically reducing computation and communication costs. Gope et al. [18] proposed an efficient authentication scheme based on RFID with privacy features. This scheme uses a distributed IoT infrastructure for secure localization servers to facilitate smart city environments. The backend server has a full command to recognize RFID tags without any trouble. However, the problem with this scheme is that the managing server is so powerful that it can know the entire communication of RFID tags. The security of the scheme depends on the backend server. If the backend server has a strong security mechanism, then the attacker cannot get security credentials, but if backend server security is compromised, then the attacker can easily get secret information and execute a forgery attack. Second, the RFID tags did not have any physical security. A signature based on an identity scheme for authentication of V2V communication has been proposed in [19]. This scheme is based on elliptic curve cryptography. The advantage of batch signature verification is that it can authenticate a large number of vehicles at a time. This scheme uses an RoR model for security proof. According to the authors, their scheme reduces the execution time and communication burden compared to other schemes. Cui et al. [20] proposed an authentication scheme that preserves the privacy property in the field of VANET. This scheme uses ECC and identity-based signatures for both V2I and V2V communication. The authors used the binary search method and the cuckoo filter method to improve the success rate of batch signature verification. Xie et al. [21] proposed a robust and secure conditional privacy-preserving scheme using identity-based authentication. The reliability and integrity of the messages are ensured using identity-based signatures for V2V communication and V2I communication. The results of this scheme show that it has a high computational cost and communication overhead. A conditional-based privacy and authentication scheme was proposed in [22]. The prevention from side channel attacks is gained by storing sensitive data on the TPD of OBU and updating it periodically. The formal security analysis of their scheme has been shown using BAN-logic. Their approach is based on a one-way hash function and ECC; therefore, according to the authors, their scheme is efficient in terms of cost compared to existing schemes [23–26]. To ensure secure communication in VANET, an authentication scheme based on ECC that satisfies privacy preservation was proposed in [27]. In this scheme, the authors combined RSU- and TPD-based schemes to handle privacy and security issues in VANET. All the system's public credentials and keys are preloaded in the TPD of RSU. Their scheme worked in four phases: initialization phase, mutual authentication, signing, and verification phases. Jie et al. [28] presented a chaos mapping-based full session key agreement scheme. This scheme worked in two phases. In the first phase, group key agreement was made between the cluster head and the fog server. In the second phase, a group key agreement is made among vehicle nodes. A secure and robust authentication and privacy scheme has been introduced for vehicular communication [24]. The trusted authority preloads the already computed private key in the vehicle's TPD via a secure medium. Jalawai et al. [27] presented an authentication mechanism using elliptic curve cryptography, which satisfied conditional privacy preservation. They addressed some security and privacy concerns based on the combined usage of TPD-based schemes with RSU-based schemes. The system's key and all the initial public parameters are preloaded in the TPD of RSU. There are some issues with privacy and security, and some attacks are also possible. Vijayakumar et al. [29] proposed an authentication and key distribution scheme for VANET. According to the authors, their scheme is efficient in terms of both computation cost and communication overhead. In addition, the vehicles that come in the orbit of RSU securely distribute the group key among the vehicles. The RSU uses the group key to send the message related to the location among the neighboring vehicles via a secure channel. Vijayakumar et al. [30] proposed a novel batch authentication and key exchange protocol based on 6G technology for VANET. In addition, their scheme reduces the load on the RSU in congested areas. An elliptic curve-based intelligent conditional privacy-preserving technique for VANET has been proposed in [31]. The authors claimed that this scheme is secure, efficient, and can easily deploy. A cuckoo filter-based authentication scheme that improved timed efficient stream loss tolerance for VANETs was proposed in [32]. The authentication information of vehicles that came under the communication range of the RSU can be saved by a cuckoo filter. This scheme provides robust, anonymous authentication and reduces costs. To provide safety in VANET, an efficient anonymous mutual authentication approach with privacy is proposed in [32]. In their scheme, the trusted authority preloaded a group of pseudonym identities and a group of private keys to each vehicle, which may cause problems for managing huge certificates, which will increase the burden for management of certificates for TA due to the limited storage capacity of the vehicle. Ren et al. [33] proposed a blockchain-based, certificateless public key signature scheme for VANET. Their scheme provides support for batch verification of signatures, and blockchains are used to protect the privacy of vehicles. Moreover, this scheme also realized the traceability property. An authentication approach for global mobility networks was proposed in [34]. This scheme is based on an elliptic curve cryptosystem and therefore takes much execution time to perform major cryptographic operations.

The schemes discussed in the literature have some problems. Due to the fast movement of vehicles in VANET, the performance of signature-based schemes is not optimal. OBU has limited storage capacity, computing power, and power. The signing and verification of road safety-related messages slows down due to heavy cryptographic operations. For example, bilinear pairing operations consume more time for message's signing and verification process [30]. Therefore, it is difficult for RSU to verify a large number of vehicles in its range moving with high speed in a short period of time. This puts a heavy burden on the verification vehicle, and behind the current demand for an efficient and lightweight scheme that validates many traffic-related messages on V2V, V2RSU, and RSU2RSU connections in high traffic density areas without compromising safety. On the other hand, a group signature-based scheme requires registration of each vehicle with the TA and receives its private key via a secure channel. These time-consuming operations create hurdles for vehicles to change private keys easily. Therefore, the likelihood of an attack increases.

Motivations

VANETs and vehicles travel at high speeds; therefore, the schemes mentioned in the literature are not optimal for such an environment. The OBU fixed in the vehicle has limited storage capacity, power supply, and computational power. Various major cryptographic operations slow down the signature generation and verification processes of road safety-related messages. For example, elliptic curve point multiplication and point addition are considered to be the most time-consuming operations in ECC-based schemes. Therefore, it is difficult to verify vehicles moving at high speeds by the RSU in a short time period in its communication range. It creates a high load on verifying entities, which is the reason it demands a secure and efficient lightweight and anonymous authentication and key establishment scheme for IoT-based vehicular ad hoc networks.

3. System Model

The network and thread models are presented in this section.

3.1. Network Model

The network model for VANET used in the SELWAK is shown in Figure 1. In this model, the entities involved are vehicles (V_i), roadside units (RSU_s), and TA. In the network model, three types of participation involved: V2V, V2RSU and RSU2RSU.The TA is responsible for generating identities, for example, keys, and identities for vehicles and RSU_s. The information generated by TA is stored in the memory of RSU_s and OBU_s, which can be used for authentication purposes. In light of the proposed model, the authentication processes that are required are V2V, V2RSU and RSU2RSU.

3.2. Threat Model

According to this model, all entities are assumed to communicate with each other through the insecure channel. RSU_s are also assumed to be semi-trusted. An attacker can easily delete, modify, or eavesdrop the transmitted message. As RSU_s are considered semi-trusted, we considered that the RSU's confidential information is stored in tamper-proof devices within RSU_s. However, we considered that OBU_s are not installed with tamper-proof devices. Moreover, by using a power analysis attack [22,23], an attacker can extract all the sensitive information from some stolen OBU_s of the vehicles. Finally, the TA is considered a fully trusted authority.

4. Proposed Scheme

In this paper, a novel lightweight and anonymous authentication and key establishment scheme for IoT-based VANETs is proposed. In SELWAK, when a vehicle joins the region of another vehicle, anonymous mutual authentication between the vehicles is performed to avoid communication with malicious vehicles. To perform different types of wireless communications in VANETs, our authentication scheme can be divided into three categories: Vehicle-to-Vehicle, Vehicle-to-Roadside Unit, and Roadside Unit-to- Roadside Unit authentication. The proposed scheme works in four phases: registration phase, authentication, and key agreement phase, RSR-to RSU key establishment phase, and password change phase. Before giving a detailed description of the various phases, we briefly describe each phase in Figure 2. The definitions of the notations in our scheme are described in Table 1.

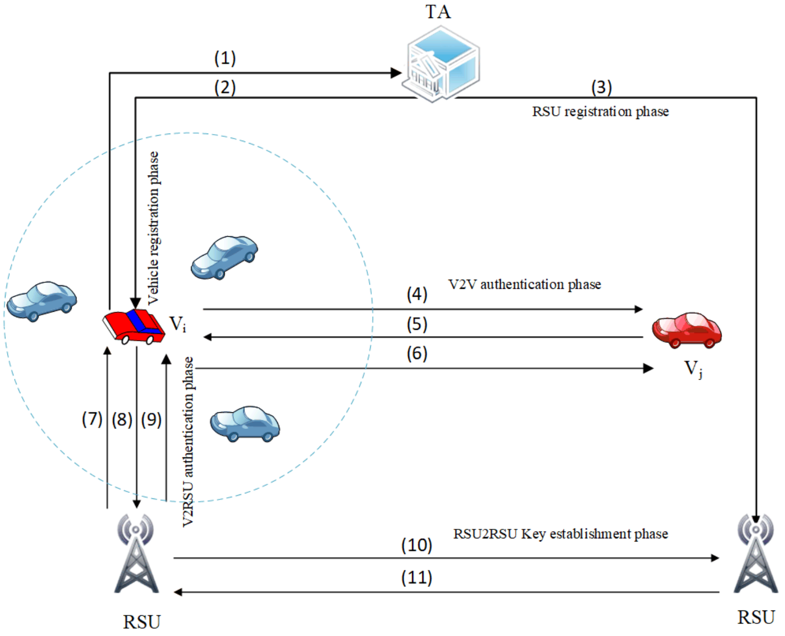


Figure 2. The phases involved in the proposed scheme. Vehicle Registration Phase (1). Registration request message (2). The registration response message. RSU Registration Phase (3). RSU′scredentials generated by TA. V2V Authentication and Key Establishment Phase (4). Authentication request message (5). Authentication reply message (6). Acknowledge message. V2RSU Authentication and Key Establishment Phase (7). Send a request message for Authentication (8). Authentication reply message (9). Acknowledgement message RSU2RSU Key Establishment phase (10). Send a request message for Key establishment (11). Key establishment response message.

Table 1. Notations used in the paper.

Notation	Description
RSU_j	jth Roadside Units
V_i	ith Vehicle
Drv_i	Driver of the vehicle V_i
drv_{id}	Identity of the driver
$RSUID_j$	Identity of RSU_j
$Mdrv_{id}$	Masked Identity of drivers
$TMRSU_j$	Time dependent masked identity of RSU_j
OBU_i	ith Onboard Unit
TA_{id}	Identity of TA
α, β	160 bits secret keys of TA
PWD_i	Password chosen by drivers
RT_{vi}	Registration time stamp of V_i
RT_{RSUj}	Registration time stamp of RSU_j
T	Current time stamp
N	Random Nonce
ΔT	Max transmission delay
$h(.)$	One way hash function
$\mid\mid$	Concatenation
$\oplus$	Bitwise XOR operation

4.1. Registration Phase

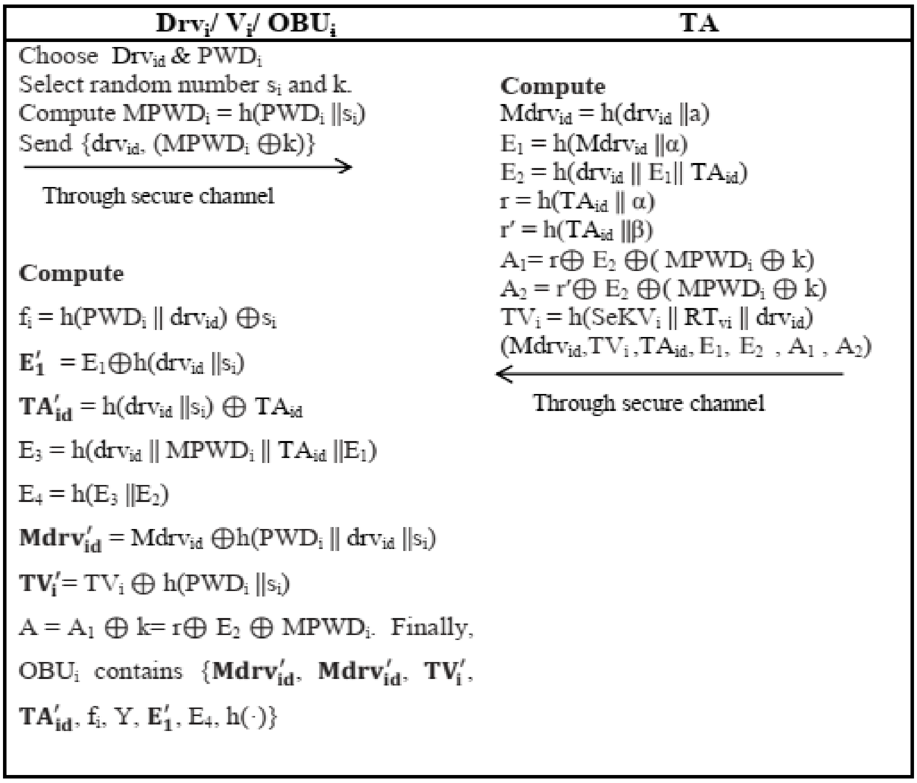
In this phase, the registration of vehicles and roadside units is done in the following ways.

4.1.1. Vehicle Registration Phase

It is necessary to register each vehicle offline with the TA for secure V2V and V2R communication. The vehicle's registration with the TA is a one-time process; hence, for the execution of this process, a secure channel is required, e.g., in person. The steps below are used for this purpose.

1. The driver Drv_i of vehicle V_i, on his own choice, chooses a password PWD_i and unique identity Drv_{id} and two 160-bit random numbers s_i and k. OBU_i computes a masked password $MPWD_i = h(PWD_i\ ||s_i)$, transmit $(drv_{id},\ (MPWD_i \oplus k))$ to the TA through a secure channel.
2. After receiving the registration request $(drv_{id},\ (MPWD_i \oplus k))$, TA calculated $Mdrv_{id} = h(drv_{id}\ ||a)$, $E\ _1 = h(Mdrv_{id}\ ||\alpha)$ using a pre-generated 160-bit secret key α. It further calculate $E_2 = h(drv_{id}||E_1||TA_{id})$, $r = h(TA_{id}||\alpha)$, $r' = h(TA_{id}||\beta)$, $A_1 = r \oplus E_2 \oplus (MPWD_i \oplus k)$, and $A_2 = r' \oplus E_2 \oplus (MPWD_i \oplus k)$. Furthermore, for every registered vehicle V_i, a unique secret key $SeKV_i$ is also generated by TA and computes time based credential $TV_i = h(SeKV_i\ ||RT_{vi}\ ||\ drv_{id})$ on the basis of timestamp generated duringregistration time RT_v of V_i and identity drv_{id} of driver. Then, TA transmit $(Mdrv_{id}, TV_i, TA_{id}, E_1, E_2, A_1, A_2)$ to through a secure channel.
3. After receiving information $(Mdrv_{id},\ TV_i, TA_{id}, E_1,\ E_2,\ A_1,\ A_2)$, OBU_i compute $f_i = h(PW\,D_i||drv_{id}) \oplus s_i$, $E'_1\ = E_1 \oplus h(drv_{id}||s_i)$, $TA'_{id}h(drv_{id}||s_i)TA_{id}$, $E_3 = h(d\ rv_{id}||MPWD_i||TA_{id}||E_1)$, $E_4 = h(E_3||E_2)$, $Mdrv'_{id} = Mdrv_{id} \oplus h(PWD_{id}||drv_{id}||s_i)$, $TV'_i = TV\,_i \oplus h(PWD_i||s_i)$, $A\ = A_1 \oplus k = r \oplus E_2 \oplus MPWD_i$.

OBU_i then deletes k, $Mdrv_{id}$, TV_i, TA_{id}, E_1, A_1 and A_2 from its memory. Finally, OBU_i contains $\{Mdrv'_{id},\ TV'_i,\ TA'_{id},\ f_i,\ Y,\ E'_1,\ E_4,\ h(\cdot)\}$. The pictorial representation of algorithm is given in Figure 3.



Drv_i/ V_i/ OBU_i

Choose Drv_{id} & PWD_i
Select random number s_i and k.
Compute $MPWD_i = h(PWD_i\ ||s_i)$
Send $\{drv_{id}, (MPWD_i \oplus k)\}$

Through secure channel

Compute

$f_i = h(PWD_i\ ||\ drv_{id}) \oplus s_i$

$\mathbf{E'_1}\ = E_1 \oplus h(drv_{id}\ ||s_i)$

$\mathbf{TA'_{id}} = h(drv_{id}\ ||s_i) \oplus TA_{id}$

$E_3 = h(drv_{id}\ ||\ MPWD_i\ ||\ TA_{id}\ ||E_1)$

$E_4 = h(E_3\ ||E_2)$

$\mathbf{Mdrv'_{id}} = Mdrv_{id} \oplus h(PWD_i\ ||\ drv_{id}\ ||s_i)$

$\mathbf{TV'_i} = TV_i \oplus h(PWD_i\ ||s_i)$

$A = A_1 \oplus k = r \oplus E_2 \oplus MPWD_i$. Finally,

OBU_i contains $\{\mathbf{Mdrv'_{id}}, \mathbf{Mdrv'_{id}}, \mathbf{TV'_i}, \mathbf{TA'_{id}}, f_i, Y, \mathbf{E'_1}, E_4, h(\cdot)\}$

TA

Compute
$Mdrv_{id} = h(drv_{id}\ ||a)$
$E_1 = h(Mdrv_{id}\ ||\alpha)$
$E_2 = h(drv_{id}\ ||\ E_1||\ TA_{id})$
$r = h(TA_{id}\ ||\ \alpha)$
$r' = h(TA_{id}\ ||\beta)$
$A_1 = r \oplus E_2 \oplus (\ MPWD_i \oplus k)$
$A_2 = r' \oplus E_2 \oplus (\ MPWD_i \oplus k)$
$TV_i = h(SeKV_i\ ||\ RT_{vi}\ ||\ drv_{id})$
$(Mdrv_{id}, TV_i, TA_{id}, E_1, E_2\ , A_1\ , A_2)$

Through secure channel

Figure 3. Vehicle Registration Phase.

4.1.2. Roadside Unit Registration Phase

Trusted authority generates 160-bit secret keys α and β, before deployment of RSU_s in VANETs. Then trusted authority generates unique identities of RSU_s like RSU_{id1}, $RSU_{id2} \ldots RSU_{idn}$ and corresponding masked identities $\gamma_i, \gamma_j \ldots \gamma_n$ that are generated as $\gamma = h\ (RSU_{idk}||\beta)$. The TA further generates identities for RSU_j as $r\,' = h(TA_{id}||\ \beta)$. In addition, TA generates time-based identities for each RSU_j as $TRSU_j = h\ \left(TA_{id}\middle|\middle|RTRSU_j\right||\ \beta)$. The RSU_j then give the information $\{r,\ \gamma, TRSU_j\}$. In our scheme γ is used for Vehicle V_i to RSU_j authentication and $TRSU_j$ is used for symmetric key establishment between RSU_s. The polynomial-based key distribution for $RSU2RSU$ key establishment. To do this, TA first selects bivariate polynomial $th(x,y) = \ th(x,y) = \sum_l^n 0 \sum_{m=0}^n s^l, m^{x^l y^m} \in GF(th)[x,y]$ over a finite field degree n. For each RSU_j TA computer polynomial share $th\left(TRSU_j,\ y\right)$. The RSU_j is also loaded with $th\left(TRSU_j,\ y\right)$ in its memory.

4.2. Authentication and Key Establishment Phase

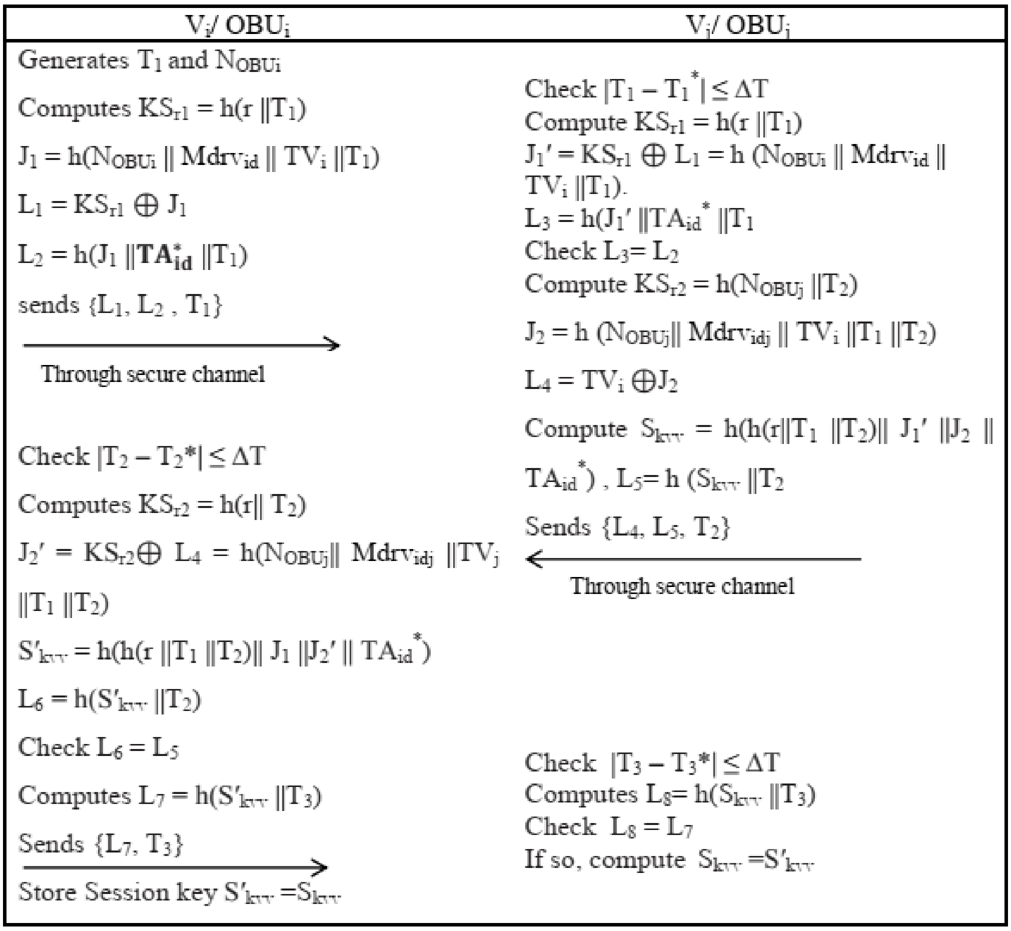
Initially, Drv_i inputs a password PWD_i^* and identity drv_{id} to OBU_i. The OBU_i calculates $s_i^* = f_1 \oplus h(PWD_i^*\ ||drv_{id})$, $E_1^* = E_1' \oplus\ h(drv_{id}||s_i^*\ ) = h(Mdrv_{id}\ ||\alpha)$, $MPDW_i^* = h(PWD_i^*\ ||s_i^*)$, $TA_{id}^* = TA_{id}' \oplus h(drv_{id}\ ||s_i^*)$ and $Mdrv_{id} = Mdrv_{id}' \oplus\ h(PWD_i^*||drv_{id}||s_i^*)$. OBU_i further computes $E_2{}^* = h\ (Mdrv_{id}||E_1^*||TA_{id}^*)$, $r\ =\ A\ \oplus\ E_2^* \oplus\ MPDW_i^*$, $r\prime\ = A\prime \oplus\ E_2^*\ \oplus\ MPDW_i^*$,$E_3^* = h\ (drv_{id}||MPDW_i^*||TA_{id}^*||E_1^*)$ and $E_4^* = h\ (E_3^*||E_2^*)$. Inputting correct credentials: password and identity by authorized users. Each vehicle also computes the same r and r′. OBU_i checks the condition if $E_4^* = E_4$. If conditions hold, it implies that drv_i is authentic users. If the condition is not satisfied, then the phase is terminated. In addition, OBU_i also computes $TV_i = TV_i'\ \oplus\ MPDW_i^*$.

4.2.1. V-To-V Authentication and Key Establishment Phase

In V2V authentication, two neighboring vehicles perform the following steps:

1. Onboard Unit OBU_i generates current timestamp T_1 and chooses random nonce N_{OBUi}, and computes secret key $KSr_1 = h(r\ ||T_1)$. Two neighbor vehicles used r and r' for authentication in VANETs. An OBU_j further compute $J_1 = h(N_{OBUi}\ ||\ Mdrv\ _{id}||\ TV_i\ ||T_1)$, $L_1\ =\ KSr_1 \oplus J_1$ and $L_2 = h(J\ _1||TA\ _{id}^*\ ||T_1)$, and sends authentication requests $\{L_1, L_2, T_1\}$ to its neighboring vehicle through a public channel.
2. "After receiving $\{L_1, L_2, T_1\}$, OBU_j validates the timeliness of T_1 by checking condition $|T1\ -\ T1*|\ \le\ \Delta T$, where $T1*$ is the time when the message is received and ΔT is the maximum transmission delay. If the condition holds, OBU_j calculates the time-dependent secret key $KSr_1 = h(r\ ||T1)$ on the basis of T_1 and previously computed r. It then computes $J_1' = KSr_1 \oplus L_1 = h\ (N_{OBUi}\ ||\ Mdrv_{id}\ ||\ TV_i\ ||T_1)$. To proceed, it then calculates $L_3 = h\ (J_1'||TA_{id}^*\ ||T_1)$. The OBU_i further checks the condition $L_3 = L_3$, if condition holds then V_j authenticate V_i and reject otherwise.
3. The OBU_j selects a random nonce N_{OBUi} and current timestamp T_2, and computes time-dependent secret key $KSr_2 = h(N_{OBUj}\ ||T_2)$, $J_2 = h\ (N_{OBUj}\ ||\ Mdrv_{idj}\ ||\ TV_i\ ||T_1\ ||T_2)$ and $L\ _4\ =\ TV_i \oplus J_2$. Then, the session key is computed $S_{kvv} = h(h(r||\ T\ _1||T_2)\ ||\ J_1'\ ||J_2\ ||\ TA_{id}^*)$ and $L_5 = h\ (S_{kvv}\ ||T_2)$, and sends $\{L_4, L_5, T_2\}$ to V_i via a public channel.
4. On the reception of $\{L_4, L_5, T_2\}$, OBU_i also checks the validity of T_2 by $|T2\ -\ T2*|\ \le\ \Delta T$, where T_2^* I message arrival time. If the condition is fulfilled, by using received T_2 and earlier computer r and $J_2' = KSr_2 \oplus L_4 = h(N_{OBUj}||\ Mdrv_{idj}\ ||TV_j\ ||T_1\ ||T_2\Big)$., OBU_i computes $KSr_2 = h\ (r||\ T_2)$. The OBU_i further computes the session key $S_{kvv}' = h\ (h(r\ ||\ T_1\ ||T_2)\ ||\ J_1\ ||J\ _2'||\ TA_{id}^*)$, $L_6 = h(S_{kvv}'\ ||T_2)$. It then checks the condition $L_6 = L_5$. If the condition is satisfied, V_i successfully authenticates. Using the current timestamp T_3, the OBU computes $L_7 = h(S_{kvv}'\ ||T_3)$, and finally sends a response message $\{L_7, T_3\}$ to V_j via a public channel.
5. On the reception of $\{L_7, T_3\}$, OBU_j checks the correctness of T_3 by checking condition $|T3 - T3*|\ \le\ \Delta T$, where $T3*$ is reaching time. Then, it computes $L_8 = h(S\ _{kvv}||T_3)$ and checks whether $L\ _8 = L_7$. If the condition is satisfied, the session key computed by OBU_i

is correct, and it guarantees that both V_i and the session key are established by V_j in this way S_{kvv} $(=S'_{kvv})$ to start mutual communication. The pictorial representation of algorithm is given in Figure 4.



V_i/ OBU_i

Generates T_1 and N_{OBUi}

Computes $KS_{r1} = h(r \,||T_1)$

$J_1 = h(N_{OBUi} \,||\, Mdrv_{id} \,||\, TV_i \,||T_1)$

$L_1 = KS_{r1} \oplus J_1$

$L_2 = h(J_1 \,||\mathbf{TA}^*_{id} \,||T_1)$

sends $\{L_1, L_2\,, T_1\}$ $\xrightarrow{\text{Through secure channel}}$

Check $|T_2 - T_2{}^*| \leq \Delta T$

Computes $KS_{r2} = h(r|| \,T_2)$

$J_2' = KS_{r2} \oplus L_4 = h(N_{OBUj}||\, Mdrv_{idj} \,||TV_j \,||T_1 \,||T_2)$

$S'_{kvv} = h(h(r \,||T_1 \,||T_2)||\, J_1 \,||J_2' \,||\, TA_{id}{}^*)$

$L_6 = h(S'_{kvv} \,||T_2)$

Check $L_6 = L_5$

Computes $L_7 = h(S'_{kvv} \,||T_3)$

Sends $\{L_7, T_3\}$ $\longrightarrow$

Store Session key $S'_{kvv} = S_{kvv}$

V_j/ OBU_j

Check $|T_1 - T_1{}^*| \leq \Delta T$

Compute $KS_{r1} = h(r \,||T_1)$

$J_1' = KS_{r1} \oplus L_1 = h\,(N_{OBUi} \,||\, Mdrv_{id} \,||\, TV_i \,||T_1).$

$L_3 = h(J_1' \,||TA_{id}{}^* \,||T_1$

Check $L_3 = L_2$

Compute $KS_{r2} = h(N_{OBUj} \,||T_2)$

$J_2 = h\,(N_{OBUj}||\, Mdrv_{idj} \,||\, TV_i \,||T_1 \,||T_2)$

$L_4 = TV_i \oplus J_2$

Compute $S_{kvv} = h(h(r||T_1 \,||T_2)||\, J_1' \,||J_2 \,|| TA_{id}{}^*)$, $L_5 = h\,(S_{kvv} \,||T_2$

Sends $\{L_4, L_5, T_2\}$ $\xleftarrow{\text{Through secure channel}}$

Check $|T_3 - T_3{}^*| \leq \Delta T$

Computes $L_8 = h(S_{kvv} \,||T_3)$

Check $L_8 = L_7$

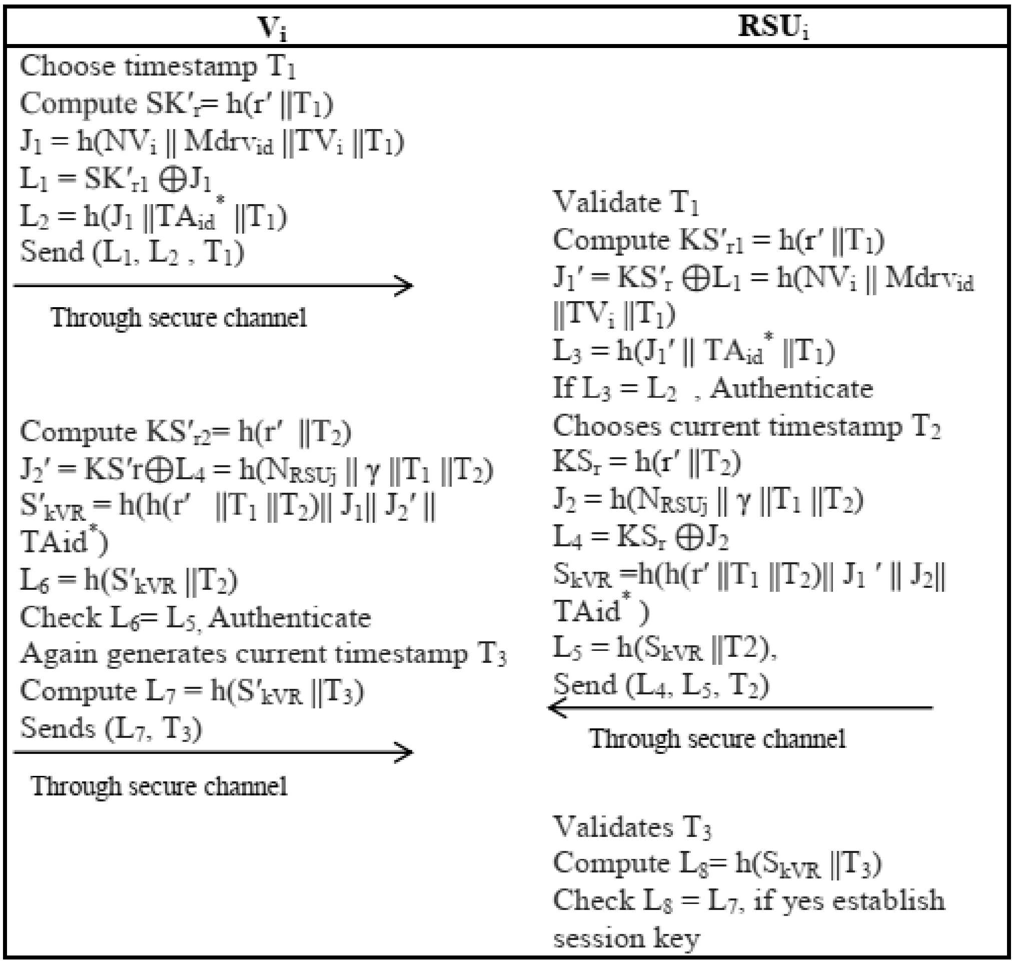
If so, compute $S_{kvv} = S'_{kvv}$

Figure 4. V2V Authentication and Key Establishment Phase.

4.2.2. V-to-RSU Authentication and Key Establishment Phase

In this phase, vehicle V_i and neighbor roadside unit RSU_j perform the following steps for authentication and key establishment:

1. An OBU_i chooses a timestamp T_1 and random nonce NV_i and calculates the time-dependent key $SK_r' = h(r' \;||T1)$ on the basis of previously calculated r. It further computes $J_1 = h(NV_i \;||\; Mdrv_{id} \;||TV_i \;||T_1)$, $L\,_1 \;=\; SK'_{r1} \oplus J_1$and $L_2 = h(J_1||TA\;^*_{id}||T_1)$ and sends $\{L_1, L_2, T_1\}$ as an authentication message to its nearby RSU_j through a public channel.
2. After receiving $\{L_1, L_2, T_1\}$ RSU_j validate T_1. If it validates the timestamp, then RSU_j calculates the time-dependent key $SK'_{r1} = h(r'||T_1)$ on the basis of T_1. It then computes $J_1' = SK_r' \oplus L_1 = h(NV_i \;||\; Mdrv_{id} \;||TV_i \;||T_1)$ and $L_3 = h(J_1' \;||\; TA\;^*_{id}||T_1)$. If $L_3 = L_2$ holds the RSU_j authenticate V_i and reject otherwise.
3. The RSU_j then chooses the current timestamp T_2 and random nonce N_{RSU} to calculate another time-dependent key $KS_r = h(r'||T_2)$,$J_2 = h(N_{RSUj} \;||\; \gamma \;||T_1 \;||T_2)$ and $L_4 = KS_r \oplus J_2$. It further calculates the session key $S_{kVR} = h(h(\,r'||T_1 \;||T_2) \;||\; J_1'||\; J_2||\; TA\;^*_{id})$ and $L_5 = h(S_{kVR} \;||T_2)$, and sends message $\{L_4, L_5, T_2\}$ to V_i through an open channel. The pictorial representation of algorithm is given in Figure 5.



V_i	RSU_i
Choose timestamp T_1 Compute $SK'_r = h(r' \|\|T_1)$ $J_1 = h(NV_i \|\| Mdrv_{id} \|\|TV_i \|\|T_1)$ $L_1 = SK'_{r1} \oplus J_1$ $L_2 = h(J_1 \|\|TA_{id}^* \|\|T_1)$ Send (L_1, L_2, T_1) Through secure channel	Validate T_1 Compute $KS'_{r1} = h(r' \|\|T_1)$ $J_1' = KS'_r \oplus L_1 = h(NV_i \|\| Mdrv_{id} \|\|TV_i \|\|T_1)$ $L_3 = h(J_1' \|\| TA_{id}^* \|\|T_1)$ If $L_3 = L_2$, Authenticate Chooses current timestamp T_2 $KS_r = h(r' \|\|T_2)$ $J_2 = h(N_{RSUj} \|\| \gamma \|\|T_1 \|\|T_2)$ $L_4 = KS_r \oplus J_2$ $S_{kVR} = h(h(r' \|\|T_1 \|\|T_2)\|\| J_1' \|\| J_2\|\| TAid^*)$ $L_5 = h(S_{kVR} \|\|T2)$, Send (L_4, L_5, T_2) Through secure channel
Compute $KS'_{r2} = h(r' \|\|T_2)$ $J_2' = KS'r \oplus L_4 = h(N_{RSUj} \|\| \gamma \|\|T_1 \|\|T_2)$ $S'_{kVR} = h(h(r' \|\|T_1 \|\|T_2)\|\| J_1\|\| J_2' \|\| TAid^*)$ $L_6 = h(S'_{kVR} \|\|T_2)$ Check $L_6 = L_5$, Authenticate Again generates current timestamp T_3 Compute $L_7 = h(S'_{kVR} \|\|T_3)$ Sends (L_7, T_3) Through secure channel	
	Validates T_3 Compute $L_8 = h(S_{kVR} \|\|T_3)$ Check $L_8 = L_7$, if yes establish session key

Figure 5. V2RSU Authentication and key establishment phase.

4.3. Key Establishment Phase between RSU_s

Two neighbor Roadside Units, namely RSU_u and RSU_v established pairwise key using the following steps.

1. The random nonce N_{RSUu} is generated by RSU_u and sends $\{TRSU_u, N_{RSUu}\}$ to RSU_v.
2. Upon receiving "$\{TRSU_u, N_{RSUu}\}$, RSU_u calculates symmetric key shared with RSU_u as $S_{kRR} = th\ (TRSU_v, TRSU_u)$ by pre-loaded polynomial share $\wp\ (TRS_v, y)$ and $S_{KV} = h\ (S_{kRR}\ ||N_{RSUu})$. The RSU_v then sends the message $\{TRSU_u, S_{KV}\}$ to RSU_u.
3. Finally, on reception of $\{TRSU_u,\ S_{KV}\}$, RSU_u calculate the symmetric key and share with RSU_uas $S'_{kRR} = th\ (TRSU_u, TRSU_v)\ (= S_{kRR})$ by pre-loaded polynomial share $\wp$ $(TRSU_u, y)$ and $S'_{KV} = h(S'_{kRR}\ ||\ N_{RSUu})$ on the basis of its own already generated random nonce N_{RSUu}. In addition to this, RSU_u proves if $S'_{KV} = S_{KV}$. If the condition is satisfied, it showed that both RSU_u and RSU_v used valid symmetric keys for their onward communication.
4. After receiving $\{L_4, L_5, T_2\}$, OBU_i also validates T_2. If it is valid, then OBU_i calculate time-dependent key $SK'_{r2} = h\ (r'||T_2)$ on the basis of T_2 and $J'_2 = SK'_r \oplus L_4 = h(N_{RSUj}\ ||\ \gamma\ ||T_1\ ||T_2)$. It further calculates a session key $S'_{kVR} = h(h(\ N_{RSUj}\ ||\ \gamma\ ||T_1\ ||T_2)\ ||\ J_1||\ J'_2\ ||TA\ ^*_{id})$ and $L_6 = h(S'_{kVR}\ ||T_2)$. If condition $L_6 = L_5$ is satisfied then V_i successfully authenticate RSU_j. The OBU_i again generates the current timestamp T_3 to calculates $L_7 = h(S'_{kVR}\ ||T_3)$ and sends $\{L_7, T_3\}$ to RSU_j through an open channel.
5. Upon receiving a message $\{L_7, T_3\}$, RSU_j Validates T_3. If it is valid, then RSU_j calculates $L_8 = h(S_{kVR}\ ||T_3)$ and checks whether $L_8 = L_7$. If the condition is satisfied, then the session key computed by OBU_i is correct.

4.4. Password Update Phase

In SELWAK, after the registration phase, the Vehicle's OBU_i can update password without using a verification table. The legal user changes the password periodically to improve the security of the system. The following steps are used:

1. Drv_i provides provides an identity drv_{id} and an old password PWD_i^{old}. The OBU_i then computes $s_i^* = f_i \oplus h(PWD_i^{old}\,||drv_{id})$, $E_1^* = E_1^{'} \oplus h(drv_{id}\,||\,s_i^*)$, $MPWD_i^{old} = h(PWD_i^{old}\,||\,s_i^*)$, $TA_{id}^* = TA_{id}^{'} \oplus h(drv_{id}||\,s_i^*)$, $Mdrv_{id}^* = Mdrv_{id}^{'} \oplus h(PWD_i^{old}\,||drv_{id}\,||s_i^*)$, $E_2^* = h(Mdrv_{id}^*\,||E_1^*||\,TA_{id}^*)$, $E_3^{old} = h(drv_{id}||\,MPWD_i^{old}\,||\,TA_{id}^*\,||\,E_1^*)$ and $E_4^{old} = h\left(E_3^{old}\,||\,E_2^*\right)$. OBU_i checks if $E_4^{old} = E_4$. If the condition is not satisfied, the password updating process is stopped. Else, Drv_i is a authentic user and allowed the OBU_i to update the password.
2. The driver Drv_i is requested to give a new password PWD_i^{new}. Then, it computes $Mdrv_{id}^{**} = Mdrv_{id}^* \oplus h(PWD_i^{new}||drv_{id}||s_i^*)$, $TV_i^* = TV_i' \oplus MPWD_i^{old}$, $TV_i^{**} = TV_i^* \oplus h(TV_i^* \oplus s_i^*)$, $f_i^{new} = h(PWD_i^{new}||drv_{id} \oplus s_i^*))$, $MPWD_i^{new} = h(PWD_i^{new}||s_i^*)$, $E_3^{new} = h(drv_{id}||MPWD_i^{new}||TA_{id}^*||E_1^*)$, $E_4^{new} = h(E_3||E_2^*)$, $A^* = A \oplus \left(MPWD_i^{old} \oplus PWD_i^{new}\right)$ $= r \oplus E_2 \oplus PWD_i^{new}$ and $A** = A\prime \oplus \left(PWD_i^{old} \oplus PWD_i^{new}\right) = r' \oplus E_2 \oplus PWD_i^{new}$.
3. Finally, OBU_i replaces PWD_i', TV_i', f_i, A, A' and E_4 with drv_{id}^{**}, TV_i^{**}, f_i^{new}, A^*, A^{**} and E_4^{new} in its memory. Therefore, OBU_i contains the message $\{Mdrv_{id}^{**}, TV_i^{**}, TA_{id}', f_i^{new}, A^*, A^{**}, A_1', E_4^{new}, h(\cdot)\}$ after the password update. The pictorial representation of algorithm is given in Figure 6.

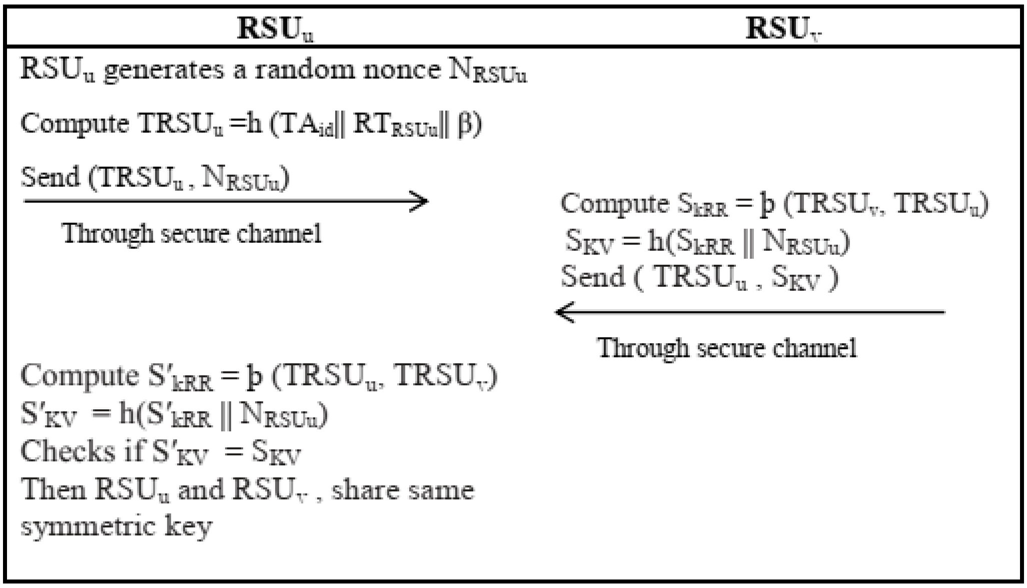

RSU$_u$
RSU$_v$
RSU$_u$ generates a random nonce N$_{RSUu}$
Compute TRSU$_u$ =h (TA$_{id}$|| RT$_{RSUu}$|| β)
Send (TRSU$_u$, N$_{RSUu}$)
Through secure channel
Compute S$_{kRR}$ = Þ (TRSU$_v$, TRSU$_u$)
S$_{KV}$ = h(S$_{kRR}$ || N$_{RSUu}$)
Send (TRSU$_u$, S$_{KV}$)
Through secure channel
Compute S′$_{kRR}$ = Þ (TRSU$_u$, TRSU$_v$)
S′$_{KV}$ = h(S′$_{kRR}$ || N$_{RSUu}$)
Checks if S′$_{KV}$ = S$_{KV}$
Then RSU$_u$ and RSU$_v$, share same symmetric key

Figure 6. RSU2RSU Key Establishment Phase.

5. Security Analysis

The RoR model [21] was used for the formal security analysis of SELWAK. We also show that our scheme is secure against well-known attacks.

5.1. Formal Security Analysis

Formal security analysis of SELWAK is presented using the Real-or-Random (RoR) model. The security of the session key is shown using the RoR model for the proposed scheme. There are two main participants in our scheme: Vehicle V_i and Roadside Unit RSU_j. The RoR [35] has the following components.

5.1.1. Participants

Let e^t_{vi} and e^u_{RSUj} be the instance t and u of the V_i and RSU_j, and called as oracles.

5.1.2. Accepted State

The e^t is an instance that is called an accepted state. Upon reception of the last message, it changes into an accepted state. The e^t concatenate the entire sent and received messages in proper order and for the current session form a session identification of e^t.

5.1.3. Partnering

Two of the instances e^{t1} and e^{t2} are called the partners of each other if they fulfill the following conditions.

- Both of e^{t1} and e^{t2} are in valid accepted states.
- Both of e^{t1} and e^{t2} mutual authenticate and share identical session identification.
- Both of e^{t1} and e^{t2} are mutual partners [36].

5.1.4. Freshness

If attacker A cannot apply the key generated for a particular session of two nodes on the bases reveal query then e^t_{vi} and e^u_{RSUj} are called fresh.

5.1.5. Adversary

Adversary A has full control over the communication between the partners and has the ability to alter the message. Adversary has the following access to queries:

- EX (e^t_{vi}, e^u_{RSUj}): An adversary executes this query to obtain a message that is exchanged between two original partners. This is called an eavesdropping attack.
- RL (e^t): An adversary using this query gets the current session key generated by e^t.
- SN (e^t, message): By executing this query, an adversary sends a message to the participant and receives the message. This is called an active attack.
- OBU (e^t_{vi}): An adversary executes this query to extract stored information in OBU. This is called a stolen attack.
- Test (e^t):It models the semantic security ofa session key. After starting the experiment, coin c is flipped, and only the adversary can know the output. This is helpful for determining the output of a test query.

5.1.6. Session Key's Semantic Security

The main task of an attacker is to differentiate the real session key from the random session key of an instance in the RoR model. An adversary has several test queries to either e^t_{vi} and e^u_{RSUj}. The random bit c and the output of the test query should be consistent. When an experiment is over, an adversary outputs a guessed bit $c\prime$ and wins the game if $c\prime = c$. Suppose Win is an event in which an adversary can win a game. The advantage of Adversary is that it breaks the semantic security of the proposed authentic key exchange schemes. Authentic key exchange is defined by $ad^{AKE}_{TA} = |2pr[Win] - 1|$. TA is secure if $ad^{AKE}_{TA} \leq \theta$ for a sufficient smart real number θ > 0.

5.1.7. Random Oracle

All the participants, including the adversary, will have to access a one-way hash function, which is called the random oracle model [36].The security proof of Theorem 1 presented in [20] is the same. The breaking of the semantic security of the session key for V2V and V2R is proved in Theorem 1 [37].

Theorem 1. *In the RoR model, intruder A runs in polynomial time t against the SELWAK. Let Q_h, $\mid Hash \mid$, Dec, $\mid Dec \mid$ and Q_{SN} be a number of the H queries, the range space of $h(\cdot)$, distributed password dictionary, size of dictionary, and number of sent queries. An adversary's advantage*

ad_{TA}^{AKE} break the semantic security of the session key between OBU and RSU in the proposed scheme is defined as

$$ad_{TA}^{AKE} \leq Q_h^2/|Hash| + \frac{2.Q_{SN}}{|Dec|}. \quad (1)$$

Proof. As in the Chang and Le scheme [36], here the sequences of the four games says G_i = (0,1,2,3). Win_i is an event where an adversary can successfully guess a bit c in game G_i. Below is a detailed description of these games. □

Game G_0: In the random oracle model, it is considered a real attack of the adversary on the proposed scheme. An adversary first guess bit c at the start of the game. By definition, we have

$$ad_{RSU}^{AKE} = |2prb[Win_0] - 1| \quad (2)$$

Game G_1: In this game, an eavesdropping attack of an adversary is simulated by executing an EX (e_{vi}^t, e_{RSUj}^u) query. At the end of the game, the adversary makes a test query. An adversary will have to know whether the test query's output is the real session key of the vehicle and RSU or a random number. We get

$$Prb[Win_0] = Prb[Win_1] \quad (3)$$

Game G_2: In this game, an active attack on an adversary is simulated. An adversary tries to cheat the participants to receive the altered message. To verify the collision in the hash output, an adversary is allowed to query several oracles. When the birthday paradox is applied, we have

$$|Prb[Win_1] - Prb[Win_2]| \leq Q_h^2/2|Hash| \quad (4)$$

Game G_3: In this game, the Corrupt OBU query is simulated. An adversary extracts the information stored in OBU_i. It is difficult to calculate the correct password. If the system only allows a specific password as an input, we can get

$$|Prb[Win_2] - Prb[Win_3]| \leq \frac{Q_{SN}}{|Dec|} \quad (5)$$

An adversary can simulate all the games except that an adversary needs to guess c to win the game after the test query to oracle; we get $Prb[Win_3] = 1/2$ from Equation (1), we have

$$(1/2)ad_{RSU}^{AKE} = |prb[Win_0] - 1/2|. \quad (6)$$

With the help of triangular inequality, we have $|Prb[Win_1] - Prb[Win_3]| \leq |Prb[Win_1] - Prb[Win_2]| + |Prb[Win_2] - Prb[Win_3]| \leq Q_h^2/2|Hash| + \frac{Q_{SN}}{|Dec|}$. As a result, Equations (2) and (6) become

$$\left|prb[Win_0] - \frac{1}{2}\right| \leq Q_h^2/2|Hash| + \frac{Q_{SN}}{|Dec|}. \quad (7)$$

Finally, from Equations (6) and (7). we get $ad_{TA}^{AKE} \leq Q_h^2/|Hash| + \frac{2.Q_{SN}}{|Dec|}$.

5.2. Informal Security Analysis

In this section, the proposed scheme's resilience against some well-known attacks is discussed, and the security features of the proposed scheme are also compared with existing schemes.

1. *Replay Attack*: In the V2V and V2RSU authentication processes, the corresponding messages MSG_1 = (L_1, L_2, T_1) and MSG_2 = (L_7, T_3) have timestamps T_1 and T_3. If an attacker wants to reply to the message with delay, then the timestamp attached to the message will fail. Therefore, our scheme is robust against reply attacks.

2. *Impersonation Attack*: During the V2V authentication an attacker can impersonate the vehicle; to do so, an attacker must create an authentic message $\mathrm{MSG}_1 = (L_1, L_2, T_1)$. For creating MSG_1 an attacker requires secret r. An attacker cannot calculate message MSG_1 even if he/she generates his/her own timestamp and random none as secret r, $\mathrm{Mdrv}_{\mathrm{id}}$, $\mathrm{T}V_i$ and $\mathrm{TA}_{\mathrm{id}}$.
3. *Man-in-the-middle Attack*: In the proposed scheme, two messages, namely $\mathrm{MSG}_1 = (L_1, L_2, T_1)$ and $\mathrm{MSG}_2 = (L_7, T_3)$ are required for V2V authentication. If an attacker wants to modify the message, then he/she first generates a current timestamp and random nonce. An attacker cannot calculate $\mathrm{KS}_{\mathrm{r1A}} = h(r \,|\,|\, T_{1\mathrm{A}}$ as he/she did not have a secret key. Thus, an attacker cannot modify messages.
4. *Stolen Verifier Attack*: The information $(Mdrv'_{id}, Mdrv'_{id}, TV'_i, TA'_{id}, f_i, Y, E'_1, E_4, h(\cdot))$ is stored in OBU_i of the vehicle. We assume that an attacker can steal stored information from OBU_i. However, the one-way hash function protects the secrets PWD_i, r, r', TA_{id}, drv_{id}. An attacker cannot guess the secrets $\mathrm{PWD_i}$, r, r', TA_{id}, drv_{id} correctly due to the collision resistance property of a one-way hash function.
5. *Stolen OBU Attack*: Suppose that an attacker has stolen the OBU_i of the vehicle. An attacker can extract the stored information $(Mdrv'_{id}, Mdrv'_{id}, TV'_i, TA'_{id}, f_i, Y, E'_1, E_4, h(\cdot))$ from OBU_i. It is difficult for an attacker to drive drv_{id} from $Mdrv_{id}$ without having the secret α.
6. *Untraceability*: In the V2V and V2RSU authentication phases of the proposed scheme, two messages are followed: $\mathrm{MSG}_1 = (L_1, L_2, T_1)$ and $\mathrm{MSG}_2 = (L_7, T_3)$. All messages are distinct in each session, and the attacker cannot trace the RSU or vehicle.
7. *Anonymity*: In the proposed scheme, the messages for V2V and V2RSU authentication do not involve the identities of the RSU and the user. Therefore, it is infeasible for an attacker to drive the real identities of the RSU and the user. Hence, the proposed scheme satisfies the anonymity property.
8. *Insider Attack*: SELWAk is robust against insider attacks. The neighboring vehicles cannot get unauthorized access to the sensitive information of a particular vehicle by stealing its credentials.

6. Performance Analysis

In this section, the performance of the proposed scheme and the existing schemes are analyzed. The proposed scheme is implemented with the following specifications: 2.66 GHz Intel(R) Core TM 2 Quad processor with 4 GB of memory using Windows 10. We compared SELWAK with some existing schemes based on computational costs, as well as communication costs. The performance result shows that our scheme is efficient in terms of computational cost and communication overhead compared to existing schemes.

6.1. Computation Overhead

The notations T_{pm}-ECC, T_{pa}-ECC, and T_{h} used in Table 2 represent Elliptic Curve Cryptographic points multiplication, Elliptic Curve Cryptographic points addition, and one-way hash function, respectively. As bitwise XOR operations take negligible time, we have not considered them for performance evaluation.

We have considered the values 0.6718 ms, 0.0031 ms, and 0.001 ms for various cryptographic operations like T_{pm}-ECC, T_{pa}-ECC, and T_{h} from existing experimental values [5,19,27]. The computational costs of SELWAK and some existing schemes are compared in Table 2. The schemes to which we compare our work include those of Zhong et al. [17], Ali et al. [19], Cui et al. [20], Xie et al. [21], Li et al. [24], Al-shareeda et al. [27], and Jalawai et al. [32]. An authentication scheme with privacy preservation property based on identity was proposed in [17]. To reduce communication overhead, a registration list is used instead of a revocation list. The security features of VANET were not affected by malicious vehicles. Moreover, their scheme did not use bilinear pairing operations, which takes more execution time. An elliptic curve cryptography-based and identity-based signature with a conditional privacy-preserving authentication scheme and general one-way hash functions for V2V communication is proposed in [19]. Cui et al. [20] presented a secure authentication approach with privacy properties for VANET. This scheme uses ECC and identity-based signatures for both V2I and V2V communication. The authors used the binary search method and the cuckoo filter method to improve the success rate of batch signature verification. Xieet al. [21] proposed a robust and secure conditional privacy-preserving scheme using identity-based authentication. The reliability and integrity of the messages are ensured using identity-based signatures for V2V and V2I communication. Performance analysis shows that this scheme has a high computational cost and communication overhead. To ensure secure communication in VANET, an authentication scheme based on ECC that satisfies privacy preservation is proposed in [27]. An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks has been proposed in [32]. Similarly, an authentication approach for global mobility networks was proposed in [38]. This scheme is based on an elliptic curve crypto system and therefore takes much execution time to perform major cryptographic operations.

Table 2. Computation Cost Comparison.

Scheme	Total Computational Overhead	Total Execution Time (ms)
[17]	$500T_h$	≈0.5
[19]	$1T_{pm} - \text{ECC} + 1T_{pa} - \text{ECC}$	≈0.6749
[20]	$2T_{pm} - \text{ECC} + 1T_{pa} - \text{ECC}$	≈1.3467
[21]	$2T_{pm} - \text{ECC} + 1T_{pa} - \text{ECC} + T_h$	≈1.3477
[32]	$6\ T_{pm} - \text{ECC} + 1\ T_{pa} - \text{ECC} + 4\ T_h$	≈4.0348
[24]	$7\ T_{pm} - \text{ECC} + 2\ T_{pa} - \text{ECC} + 4\ T_h$	≈4.7128
[27]	$5\ T_{pm} - \text{ECC} + 1\ T_{pa} - \text{ECC} + 4\ T_h$	≈3.3661
[38]	$4T_{pm} - \text{ECC} + 12T_h$	≈2.6992
SELWAK	$16\ T_h + 11\ T_{XOR}$	≈0.016

The total computational cost for SELWAK is $16T_h + 11T_{XOR}$, which is less than that of all compared schemes. The performance result shows that our scheme is efficient in terms of computational cost and communication overhead compared to existing schemes.

6.2. Communication Overhead

In this section, we have compared our scheme with [17,19–21,24,27,32], schemes. The authentication message of [17] is {T, m, σ}. Thus, the size of the authentication message is 160 × 2 + 4 = 352 bits. In [19] the size of the authentication message is 2 × 40 + 2 × 20 + 4 + 160 = 1152 bits. In [20] the size of message authentication is 40 + 2 × 20 + 4 + 160 + 256 = 1084 bits. The communication cost analysis shows that the corresponding authentication message of [21] scheme is [T_i, δ]. Thus, the size of the message is 320 × 2 + 100 × 2 + 32 = 992 bits. In our scheme, the authentication and key establishment phase require two messages $\text{MSG}_1 = (L_1, L_2, T_1)$ and $\text{MSG}_2 = (L_7, T_3)$ and need (160 + 160 + 32) = 352 bits and (160 + 32) = 192 bits. Thus, the total computational cost for V2V and V2RSU authentication phases is equal to (352 + 192) = 544 bits. The communication overhead of various schemes have been shown in Table 3.

As shown in Figure 7, the execution time taken by our proposed scheme is much less than that of the other four schemes. The proposed scheme is also efficient, even in the worst case, compared to other schemes.

Table 3. Communication Cost Comparison.

Schemes	Communication Overhead (Bits)
[17]	352 bits
[19]	1152 bits
[20]	1084 bits
[21]	992 bits
[32]	1152 bits
[24]	1024 bits
[27]	832bits
[38]	2176 bits
SELWAK	544 bits

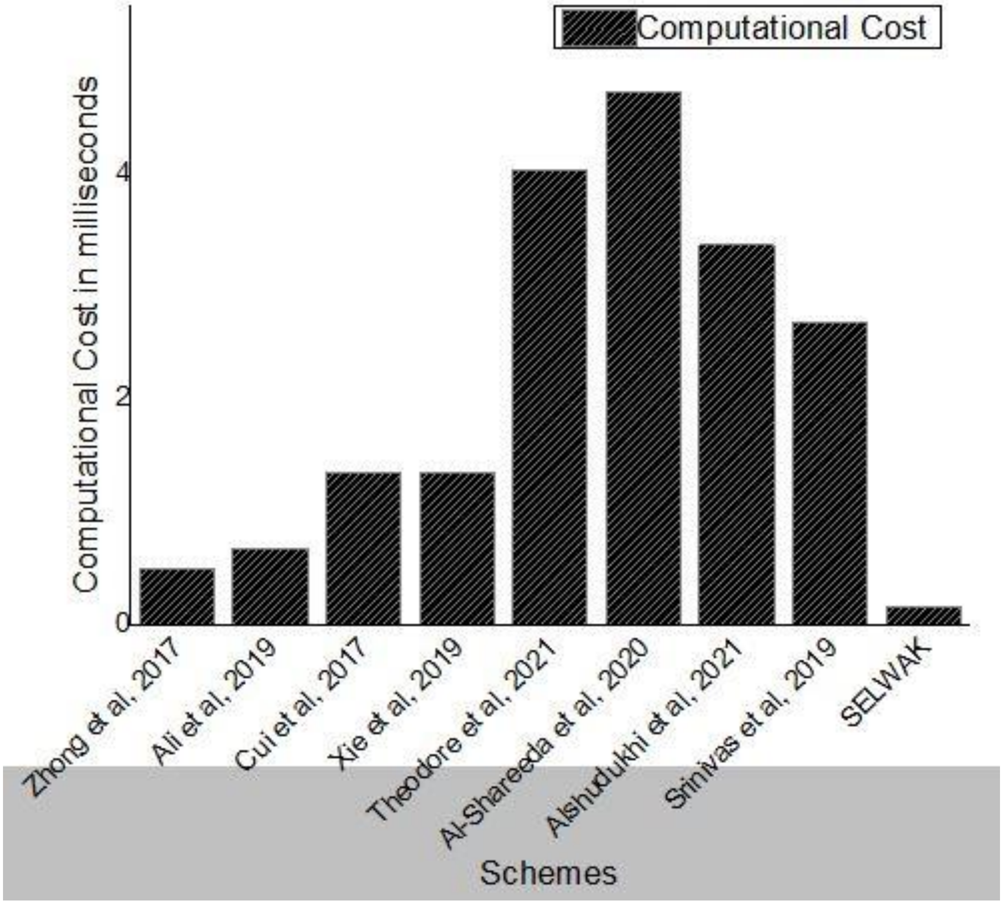


Figure 7. Computation Cost Comparison.

In Figure 8, we show total extra bits sent with the original message during vehicle communication for various schemes.

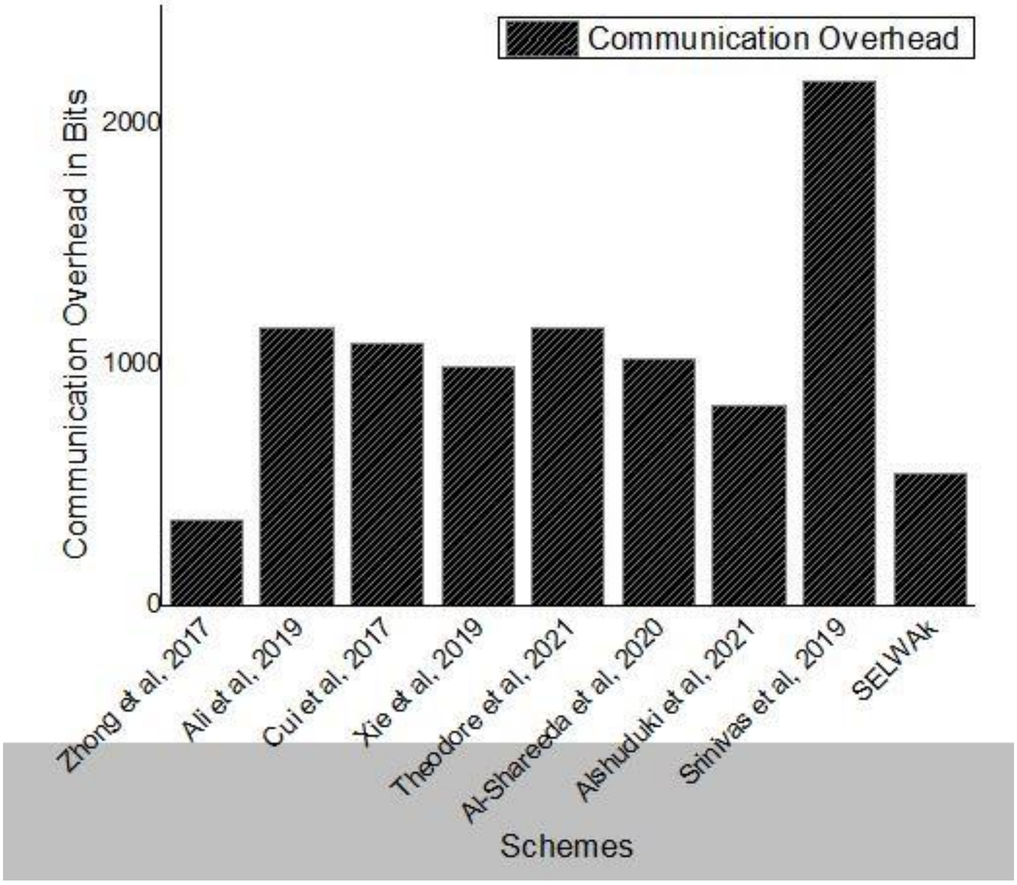


Figure 8. Communication Overhead Comparison.

7. Conclusions

We proposed a novel SELWAK scheme for VANETs. Our scheme is efficient in terms of computational cost and communication overhead due to the one-way hash function and bitwise XOR operations. The SELWAK has extra features, such as mutual authentication and Vehicles and roadside unit anonymity properties. The proposed scheme is robust against driver impersonation attacks, OBU impersonation attacks, OBU capture attacks, RSU impersonation attacks, anonymity, and untraceability, perfect forward and backward secrecy, eavesdropping attacks, and insider attacks. The formal analysis of the proposed scheme was conducted using the RoR model. Therefore, the proposed scheme works efficiently for intelligent transportation systems.

In future work, anonymous mutual authentication will be carried out using BAN Logic and some simulation platforms, such as NS2, SUMO, and OMNET++, to simulate VANETs.

Author Contributions: Conceptualization, S.A.J. and M.A.; methodology, N.U.A.; software, J.S.; validation, S.A.J., A.A. and M.M.; formal analysis, S.A.J.; investigation, N.U.A.; resources, J.S.; data curation, S.A.J.; writing—original draft preparation, S.A.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zafar, F.; Khattak, H.A.; Aloqaily, M.; Hussain, R. Carpooling in Connected and Autonomous Vehicles: Current Solutions and Future Directions. *ACM Comput. Surv.* **2022**, 1–33. [CrossRef]
2. King, J.; Awad, A.I. A distributed security mechanism for resource-constrained IoT devices. *Informatica* **2016**, *40*, 133–143.
3. Zahra, S.; Gong, W.; Khattak, H.A.; Shah, M.A.; Song, H. Cross-Domain Security and Interoperability in Internet of Things. *IEEE Internet Things J.* **2021**. [CrossRef]
4. Chaubey, N.K. Security analysis of vehicular ad hoc networks (VANETs): A comprehensive study. *Int. J. Secur. Its Appl.* **2016**, *10*, 261–274. [CrossRef]
5. Cui, J.; Tao, X.; Zhang, J.; Xu, Y.; Zhong, H. HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs. *Veh. Commun.* **2018**, *14*, 15–25. [CrossRef]
6. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. *Comput. Netw.* **2018**, *141*, 199–221. [CrossRef]
7. Sicari, S.; Rizzardi, A.; Miorandi, D.; Coen-Porisini, A. Internet of Things: Security in the keys. In Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Malta, Malta, 13–17 November 2016; pp. 129–133.
8. Wang, Y.; Zhong, H.; Xu, Y.; Cui, J. ECPB: Efficient conditional privacy-preserving authentication scheme supporting batch verification for VANETs. *Int. J. Netw. Secur.* **2016**, *18*, 374–382.
9. Islam, S.H.; Obaidat, M.S.; Vijayakumar, P.; Abdulhay, E.; Li, F.; Reddy, M.K.C. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. *Futur. Gener. Comput. Syst.* **2018**, *84*, 216–227. [CrossRef]
10. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2467–2476. [CrossRef]
11. Islam, S.H.; Biswas, G.P. A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks. *Ann. Telecommun.* **2012**, *67*, 547–558. [CrossRef]
12. Malik, A.; Pandey, B. Security Analysis of Discrete Event Based Threat Driven Authentication Approach in VANET Using Petri Nets. *Int. J. Netw. Secur.* **2018**, *20*, 601–608.
13. Zhang, L.; Men, X.; Choo, K.-K.R.; Zhang, Y.; Dai, F. Privacy-Preserving Cloud Establishment and Data Dissemination Scheme for Vehicular Cloud. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 634–647. [CrossRef]
14. Liu, J.; Li, J.; Zhang, L.; Dai, F.; Zhang, Y.; Meng, X.; Shen, J. Secure intelligent traffic light control using fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 817–824. [CrossRef]
15. Wazid, M.; Das, A.K.; Kumar, N.; Odelu, V.; Reddy, A.G.; Park, K.S.; Park, Y. Design of Lightweight Authentication and Key Agreement Protocol for Vehicular Ad Hoc Networks. *IEEE Access* **2017**, *5*, 14966–14980. [CrossRef]
16. Ibrahim, S.; Hamdy, M.; Shaaban, E. Towards an optimum authentication service allocation and availability in VANETs. *Int. J. Netw. Secur.* **2017**, *19*, 955–965.
17. Zhong, H.; Huang, B.; Cui, J.; Xu, Y.; Liu, L. Conditional Privacy-Preserving Authentication Using Registration List in Vehicular Ad Hoc Networks. *IEEE Access* **2017**, *6*, 2241–2250. [CrossRef]
18. Gope, P.; Amin, R.; Islam, S.H.; Kumar, N.; Bhalla, V.K. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Gener. Comput. Syst.* **2018**, *83*, 629–637. [CrossRef]
19. Ali, I.; Lawrence, T.; Li, F. An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs. *J. Syst. Arch.* **2019**, *103*, 101692. [CrossRef]
20. Cui, J.; Zhang, J.; Zhong, H.; Xu, Y. SPACF: A Secure Privacy-Preserving Authentication Scheme for VANET With Cuckoo Filter. *IEEE Trans. Veh. Technol.* **2017**, *66*, 10283–10295. [CrossRef]
21. Xie, L.; Ding, Y.; Yang, H.; Wang, X. Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs. *IEEE Access* **2019**, *7*, 56656–56666. [CrossRef]
22. Alshudukhi, J.S.; Mohammed, B.A.; Al-Mekhlafi, Z.G. An Efficient Conditional Privacy-Preserving Authentication Scheme for the Prevention of Side-Channel Attacks in Vehicular Ad Hoc Networks. *IEEE Access* **2020**, *8*, 226624–226636. [CrossRef]
23. Bayat, M.; Barmshoory, M.; Rahimi, M.; Aref, M.R. A secure authentication scheme for VANETs with batch verification. *Wirel. Netw.* **2014**, *21*, 1733–1743. [CrossRef]
24. Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H.; Abdullah, N.; Hamdi, M.M.; Al-Hiti, A.S. NE-CPPA: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (VANETs). *Appl. Math.* **2020**, *14*, 1–10.
25. Al-Shareeda, M.A.; Anbar, M.; Alazzawi, M.A.; Manickam, S.; Al-Hiti, A.S. LSWBVM: A Lightweight Security Without Using Batch Verification Method Scheme for a Vehicle Ad Hoc Network. *IEEE Access* **2020**, *8*, 170507–170518. [CrossRef]
26. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
27. Alshudukhi, J.S.; Al-Mekhlafi, Z.G.; Mohammed, B.A. A Lightweight Authentication With Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography. *IEEE Access* **2021**, *9*, 15633–15642. [CrossRef]
28. Cui, J.; Wang, Y.; Zhang, J.; Xu, Y.; Zhong, H. Full Session Key Agreement Scheme Based on Chaotic Map in Vehicular Ad Hoc Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 8914–8924. [CrossRef]

29. Vijayakumar, P.; Azees, M.; Chang, V.; Deborah, J.; Balusamy, B. Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks. *Clust. Comput.* **2017**, *20*, 2439–2450. [CrossRef]
30. Vijayakumar, P.; Azees, M.; Kozlov, S.A.; Rodrigues, J.J.P.C. An Anonymous Batch Authentication and Key Exchange Protocols for 6G Enabled VANETs. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 1630–1638. [CrossRef]
31. Pulagara, S.B.; Alphonse, P. An intelligent and robust conditional privacy preserving authentication and group-key management scheme for vehicular ad hoc networks using elliptic curve cryptosystem. *Concurr. Comput. Pract. Exp.* **2019**, *33*, e5153. [CrossRef]
32. Theodore, S.K.A.; Gandhi, K.R.; Palanisamy, V. A novel lightweight authentication and privacy-preserving protocol for vehicular ad hoc networks. *Complex Intell. Syst.* **2021**, 1–11. [CrossRef]
33. Ren, Y.; Li, X.; Sun, S.-F.; Yuan, X.; Zhang, X. Privacy-preserving batch verification signature scheme based on blockchain for Vehicular Ad-Hoc Networks. *J. Inf. Secur. Appl.* **2021**, *58*, 102698. [CrossRef]
34. Srinivas, J.; Mishra, D.; Mukhopadhyay, S.; Kumari, S.; Guleria, V. An Authentication Framework for Roaming Service in Global Mobility Networks. *Inf. Technol. Control* **2019**, *48*, 129–145. [CrossRef]
35. Abdalla, M.; Fouque, P.-A.; Pointcheval, D. Password-based authenticated key exchange in the three-party setting. In Proceedings of the International Workshop on Public Key Cryptography, Edinburgh, UK, 4–7 May 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 65–84.
36. Chatterjee, S.; Roy, S.; Das, A.K.; Chattopadhyay, S.; Kumar, N.; Vasilakos, A.V. Secure Biometric-Based Authentication Scheme Using Chebyshev Chaotic Map for Multi-Server Environment. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 824–839. [CrossRef]
37. Chang, C.-C.; Le, H.-D. A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks. *IEEE Trans. Wirel. Commun.* **2015**, *15*, 357–366. [CrossRef]
38. Li, J.; Choo, K.-K.R.; Zhang, W.; Kumari, S.; Rodrigues, J.J.; Khan, M.K.; Hogrefe, D. EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *Veh. Commun.* **2018**, *13*, 104–113. [CrossRef]