Cyber Security and Applications 1 (2023) 100001

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Bilinear pairing-based access control and key agreement scheme for smart transportation

Palak Bagga[a], Ashok Kumar Das[b,*], Joel J.P.C. Rodrigues[c,d]

[a] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, Gachibowli, Hyderabad, 500032, Telangana, India
[b] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, Gachibowli, Hyderabad, 500032, Telangana, India
[c] College of Computer Science and Technology, China University of Petroleum (East China), Qingdao 266555, China
[d] Instituto de Telecomunicações, Covilhã, 6201-001, Portugal

ARTICLE INFO

Keywords:
Internet of Vehicles (IoV)
Smart transportation
Intelligent Transportation System (ITS)
Authentication
Bilinear pairing
Security

ABSTRACT

Internet of Vehicles (IoV) enabled Intelligent Transportation System (ITS) allows smart vehicles to communicate with other vehicles on road, humans (customers or pedestrians), infrastructure (parking areas, traffic lights etc), Internet, Cloud etc. The vehicles communicate with other entities over wireless open channels directly or indirectly through messages or beacons. Open channel allows various attacks, like replay, man-in-the-middle, impersonation, fabrication etc., during communication. Also, malicious vehicles can be deployed in the network to misuse or have an unauthorized access to the services. To mitigate these issues, we propose a new remote access control scheme that ensures the secure communication among the vehicles. The vehicles are dynamic in nature in an IoV paradigm, that is, they are not under fixed domains. Therefore, whenever a vehicle changes its location it has to register to the nearest trusted authority (TA) in offline or secured channel mode. To make it applicable, we propose *remote registration* of the vehicles via the TA. Access control mechanism occurs in two phases: 1) node authentication phase, where vehicles are remotely authenticated by TA and 2) key agreement phase, where after successful mutual authentication they compute a session key by using cryptographic techniques and pre-loaded information. The computed secret session keys are used for ensuring secure communications in future between two vehicles in a cluster as well. Informal security analysis along with formal security verification using the broadly-used Automated Validation of Internet Security Protocols and Applications (AVISPA) show that our access control scheme is secured against various potential attacks. We also show the competency of our scheme by comparing it with other existing schemes in terms of computation and communication costs.

1. Introduction

Internet of Things (IoT) combines various technologies like embedded systems, wireless sensors networks, control system appliance automation, real time analysis, artificial intelligence, machine learning etc. Likewise, Internet of vehicle (IoV) is a concept/subset derived from the vast emerging concept IoT. It is an extended vehicular adhoc network (VANET) that modifies a vehicle into a smart vehicle by installing an on board unit (OBU) in them, thus making them eligible to communicate with other vehicles, humans (customers or pedestrians), infrastructure (parking areas, traffic lights), Internet, Cloud etc. Vehicles collect the information from the surroundings, and other vehicles. The collected information is comprehended to provide multiple services to the customers. IoV advances to claim a new concept of Intelligent Transportation System (ITS) in smart cities. Smart vehicles (with installed OBU), vehicle's intelligence, diverse communication patterns, connection to Internet together forms ITS. ITS regulates the coordination between vehicular sensors, on board units, trusted platform module (TPM) etc.

ITS aims to provide safe, secured and luxurious on road experience to users. It provides safety by reducing accidents, generating warnings to avoid mis-happenings, emergency warnings, rule violation warnings etc. It offers comfort and infotainment applications like intelligent navigation, parking, file sharing, toll collection etc. It provides 24x7 high speed Internet access and multimedia services. It efficiently manages traffic on road, saves time and cost. IoV is quite similar to IoT as it borrows its technologies and benefits. But, at the same time it also has to deal with other crucial and strict requirements like limited communication time, strict real time operations, specific bandwidth, heavy volume of data, scalability and most crucially 'security issues'. Various security issues arise because the vehicles communicate with other entities over

* Corresponding author.
E-mail addresses: palak.bagga@research.iiit.ac.in (P. Bagga), iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in (A.K. Das), joeljr@ieee.org (J.J.P.C. Rodrigues).

https://doi.org/10.1016/j.csa.2022.100001
Received 1 November 2021; Received in revised form 14 December 2021; Accepted 3 January 2022
Available online 4 April 2022

wireless open channel directly or indirectly through messages or beacons. Therefore, there is high demand for well managed, reliable and robust *cybersecurity measures in ITS* such as authentication mechanisms, identity preservation techniques, intrusion detection system, access control schemes etc. These mechanisms would provide the required "security and functionality features to smart transportation".

The authors in [10] provided a detailed taxonomy of various security protocols that are necessary to maintain a secured IoV environment. The basic security protocols related to IoV and other networking environments are categorized as key management like the schemes of [19], [32], [34], [16], [26], [43], authentication schemes such as [20], [39], [36], [28], [35], [18], [44], [42], privacy preservation schemes such as [11], [33], [47], [8], [25], [41], intrusion detection systems proposed by [1], [23], [24], and access control schemes.

In this paper, we focus mainly on access control mechanism. An access control scheme ensures a secured environment to provide uninterrupted services. IoV is a dynamic network where the location of the vehicle keeps changing every instant so does the nearest neighbors. Also, due to increasing population, the number of vehicles bought and registered are increasing drastically everyday. Therefore, the need of an hour is to have an access control scheme which ensures that the members joining the cluster are authenticated and legal. On the other hand, an adversary can even deploy malicious nodes in the network to harm the integrity network. So it becomes necessary to be able to differentiate between a genuine and a malicious vehicle. Therefore a successful access control mechanism controls the flow of false, invalid, illegal and unauthorized information within the network. It also manages access permissions, monitors the scalable IoV architecture, handles huge amount of data stream, and also keeps a track of allocation and utilization of resources in the network.

An access control scheme accomplishes the requirement in two steps.

- *Node authentication*: When a new node (a vehicle) wishes to join the network, the node should prove its legitimacy to the neighboring nodes, by authenticating itself to the other existing nodes or TA, after which it is deployed and allowed to communicate and access the network.
- *Key establishment:* After the successful authentication, a newly deployed node and the TA compute a secret session key that is used to ensure secured communication over a public channel. The key computed is to used to encrypt the messages shared further in the process that maintains the confidentiality and resists various attacks.

An efficient access control mechanism should be able to add new nodes through out the network. That is, the increase in the network size should not affect the computation and communication time of the mechanism. It should also resist new node deployment attack where a malicious node should not be allowed to be deployed in the network and no existing node should be compromised. An access control mechanism should be able to maintain the functionality of the network even when few nodes are captured.

1.1. Research contributions

The major contributions of the paper as stated as follows.

- We propose a remote access control scheme which is implemented between a vehicle and its nearest TA. The vehicles are registered via the TA over secure channel. The access control mechanism works in two phases. In the first phase, a remote mutual authentication occurs between TA and a vehicle. After successful authentication, a session key is computed for future communications in the second phase.
- Our proposed scheme facilitates vehicle addition phase and password update phase. The proposed scheme can be also extended in establishing session keys between any two vehicles in a dynamically formed cluster of vehicles with the help of the TA.
- In the later part, we also analyze the security of our scheme. An informal security analysis exhibits that our scheme can resist various well known attacks. Further, a formal security verification using the broadly-accepted "Automated Validation of Internet Security Protocols and Applications (AVISPA)" [6] software tool, shows that our scheme can resist passive/active adversarial attacks.
- A comprehensive performance analysis evaluates computation, communications cost of our scheme in comparison to other existing schemes. We also list down other security and functionality features.

1.2. Paper outline

The layout of the paper is as follows.

- In Section 2 we describe the network and the threat model used in the scheme.
- Next, in Section 3 we give brief description of few existing access control schemes. We also summarize the characteristics of all the scheme in a table for better comprehension.
- Following to this, in Section 4 we describe our proposed scheme in six phases which are defined in Sections 4.1 – 4.6. In Section 5, we then extended this basic scheme where any two vehicles in a cluster can establish session key for their secret communication.
- In Section 6 we provide the security analysis of our scheme. We provide the correctness proof of our verification phase. Severeal propositions give an informal security analysis of our scheme. We also provide formal security analysis of our scheme using the widely-accepted "Automated Validation of Internet Security Protocols and Applications (AVISPA)" tool [6].
- In Section 7 we perform a detailed comparative analysis of our scheme against few existing schemes in terms of computation, communication costs and other security and functionality features.
- The conclusion of the paper is presented in Section 8.

2. System models

The network and threat model is described as follows.

2.1. Network model

A general IoV network comprises of vehicle, RSU, TA. Vehicles are installed with sensors like location based system, monitoring/warning systems, analytic systems, partner systems, speed control, camera, multimedia settings, mass airflow sensor, engine speed sensor, spark knock sensor, coolant sensor, fuel temperature sensor, voltage sensor, smart card device, finger print device etc. The sensors of the vehicles collect the data from the surrounding via on-board unit (OBU) through a data collecting agent. The data collected is processed via inference logics to make decisions and is saved in tampered proof device (TPD). In our scheme, a vehicle remotely registers itself to the nearest trusted authority (TA). They can be single or multiple TAs to supervise a smart city. To preserve the identity, the TAs are the only entities to store the real identities of the vehicles. After getting registered the vehicle is deployed in the the network. IoV enabled ITS supports various types of communications like interactions with other vehicles via *Vehicle to Vehicle (V2V) communication*. The vehicles exchange updated traffic related information. The communication between TA and vehicle occurs via *Vehicle to Infrastructure (V2I) communication*. Vehicle to pedestrian, vehicle to customer communication occurs via *Vehicle to Human (V2H) communication* through which vehicle provides user services and safe transportation facilities to passengers and customers. Vehicles can even exchange information with personal devices through *Vehicle to Personal devices (V2P) communication*. The vehicles are installed with sensors and the communication between them occurs via *Vehicle to Sensor (V2S) communication* [40]. TA checks the authenticity of the messages flown by the vehicle in the network. Our proposed scheme supports remote authentication, therefore, the communication between the vehicle and TA takes place through "wireless medium using the IEEE 802.11p protocol" and "Dedicated Short-Range Communications (DSRC)" [30].

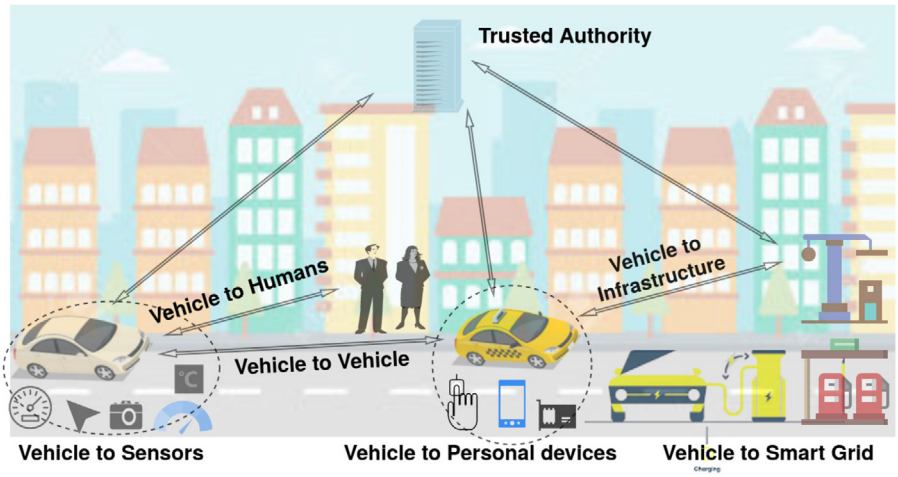

Fig. 1. IoV network model

Figure 1 shows the architecture of smart transportation network model.

2.2. Threat model

We have considered "Dolev-Yao threat (DY) model" [21] as the threat model for the proposed scheme. The model considers the following assumptions.

- The communication channel between the end entities (vehicle or RSU) is considered insecure, open and public.
- The end nodes like vehicles are not trusted, whereas the trusted authorities (TAs) are assumed to be fully trusted entities.
- Following to this the model considers an adversary $\mathcal{A}$, with enough capabilities such the an adversary can perform fabrication, eavesdropping, modification, tampering, deletion and replay attacks on the messages exchanged on the public communication channel.

The vehicles are equipped with tampered proof device in on board units where they store secret information and the stored information cannot be tampered.

Another threat model considered for this scheme is, "Canetti and Krawczyk's adversary model (CK-adversary model)" [13]; also stated as a "current de facto standard model in modeling authenticated key-exchange protocols". The model extends the capabilities of the adversary as in DY model. The model assumes that the adversary can not only eavesdrop or send the messages flown in the network like in DY model, but can also compromise the secret credentials, secret keys or session keys during the communication. This model is an essential model while analyzing the security of key exchange protocols because compromised secret credentials during communication should have least impact on the session key established.

3. Related work

[45] proposed an "anonymous and lightweight authentication for secure vehicular networks (ASC)" based on difficulty of Diffie-Hellman and Discrete Logarithm (DL) problem. Vehicles are issued with a smart card during registration. The scheme uses geo synchronised timestamps to achieve freshness. Users use their smart card and passwords to log in their vehicles. Vehicle proves its legitimacy to TA via RSU and establishes a secret key for data transmissions during user authentication phase. Messages shared by the vehicle are also authenticated using hash chains in data authentication phase. The scheme suffers from various well known attacks.

[17] addressed the short comings in ASC by [45] and proposed an efficient protocol. They assumed a single TA with multiple RSU model, where TA and RSU always have secured communications. The vehicle sends a request message to RSU which is relayed to TA after checking its authenticity. The reply from the TA is broadcasted to RSU and other near by RSUs. The use of passwords (used in ASC) is removed to avoid password guessing attacks. Instead message authenticated codes (MAC) are added on all the messages exchanged with TAs to assure security and authenticity. The scheme is secured against "insider attack, stolen smart card attack, offline password guessing attack, replay attack and impersonation attack".

[46] designed a password based secure authentication protocol for wireless sensor networks (WSNs) in vehicular communications. The protocol is light weight and efficient in communication an computation cost as it uses XOR operation and hash function. The sink nodes are deployed at fixed locations on the network. Users are authenticated by the sink nodes in the user authentication phase. Following to this, the data collected by authenticated vehicles is sent and collected in the sink node, which is accessed to provide user services in future. [38] claimed that the Yu *et al.*'s scheme cannot resist "sensor capture attack, user traceability attack, impersonation attack, and offline sink node's secret key guessing attack". They proposed a two-factor authentication protocol in WSNs for IoV which overcomes the shortcomings of Yu *et al.*'s scheme. Their scheme by [38] uses biometric templates instead of passwords for authentication. A shared key is established between the user and sink node, also between a vehicle and sink node. Although the scheme is secured against replay, stolen sink node database, stolen smart card attack but it requires lots of storage space in the sink node's memory and incurs heavy computation and communication cost. It does support revocation phases.

[44] proposed an "efficient privacy-preserving mutual authentication scheme for secure V2V communications" where a vehicle is authenticated by a law executor. Once the authentication is successful, the vehicle receives authentication key and becomes a trustful vehicle until the key expires. Further, a trustful vehicle can also authenticate other vehicles by trust extended phase. Two trustful vehicles compute a session key and can have secure communications. Later, [42] proposed a two factor light weight authentication mechanism. The scheme incurs less computation overheads because it uses less expensive cryptographic operations like XOR operations and hashing. After authentication, a key is established between entities for secure communication. The session key computed in the schemes proposed by [42], and [44], is not secured against CK-adversary attack.

[3] proposed a "multi-factor secured and lightweight privacy-preserving authentication scheme (MSPF)". The security of the scheme is

based on multiple authentication factors like physical unclonable functions (PUF), vehicle's private key and one time pseudo identity. The mechanism is decentralized and reduces redundant authentications. After vehicle to central authority mutual authentication phase, a regional key is established which is valid until the vehicle reaches a new region. [27] also proposed an authentication-based secure data dissemination protocol and framework for 5G-enabled VANET. The authenticated vehicles are allowed to exchange messages only after validating each other. The message integrity is checked by calculating the disparity in the communication bits.

[2] designed an "efficient conditional privacy preservation with mutual authentication". The TA divides the system into domains with specified number of RSUs to cover the region. At the time of authentication, the RSU provides a pool of pseudo identities and their corresponding secret keys with expiry to the vehicle, that can be used for communication within the RSU's coverage area. OBU uses the pseudo identity and the secret key from the pool to sign the traffic related message. The malicious vehicles' secret key is not renewed once it has expired. The scheme incurs higher storage cost to store pool of identities and secret keys.

Another "mutual authentication and key agreement scheme" is designed in [9] where a cluster head is chosen in the dynamic cluster of vehicles and the authentication occurs in two levels. In the first level, the cluster head and RSU mutually authenticate each other,and in the other level the authentication happens between two vehicles. After authentication a session key is also established.

Recently, [5] proposed a "privacy-preserving and scalable authentication protocol for the IoV" which is also based on "physical unclonable function (PUF)". PUF is installed in the vehicle's OBU. During registration, vehicles generate crypto identity using PUF, random nonce and hashing, and send it to TA along with few challenge response pairs. All RSUs also store current challenge and nonce. During vehicle to TA authentication phase, all vehicles send their crypto identities to RSU where RSU consolidates request messages, creates a reply by encrypting and hashing, and forwards to RSU gateway. RSU gateway forwards the request to TA after verification. TA generates a token for each verified vehicle containing a challenge and sends the authorized response to the gateway. The gateway forwards the reply to all RSUs in its region after which it is sent to vehicles. The vehicles generates a crypto-identity using the challenge received in the token and acknowledges the TA.

Another "lightweight authentication and attestation scheme for in-transit vehicles" based on PUF is proposed by [4]. IoV cloud servers are database that stores the challenge responses and other information. TA registers vehicles and RSUs. A vehicle sends an authentication request message to RSU whenever it comes in range of any RSU. RSU verifies the vehicle by contacting edge servers (attached to RSU for storage and computation purposes) for registration details. A session key is established which is used for encryption and for an in-transit attestation mechanism that lets the edge servers verify the main ECU firmware installed in the vehicle. For attestation, both vehicle and edge server run an attestation algorithm and verify their checksums computed on memory blocks of ECU firmware using pseudo random functions. The primary ECU firmware after getting verified verifies other ECU's present in the vehicle by same process.

Table 1 summarises the characteristics and limitations of the discussed schemes.

4. The proposed scheme

In this section, we present a new remote access control scheme for smart transportation. The scheme is based on the architecture described in Section 2.1. According to our scheme, initially a vehicle remotely mutually authenticates TA and then both vehicle and TA compute secret session key for secure communication in future. Our scheme occurs in following phases. 1) TA initial set up phase. 2) Registration phase. 3) Log in phase. 4) Authentication and verification phase. 5) Key agreement phase. 6) Password update phase. To avoid replay attacks we use timestamp while exchanging the messages. For that we assume that all the entities are synchronized with their clocks. Towards the end, we also propose a mechanism where the vehicle can anytime change its password if in case the password is lost or breached. The notations used through out the description of the scheme is defined in the Table 2. We now present the proposed scheme in following subsections.

4.1. Initial setup phase

The initial set up phase is performed by the TA authorized for a smart city. The TA sets it private and public key, and initializes the system by computing public parameters by executing the following steps.

- **Step 1:** In the first step, TA chooses a non-singular elliptic curve $E_q(u, v)$ of the form: $y^2 = x^3 + ux + v \pmod q$ such that $4u^3 + 27v^2 \neq 0 \pmod q$. TA also picks an additive group G_1 with point at infinity $\mathcal{O}$ and a multiplicative group G_2 with identity 1 of prime order q. It selects P as a randomly-chosen generator of G_1. It chooses e as a bilinear mapping e: $G_1 \times G_1 \rightarrow G_2$. The bilinear mapping has following properties [12,37]:
  - **Bilinearity**: For all "$P, Q, R \in G_1$, $e(P + Q, R) = e(P, R)e(Q, R)$ and $e(P, Q + R) = e(P, Q)e(P, R)$". In general, for all "$a, b \in Z_q^* = \{1, 2, \cdots, q - 1\}$, $e(aP, bQ) = e(P, Q)^{ab}$".
  - **Non-degeneracy**: If 1_{G_1} denotes the identity in G_1, then $e(P, P) \neq 1_{G_1}$ for all $P \in G_1$.
  - **Computability**: There exists an efficient algorithm to calculate "$e(P, Q)$ for all $P, Q \in G_1$".
- **Step 2:** In the second step, TA randomly selects $pr_{TA} \in Z_q^*$, and sets it as its private key. Using its private key pr_{TA}, TA calculates its public key by $Pub_{TA} = pr_{TA} \cdot P$.
- **Step 3:** Next, TA computes a public verification factor ver as, $ver = e(Pub_{TA}, P)$ and also chooses two cryptographic hash functions, defined as $h(\cdot)$: $\{0, 1\}^* \rightarrow \{0, 1\}^*$, and H: $\{0, 1\}^* \rightarrow G_1$.
- **Step 4:** Finally, TA publicly publishes the system parameters: $\{G_1, G_2, e, q, P, h(\cdot), H(\cdot), Pub_{TA}, ver\}$ at the end of the set up phase.

4.2. Registration phase

The TA is responsible for registering vehicles before their deployment. TA maintains a database where it stores the unique number of vehicles (VUN) assigned by Regional Transport Office (RTO) at the time of buying a vehicle. So, when a new vehicle wishes to join the network it needs to register itself to its corresponding TA. To successfully register vehicle V_i, following steps are performed between V_i and TA.

- **Step 1:** Vehicle V_i chooses its unique identity ID_i and calculates its pseudo identity RID_i as $RID_i = H(ID_i)$. V_i sends its pseudo identity RID_i, and hashed unique number $h(VUN_i)$ to TA via a secure channel. For instance, the information $\{RID_i, h(VUN_i)\}$ can be encrypted with the help of the public key of the TA and the encrypted credentials can be sent via public channel to the TA, and the TA will decrypt the encrypted credentials using its own private key pk_{TA}.
- **Step 2:** On receiving RID_i, $h(VUN_i)$ from V_i, TA checks for the presence of $h(VUN_i)$ in its database. If the entry is present in its database it stops the further process to avoid multiple registration of the same vehicle. If $h(VUN_i)$ is not present in the database, it makes the entry of the vehicle's number in the table and proceeds the registration process. TA computes Reg_{ID_i} as, $Reg_{ID_i} = pk_{TA} \cdot RID_i$. TA chooses a temporary identity TID_i for vehicle V_i, and computes pseudo temporary identity as $RTID_i = h(TID_i \| pk_{TA})$.
- **Step 3:** Finally, TA generates a current timestamp as TS_{TA_1}, and sends the registration reply message $\{TID_i, Reg_{ID_i}, RTID_i, TS_{TA_1}\}$ to V_i over secure channel.

Table 1
Summary of limitations/drawbacks of the state-of-art existing access control schemes

Scheme	Description & Limitations/Drawbacks
[45]	The smart card based scheme uses hardness of CDH and DL problem to achieve authentication. A session key is established for secure communications. The scheme supports password update phase. It cannot resist offline identity guessing attack, session linking attack, stolen smart card attack, and replay attack.
[17]	The smart card based scheme uses MAC to achieve security and authentication in less computation and communication time. The scheme is secured against insider attack, stolen smart card attack, offline password guessing attack, replay attack and impersonation attacks.
[46]	Although the scheme is light weight, but it does not provide anonymity. The scheme cannot resist sensor capture attack, user traceability attack, impersonation attack, and offline sink node's secret key guessing attack. The scheme does not provide smart card revocation process.
[38]	A two factor based scheme implements biometric based authentication. The scheme is secured against replay, stolen sink node database attack and also supports revocation phase. The limitation of the scheme is that it incurs huge computation, communication and sink node's storage costs.
[5]	A challenge response based protocol using PUF. The scheme is scalable and incurs less latency as it accomplishes using fewer authentication request message overheads. The scheme ensures integrity as it concatenates secure hash of a message along with the message. However when vehicle crosses the region of current RSU gateway, it has to undergo the authentication again.
[4]	A light weight authentication scheme based on PUF. After successful authentication of the vehicle the scheme provides an attestation procedure to verify the firmware running in the ECUs of the vehicle.
[44]	A privacy preserving V2V mutual authentication scheme. A vehicle after authentication receives an authentication key and becomes a trustful vehicle. Two trustful vehicles compute a session key for communication. The communication cost is slightly high. Also session key is insecure under CK adversary attack.
[3]	A multi factor decentralised, mutual authentication mechanism that reduces complexity by reducing redundant authentications. The scheme can even withstand TPD physically capture attacks, as it does not depends on sensitive TPD storage.
[2]	A privacy preserving scheme, where authenticated vehicles are given a pool of pseudo identities and secret keys to sign the messages. The storage cost is high as revocation list, pseudo identity and secret key pairs needs to be stored. The secret keys are alloted with expiry time which is renewed time and again.
[27]	The mechanism validates the vehicles before exchanging the messages. It is a light weight protocol using hash function. The scheme does not establish a session key.
[42]	A light weight authentication scheme that establishes a key for secure communication. The scheme has less computation overheads, but the session key is not secured under CK adversary attack.
[9]	A mutual authentication and key agreement scheme which proposes cluster head to *RSU* authentication and V2V authentication. The scheme also proposes dynamic node addition phases.

Table 2
Notations and their meanings

Symbol	Description
TA	Trusted authority managing city
pr_{TA}	private key of TA
Pub_{TA}	private key of TA
V_i, OBU_i	i^{th} vehicle and its On-Board Unit (OBU)
ID_i	Unique identity of V_i
PW_i	Password of V_i
RID_i	Pseudo identity of V_i
TID_i	Temporary identity of V_i
TS_{TA_1}, TS_{TA_2}	Current system timestamps generated by TA
$TS_{V_{i_1}}$	Current system timestamp generated by V_i
ΔTS	Maximum transmission delay associated with a message
r_i, r_1, r_2	Random nonces generated by vehicle V_i
r_3	Random nonce generated by TA
G_1, G_2	An additive group and a multiplicative group of prime order q, respectively
e	Bilinear mapping
P	A generator of G_1
$H(\cdot)$	Map to Point hash function $H(\cdot): \{0,1\}^* \rightarrow G_1$
$h(\cdot)$	A collision-resistant cryptographic one-way hash function
q	A large prime number
$GF(q)$	Galois finite field over prime q
$E_q(a,b)$	A non-singular elliptic curve: $y^2 = x^3 + ax + b \pmod q$ over $GF(q)$ with $a, b \in Z_q = \{0,1,\cdots,q-1\}$ and $4a^3 + 27b^2 \neq 0 \pmod q$
Eg	An additive cyclic elliptic curve group generated by a base point G of prime order q
$P + Q$	"Elliptic curve point addition" of two points $P, Q \in E_q(a,b)$
$k \cdot P$	"Elliptic curve point multiplication"; $k \cdot P = P + P + \cdots P$ (k times), $P \in Eg, k \in Z_q^*$
ΔTS	Maximum transmission delay associated with a message
$x * y$	Modular multiplication of elements $x, y \in Z_q$
$\|, \oplus$	Data concatenation & exclusive-OR operators, respectively

- **Step 4:** After receiving registration reply message $\{TID_i, Reg_{ID_i}, RTID_i, TS_{TA_1}\}$ from TA, OBU_i of V_i first verifies the received timestamp TS_{TA_1} against the current timestamp by the condition: $|TS^*_{TA_1} - TS_{TA_1}| \leq \Delta TS$, where ΔTS is the "maximum transmission delay associated with a message". If the timestamp is valid, OBU_i of V_i asks the user of the vehicle to choose and enter password PW_i associated with V_i. Then OBU_i generates a random nonce $r_i \in Z_q^*$, and computes $VDID_i$, VD_i, VA_i, VB_i as, $VDID_i = Reg_{ID_i} + H(PW_i \| r_i)$, $VD_i = RTID_i \oplus h(ID_i \| PW_i \| r_i)$, $VA_i = h(ID_i \| Reg_{ID_i} \| h(r_i \| PW_i))$, $VB_i = h(ID_i \| r_i \| PW_i) \oplus RID_i$.
- **Step 5:** OBU_i of vehicle V_i stores $\{TID_i, VDID_i, VD_i, VA_i, VB_i\}$ in its memory, and deletes $\{Reg_{ID_i}, RTID_i\}$ permanently from its memory.

Figure 2 summarizes the registration phase.

4.3. Login phase

In login phase, user of vehicle V_i inputs its identity ID_i and password PW_i associated with vehicle in the OBU_i. Then, OBU_i executes the following steps.

- **Step 1:** OBU_i computes random nonce r_i^* as, $r_i^* = r_i \oplus h(IDi \| PW_i)$ and then computes $Reg^*_{ID_i}$ as, $Reg^*_{ID_i} = VDID_i - H(PW_i \| r_i^*)$, $VA_i^* = h(ID_i \| Reg^*_{ID_i} \| h(r_i^* \| PW_i))$ and verifies if $VA_i = VA_i^*$ is valid. If the condition is not valid, the further processing is stopped, as the user has not provided the correct identity or password and is therefore not authenticated. And if valid, the user of the vehicle is authorized and has provided correct identity and password.
- **Step 2:** Following this, OBU_i generates two random nonces $r_1, r_2 \in Z_q^*$, and performs the following computations. It computes $VZ_i = VD_i \oplus h(RID_i \| PW_i \| r_i^*)$, $VF_i = RID_i \oplus h(VZ_i \| r_1)$, $VG_i = r_2 \cdot Pub_{TA} + Reg_{ID_i}$, $VL_i = h(r_2 \cdot Pub_{TA} \| RID_i)$.
- **Step 4:** V_i generates a current timestamp as $TS_{V_{i_1}}$ and sends authentication request message consisting of $\{TID_i, VF_i, VG_i, VL_i, r_1, TS_{V_{i_1}}\}$ to TA via open public channel.

4.4. Remote authentication, verification and session key establishment phase

The communication between TA and vehicles needs to be secured because the vehicles share data with the TAs. The data shared between them is traffic related data which is further used for decision making and providing on road traffic related services. Any modification or delay in the data can lead to mis-happenings and even risks lives. The following steps are executed to remotely authenticate and verify the vehicle.

- **Step 1:** After receiving authentication request message $\{TID_i, VF_i, VG_i, VL_i, r_1, TS_{V_{i_1}}\}$ from V_i, TA first verifies the

Vehicle (V_i)	Trusted authority (TA)
Select unique identity ID_i and Calculate pseudo identity $RID_i = H(ID_i)$. $\{RID_i, h(VUN_i)\}$ (via secure channel)	
	Receive RID_i, $h(VUN_i)$ Check if $h(VUN_i)$ is present in database? If yes, abort; else, make the entry and proceed Compute $Reg_{ID_i} = pk_{TA} \cdot RID_i$ Choose a temporary identity TID_i Compute $RTID_i = h(TID_i \| pk_{TA})$ Generates current timestamp TS_{TA_1} $\{TID_i, Reg_{ID_i}, RTID_i, TS_{TA_1}\}$ (via secure channel)
Receive $\{TID_i, Reg_{ID_i}, RTID_i, TS_{TA_1}\}$ Check if $\|TS^*_{TA_1} - TS_{TA_1}\| \leq \Delta TS$? Generate a random nonce $r_i \in Z^*_q$ Computes $VDID_i = Reg_{ID_i} + H(PW_i \| r_i)$ $VD_i = RTID_i \oplus h(ID_i \| PW_i \| r_i)$ $VA_i = h(ID_i \| Reg_{ID_i} \| h(r_i \| PW_i))$ $VB_i = h(ID_i \| r_i \| PW_i) \oplus RID_i$ Store $\{TID_i, VDID_i, VD_i, VA_i, VB_i\}$ Delete $\{Reg_{ID_i}, RTID_i\}$ permanently	

Fig. 2. Summary of vehicle registration phase

received timestamp $TS_{V_{i_1}}$ against the current timestamp by the condition: $|TS^*_{V_{i_1}} - TS_{V_{i_1}}| \leq \Delta TS$. If the timestamp is valid, it computes $VZ^*_i = h(TID_i \| pk_{TA})$, $RID^*_i = VF_i \oplus h(VZ^*_i \| r_1)$.

- **Step 2:** After computing RID^*_i, TA checks its validity against the stored RID_i by the equation $RID_i = RID^*_i$? If it is valid, TA computes $Reg^*_{ID_i} = pk_{TA} \cdot RID^*_i$, $VY_i = VG_i - Reg^*_{ID_i}$. Then TA uses the bilinear pairing equation: $e(pr_{TA} \cdot (RID^*_i) \cdot P, P) = ver^{RID^*_i}$ to verify the authenticity of the vehicle. It the equation is valid, TA computes $VL^*_i = h(VY_i \| RID^*_i)$ for the corresponding authorized vehicle.
- **Step 3:** In the next step, TA computes a session key. For this, it generates a random nonce $r_3 \in Z^*_q$, and computes $V_1 = r_3 \cdot P$, $V_2 = V_1 - Reg_{ID_i}$. Finally it computes the session key between TA and V_i, as $SK_{TA-V_i} = h(Reg_{ID_i} \| V_1 \| VY_i)$.
- **Step 4:** To ensure the integrity of the session key SK_{TA-V_i}, while sending it on an open channel, TA computes $Q_i = h(RID^*_i \| SK_{TA-V_i} \| V_1)$. It generates a new temporary identity TID^{new}_i, and computes new pseudo temporary identity by $RTID^{new}_i = h(TID^{new}_i \| pk_{TA})$. It computes $V_3 = RTID^{new}_i \oplus SK_{TA-V_i}$ and $V_4 = TID^{new}_i \oplus h(V_1)$. Finally, TA generates another timestamp TS_{TA_2} and sends the authentication reply message as $\{Q_i, V_2, V_3, V_4, TS_{TA_2}\}$ to V_i on an open public channel.
- **Step 5:** On receiving the authentication reply message from TA, V_i checks the freshness of the message by checking the time delay using the condition: $|TS^*_{TA_2} - TS_{TA_2}| \leq \Delta TS$. Then, V_i calculates $V^*_1 = V_2 + Reg_{ID_i}$. It uses the value of V^*_1 to compute session key SK_{V_i-TA} as $SK_{V_i-TA} = h(Reg_{ID_i} \| V^*_1 \| (r_2 \cdot Pub_{TA}))$. To ensure the integrity of the calculated session key, V_i calculates $Q^*_i = h(RID^*_i \| SK_{V_i-TA} \| V^*_1)$ and checks if $Q^*_i = Q_i$?
- **Step 6:** If the equation $Q^*_i = Q_i$ is valid, V_i extracts the credentials by, $RTID^{new}_i = V_3 \oplus SK_{V_i-TA}$, $TID^{new}_i = V_4 \oplus h(V^*_1)$ and $VD^{new}_i = RTID^{new}_i \oplus h(ID_i \| PW_i \| r_i)$. Subsequently, after successful authentication and session key establishment, OBU_i of vehicle V_i replaces $\{TID_i, VD_i\}$ with $\{TID^{new}_i, VD^{new}_i\}$ for availing further services.

Figure 3 summarizes the log in, authentication, verification and key establishment phases.

4.5. Vehicle addition phase

With the increase in number of vehicles every day, a new vehicle may wish to join the network. Also, there can be a possibility where an existing vehicle might get physically captured or may stop working for some reason. Therefore, a flexible access control scheme should only allow authenticated vehicle to be deployed in the network. Following steps are performed between new vehicle V^{new}_i and TA.

- **Step 1:** Vehicle V^{new}_i chooses its unique identity ID^{new}_i and calculates its pseudo identity RID^{new}_i as $RID^{new}_i = H(ID^{new}_i)$. V^{new}_i sends its pseudo identity RID^{new}_i, hashed unique number $h(VUN^{new}_i)$ to TA via a secure channel.
- **Step 2:** On receiving RID^{new}_i, $h(VUN^{new}_i)$ from V^{new}_i, the TA checks for the presence of $h(VUN^{new}_i)$ in its database. If the entry is present in its database it stops the further process to avoid multiple registration of the same vehicle. If $h(VUN^{new}_i)$ is not present in the database, it makes the entry of the vehicle's number in the table and proceeds the registration process. TA computes $Reg^{new}_{ID_i}$ as, $Reg^{new}_{ID_i} = pk_{TA} \cdot RID^{new}_i$. TA chooses a temporary identity TID^{new}_i for vehicle V^{new}_i, and computes pseudo temporary identity by $RTID^{new}_i = h(TID^{new}_i \| pk_{TA})$.
- **Step 3:** Finally, TA generates a current timestamp as TS_{TA_1}, and sends the registration reply message $\{TID^{new}_i, Reg^{new}_{ID_i}, RTID^{new}_i, TS_{TA_1}\}$ to V_i on a secure channel.
- **Step 4:** After receiving registration reply message $\{TID^{new}_i, Reg^{new}_{ID_i}, RTID^{new}_i, TS_{TA_1}\}$ from TA, OBU^{new}_i of V^{new}_i first verifies the received timestamp TS_{TA_1} against the current timestamp by the condition: $|TS^*_{TA_1} - TS_{TA_1}| \leq \Delta TS$. If the timestamp is valid, OBU^{new}_i requests the user of V^{new}_i to choose and enter a password PW^{new}_i associated with V^{new}_i. OBU^{new}_i generates a random nonce $r^{new}_i \in Z^*_q$, and computes $VDID^{new}_i$, VD^{new}_i,

Vehicle (V_i)	Trusted Authority TA
Compute $r_i^* = r_i \oplus h(IDi \Vert PW_i)$ Calculate $Reg_{ID_i}^* = VDID_i - H(PW_i \Vert r_i^*)$, $VA_i^* = h(ID_i \Vert Reg_{ID_i}^* \Vert h(r_i^* \Vert PW_i))$ Verify if $VA_i = VA_i^*$? Generate $r_1, r_2 \in Z_q^*$ Compute $VZ_i = VD_i \oplus h(RID_i \Vert PW_i \Vert r_i^*)$, $VF_i = RID_i \oplus h(VZ_i \Vert r_1)$ $VG_i = r_2 \cdot Pub_{TA} + Reg_{ID_i}$ $VL_i = h(r_2 \cdot Pub_{TA} \Vert RID_i)$ Generate a current timestamp as $TS_{V_{i_1}}$ $\{TID_i, VF_i, VG_i, VL_i, r_1, TS_{V_{i_1}}\}$ →	
(via open channel)	
	Receive authentication request message Verify $\vert TS_{V_{i_1}}^* - TS_{V_{i_1}} \vert \leq \Delta TS$? Compute $VZ_i^* = h(TID_i \Vert pk_{TA})$ $RID_i^* = VF_i \oplus h(VZ_i^* \Vert r_1)$ Verify $RID_i = RID_i^*$? Computes $Reg_{ID_i}^* = pk_{TA} \cdot RID_i^*$ $VY_i = VG_i - Reg_{ID_i}^*$ Verify $e(pr_{TA} \cdot (RID_i^*) \cdot P, P) = ver^{RID_i^*}$? Compute $VL_i^* = h(VY_i \Vert RID_i *)$ Generate $r_3 \in Z_q^*$ Compute $V_1 = r_3 \cdot P$ $V_2 = V_1 - Reg_{ID_i}$ Calculate $SK_{TA-V_i} = h(Reg_{ID_i} \Vert V_1 \Vert VY_i)$ Compute $Q_i = h(RID_i^* \Vert SK_{TA-V_i} \Vert V_1)$ Generate temporary identity TID_i^{new} Compute $RTID_i^{new} = h(TID_i^{new} \Vert pk_{TA})$ $V_3 = RTID_i^{new} \oplus SK_{TA-V_i}$ $V_4 = TID_i^{new} \oplus h(V_1)$ Generates another timestamp TS_{TA_2} $\{Q_i, V_2, V_3, V_4, TS_{TA_2}\}$ ←
	(via open channel)
Receive authentication reply message Verify $\vert TS_{TA_2}^* - TS_{TA_2} \vert \leq \Delta TS$? Calculate $V_1^* = V_2 + Reg_{ID_i}$ Compute $SK_{V_i-TA} = h(Reg_{ID_i} \Vert V_1^* \Vert (r_2 \cdot Pub_{TA}))$ Compute $Q_i^* = h(RID_i^* \Vert SK_{V_i-TA} \Vert V_1^*)$ Verify $Q_i^* = Q_i$? Extract $RTID_i^{new} = V_3 \oplus SK_{V_i-TA}$, $TID_i^{new} = V_4 \oplus h(V_1^*)$ $VD_i^{new} = RTID_i^{new} \oplus h(ID_i \Vert PW_i \Vert r_i)$ Replace $\{TID_i, VD_i\}$ with $\{TID_i^{new}, VD_i^{new}\}$	

Fig. 3. Authentication and key establishment phase

VA_i^{new}, VB_i^{new} as, $VDID_i^{new} = Reg_{ID_i}^{new} + H(PW_i^{new} \Vert r_i^{new})$, $VD_i^{new} = RTID_i^{new} \oplus h(ID_i^{new} \Vert PW_i^{new} \Vert r_i^{new})$, $VA_i^{new} = h(ID_i^{new} \Vert Reg_{ID_i}^{new} \Vert h(r_i^{new} \Vert PW_i^{new}))$, $VB_i^{new} = h(ID_i^{new} \Vert r_i^{new} \Vert PW_i^{new}) \oplus RID_i^{new}$.

- **Step 5:** OBU_i^{new} of vehicle V_i^{new} stores $\{TID_i^{new}, VDID_i^{new}, VD_i^{new}, VA_i^{new}, VB_i^{new}\}$ in its memory, and deletes $\{Reg_{ID_i}^{new}, RTID_i^{new}\}$ permanently from its memory.

For better understanding, Figure 4 shows the complete phases of execution of our scheme.

4.6. Password change phase

In a vulnerable paradigm like smart transportation, it is likely to happen that the password of the vehicle can be breached or stolen. So in a password based authentication mechanism, it should be easy to change or update the password. Following steps are executed by the OBU_i of the vehicle to update the password.

- **Step 1:** Vehicle V_i enters its identity ID_i and old password PW_i. Now, the OBU_i, executes the **Step 1** of log in phase (described in Section 4.3) to check the authenticity of the vehicle.
- **Step 2:** A valid vehicle enters the new password PW_i^{new}. Then, OBU_i computes $VZ_i = VD_i \oplus h(RID_i \Vert PW_i \Vert r_i^*)$, $Reg_{ID_i} = VDID_i - H(PW_i \Vert r_i^*)$.
- **Step 3:** Using the new password PW_i^{new}, OBU_i calculates $VDID_i^{new} = Reg_{ID_i} + H(PW_i^{new} \Vert r_i^*)$, $VD_i^{new} = VZ_i \oplus h(ID_i \Vert PW_i \Vert r_i^*)$, $VA_i^{new} = h(ID_i \Vert Reg_{ID_i} \Vert h(r_i^* \Vert PW_i^{new}))$, $VB_i = h(ID_i \Vert r_i^* \Vert PW_i^{new}) \oplus RID_i$.
- **Step 4:** OBU_i of vehicle V_i replaces the old $\{VDID_i, VD_i, VA_i, VB_i\}$ with new values $\{VDID_i^{new}, VD_i^{new}, VA_i^{new}, VB_i^{new}\}$.

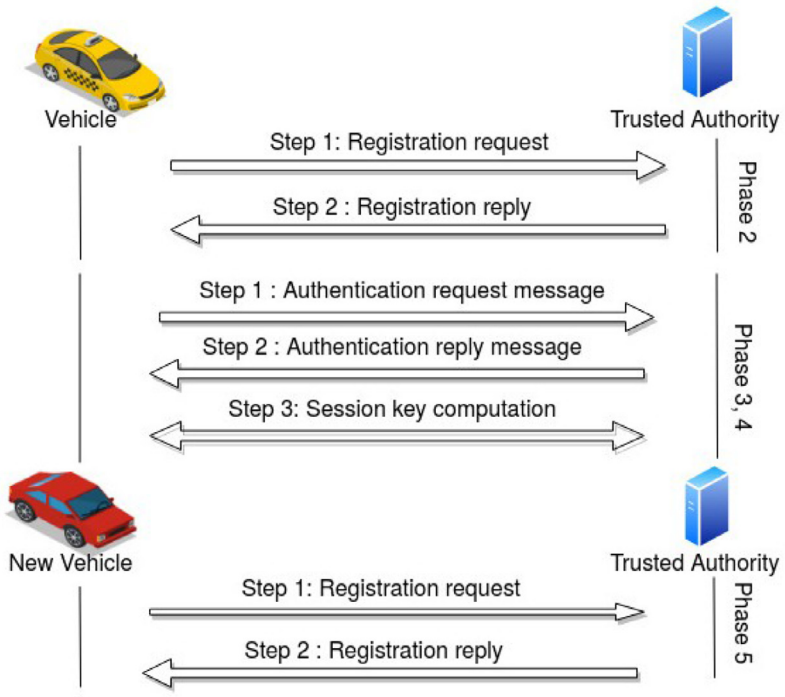

Fig. 4. Overview of the proposed access control scheme

5. The extended scheme

In this section, we provide an extended scheme from the basic scheme discussed in Section 4 for an IoV application.

In IoV environment, we consider a dynamic clustering mechanism for the vehicles proposed by [29] and [22] to creating different clusters of vehicles on the fly. The dynamic clustering can be considered as follows. The vehicles moving on a same lane segment that ends at the intersection with the other lane are included in a cluster. Thus, a vehicle needs to find its neighboring vehicles moving on the same lane segment towards the same direction almost with the same speed. In this way, a dynamic cluster will have a group of members as the vehicles. Next, a cluster head (CH) will be selected among the members in each cluster. Now, every vehicle needs to securely communicate with their CH in a cluster.

Note that both the cluster head (CH) and a vehicle, say V_i in each cluster have already established session keys $SK_{TA,CH}$ and SK_{TA,V_i}, respectively, for their secure communication with the TA. For establishing a session key between the cluster head (CH) and its member vehicle V_i, the following steps need to be executed with the help of the TA:

- **Step 1:** The initiator vehicle V_i generates a current timestamp TS_i and sends a session key request message $Msg_1 = \{TID_i, TS_i\}$ to its cluster head CH via a public channel.
- **Step 2:** After receiving the message Msg_1, the CH validates the timeliness of the received timestamp TS_i. If it is valid, CH generates a current timestamp TS_{CH} and a random secret $r_{CH} \in Z_q^*$, and encrypts $(TID_i, TID_{CH}, TS_i, r_{CH}, TS_{CH})$ using the shared session key $SK_{TA_{CH}}$ with the TA. After that CH sends a request message $Msg_2 = \{TS_{CH}, E_{SK_{TA,CH}}(TID_i, TID_{CH}, TS_i, r_{CH}, TS_{CH})\}$ to the TA via public channel, where $E_K(\cdot)$ denotes the symmetric encryption using the shared key K.
- **Step 3:** Once the message Msg_2 is received by the TA, it checks the timeliness of timestamp TS_{CH}. If it is valid, the TA decrypts $E_{SK_{TA,CH}}(TID_i, TID_{CH}, TS_i, r_{CH}, TS_{CH})$ using the shared key $SK_{TA,CH}$ as $(TID_i, TID_{CH}, TS_i, r_{CH}, TS'_{CH}) = D_{SK_{TA,CH}}[E_{SK_{TA,CH}}(TID_i, TID_{CH}, TS_i, r_{CH}, TS_{CH})]$, where $D_K(\cdot)$ denotes the symmetric decryption using the shared key K. Next, the TA checks the validity of $TS'_{CH} = TS_{CH}$, and if this is valid, the TA fetches the already established session keys SK_{TA,V_i} and SK_{TA-CH} corresponding to TID_i and TID_{CH} respectively, and generates a current timestamp TS_{TA} and a random secret $r_{TA} \in Z_q^*$. The TA computes a shared session key $SK_{V_i,CH}$ between V_i and CH as $SK_{V_i,CH} = h(r_{TA} || r_{CH} || TS_i || TS_{CH} || TID_i || TID_{CH} || SK_{TA,V_i} || SK_{TA,CH})$. The TA also generates new temporary identities TID_i^{new} and TID_{CH}^{new} to compute $TID_i^* = TID_i^{new} \oplus h(TS_{TA} || SK_{TA,V_i} || SK_{V_i,CH})$ and $TID_{CH}^* = TID_{CH}^{new} \oplus h(TS_{TA} || SK_{TA,CH} || SK_{V_i,CH})$. Once these parameters are calculated, the TA sends the messages $Msg_3 = \{TID_i^*, TS_{TA}, E_{SK_{TA,V_i}}(SK_{V_i,CH}, TS_{TA})\}$ and $Msg_4 = \{TID_{CH}^*, TS_{TA}, E_{SK_{TA,CH}}(SK_{V_i,CH}, TS_{TA})\}$ to V_i and CH, respectively, over the public channel.
- **Step 4:** After receiving the message Msg_3 from the TA, V_i checks the timeliness of received timestamp TS_{TA} and if it is valid, V_i decrypts $E_{SK_{TA,V_i}}(SK_{V_i,CH}, TS_{TA})$ using the shared key SK_{TA,V_i} with the TA as $(SK_{V_i,CH}, TS'_{TA}) = D_{SK_{TA,V_i}}[E_{SK_{TA,V_i}}(SK_{V_i,CH}, TS_{TA})]$. If $TS'_{TA} = TS_{TA}$, V_i calculates $TID_i^{new} = TID_i^* \oplus h(TS'_{TA} || SK_{TA,V_i} || SK_{V_i,CH})$. Next, V_i updates TID_i by the calculated TID_i^{new} in its database and also stores the session key $SK_{V_i,CH}$ shared with the CH for secret communication.
- **Step 5:** After receiving the message Msg_4 from the TA, CH also checks the timeliness of received timestamp TS_{TA} and if it is valid, CH decrypts $E_{SK_{TA,CH}}(SK_{V_i,CH}, TS_{TA})$ using the shared key $SK_{TA,CH}$ with the TA as $(SK_{V_i,CH}, TS^*_{TA}) = D_{SK_{TA,CH}}[E_{SK_{TA,CH}}(SK_{V_i,CH}, TS_{TA})]$. If $TS^*_{TA} = TS_{TA}$, CH proceeds to compute $TID_{CH}^{new} = TID_{CH}^* \oplus h(TS^*_{TA} || SK_{TA,CH} || SK_{V_i,CH})$. Finally, CH updates TID_{CH} by the calculated TID_{CH}^{new} in its database and also stores the session key $SK_{V_i,CH}$ shared with V_i for secret communication.

The summary of the extended scheme is briefed in Figure 5.

6. Security analysis

In this section we analyze the security of proposed scheme. We show the correctness of bilinear pairing based verification equation used in section 4.4 and the correctness of session key computed by vehicle V_i and TA. In the next subsection, we present an informal security analysis

Vehicle (V_i)	Cluster Head (CH)	Trusted Authority TA
Generate current timestamp TS_i.		
$\underline{Msg_1 = \{TID_i, TS_i\}}$ (to CH via open channel)	Check timestamp TS_i. If valid, generate current timestamp TS_{CH}, random secret $r_{CH} \in Z_q^*$.	
	$\underline{Msg_2 = \{TS_{CH}, E_{SK_{TA,CH}}(TID_i, TID_{CH}, TS_i, r_{CH}, TS_{CH})\}}$ (to TA via open channel)	Check timestamp TS_{CH}. If so, compute $(TID_i, TID_{CH}, TS_i, r_{CH}, TS'_{CH}) = D_{SK_{TA,CH}}[E_{SK_{TA,CH}}(TID_i, TID_{CH}, TS_i, r_{CH}, TS_{CH})]$. If $TS'_{CH} = TS_{CH}$, fetch session keys SK_{TA,V_i} and SK_{TA-CH} corresponding to TID_i & TID_{CH}, respectively. Generate timestamp TS_{TA} and random secret $r_{TA} \in Z_q^*$. Compute $SK_{V_i,CH} = h(r_{TA} \|r_{CH} \|TS_i \|TS_{CH} \|TID_i \|TID_{CH} \|SK_{TA,V_i} \|SK_{TA,CH})$. Generate new temporary identities TID_i^{new} and TID_{CH}^{new}. Compute $TID_i^* = TID_i^{new} \oplus h(TS_{TA} \|SK_{TA,V_i} \|SK_{V_i,CH})$ and $TID_{CH}^* = TID_{CH}^{new} \oplus h(TS_{TA} \|SK_{TA,CH} \|SK_{V_i,CH})$.
		$\underline{Msg_3 = \{TID_i^*, TS_{TA}, E_{SK_{TA,V_i}}(SK_{V_i,CH}, TS_{TA})\}}$ (to V_i via open channel)
		$\underline{Msg_4 = \{TID_{CH}^*, TS_{TA}, E_{SK_{TA,CH}}(SK_{V_i,CH}, TS_{TA})\}}$ (to CH via open channel)
Check timestamp TS_{TA}. If valid, $(SK_{V_i,CH}, TS'_{TA}) = D_{SK_{TA,V_i}}[E_{SK_{TA,V_i}}(SK_{V_i,CH}, TS_{TA})]$. If $TS'_{TA} = TS_{TA}$, compute $TID_i^{new} = TID_i^* \oplus h(TS'_{TA} \|SK_{TA,V_i} \|SK_{V_i,CH})$. Update TID_i by TID_i^{new} and store session key $SK_{V_i,CH}$ shared with CH.		
	Check received timestamp TS_{TA}. If valid, calculate $(SK_{V_i,CH}, TS^*_{TA}) = D_{SK_{TA,CH}}[E_{SK_{TA,CH}}(SK_{V_i,CH}, TS_{TA})]$. If $TS^*_{TA} = TS_{TA}$, compute $TID_{CH}^{new} = TID_{CH}^* \oplus h(TS^*_{TA} \|SK_{TA,CH} \|SK_{V_i,CH})$. Update TID_{CH} by TID_{CH}^{new} and store the session key $SK_{V_i,CH}$ shared with V_i.	

Fig. 5. Summary of the extended scheme

of the scheme. And later, a formal security analysis using AVISPA is provided in 6.3.

6.1. Correctness proof

We provide below the correctness proof of our authentication, verification and key establishment phase that is described in Section 4.4 using the theorems 1 and 2.

Theorem 1. *During the authentication phase described in Section 4.4, a vehicle V_i sends authentication request message $\{TID_i, VF_i, VG_i, VL_i, r_1, TS_{V_{i_1}}\}$ to TA. Authentication and verification is successful, if and only if the received message is valid.*

Proof. TA receives the authentication request message $\{TID_i, VF_i, VG_i, VL_i, r_1, TS_{V_{i_1}}\}$ from vehicle V_i. Vehicle V_i is authenticated if the following equation holds:

$$e(pr_{TA} \cdot (RID_i^*) \cdot P, P) = ver^{RID_i^*}$$

Now,

$$\begin{aligned} ver^{RID_i^*} &= e(Pub_{TA}, P)^{RID_i^*} \\ &= e(pr_{TA} \cdot P, P)^{RID_i^*} \\ &= e(pr_{TA} \cdot P, P)^{RID_i^* \cdot 1} \\ &= e(pr_{TA} \cdot P \cdot RID_i^*, P \cdot 1) \\ &= e(pr_{TA} \cdot (RID_i^*) \cdot P, P). \end{aligned}$$

Since the above equation holds, the message received from V_i is valid. Hence, the theorem follows. □

Theorem 2. *During the key establishment phase, described in Section 4.4, session key computed by TA : SK_{TA-V_i}, is same as the session key computed by vehicle V_i : SK_{V_i-TA}.*

Proof. The session key computed by TA after successful authentication is $SK_{TA-V_i} = h(Reg_{ID_i} \|V_1 \|VY_i)$. And the session key computed by V_i after receiving authentication reply message is $SK_{V_i-TA} = h(Reg_{ID_i} \|V_1^* \|(r_2 \cdot Pub_{TA}))$.

Now, we have,

$$\begin{aligned} SK_{TA-V_i} &= h(Reg_{ID_i} \|V_1 \|VY_i) \\ &= h(Reg_{ID_i} \|V_1 \|(VG_i - Reg_{ID_i})) \\ &= h(Reg_{ID_i} \|V_1 \|(r_2 \cdot Pub_{TA} \\ &\quad + Reg_{ID_i} - Reg_{ID_i})) \\ &= h(Reg_{ID_i} \|V_1 \|r_2 \cdot Pub_{TA}). \end{aligned}$$

$$\begin{aligned} SK_{V_i-TA} &= h(Reg_{ID_i} \|V_1^* \|(r_2 \cdot Pub_{TA})) \\ &= h(Reg_{ID_i} \|(V_2 + Reg_{ID_i}) \|(r_2 \cdot Pub_{TA})) \\ &= h(Reg_{ID_i} \|(V_1 - Reg_{ID_i} + Reg_{ID_i}) \\ &\quad \|(r_2 \cdot Pub_{TA})) \\ &= h(Reg_{ID_i} \|V_1 \|r_2 \cdot Pub_{TA}). \end{aligned}$$

Since the above equations are equal to each other. Thus, the theorem follows. □

6.2. Informal security analysis

We analyze the proposed access control scheme informally in the following propositions, and show that our scheme is resilient against various known attacks.

Proposition 1. *Proposed remote access control scheme is secured against replay attack.*

Proof. Three messages are exchanged in our scheme to accomplish authentication and session key establishment. The first message is a registration reply message $\{TID_i, Reg_{ID_i}, RTID_i, TS_{TA_1}\}$ which is sent from TA to V_i. The second is during log in phase, where a vehicle sends an authentication request message $\{TID_i, VF_i, VG_i, VL_i, r_1, TS_{V_{i_1}}\}$ to TA and third is an authentication reply message as $\{Q_i, V_2, V_3, V_4, TS_{TA_2}\}$ sent to V_i from TA. All the messages include the current timestamp TS_{TA_1}, $TS_{V_{i_1}}$, TS_{TA_2}. On receiving the messages, the receiver checks the freshness of the message by finding the delay in the message. The delay in message is calculated by computing the difference in the received timestamp and the current timestamp. To avoid replay attacks, we have considered a very small value ΔTS as the difference in timestamp values. Hence, including the timestamp in every message assures that the scheme is secured against replay attacks. □

Proposition 2. *Proposed remote access control scheme is secured against OBU physical capture attack.*

Proof. During the vehicle registration phase described in Section 4.2, OBU_i stores the credentials $\{TID_i, VDID_i, VD_i, VA_i, VB_i\}$ in its memory, and deletes $\{Reg_{ID_i}, RTID_i\}$ permanently from its memory. So if the adversary has physically stolen OBU_i of vehicle V_i, he/she can extract all the credentials from OBU_i using power analysis attack. As seen in the registration phase, $VDID_i = Reg_{ID_i} + H(PW_i \| r_i)$, $VD_i = RTID_i \oplus h(ID_i \| PW_i \| r_i)$, $VA_i = h(ID_i \| Reg_{ID_i} \| h(r_i \| PW_i))$, $VB_i = h(ID_i \| r_i \| PW_i) \oplus RID_i$. However, to retrieve secrets like Reg_{ID_i}, RTD_i the adversary needs to know r_i, ID_i, PW_i. Therefore it can clearly be concluded that the adversary cannot know any secret credentials by OBU_i physical capture attack. □

Proposition 3. *Proposed remote access control scheme is secured against man-in-the-middle attack.*

Proof. Assume that an adversary intercepts the authentication request message $\{TID_i, VF_i, VG_i, VL_i, r_1, TS_{V_{i_1}}\}$ and tries to create another authentication request message as $\{TID_i^a, VF_i^a, VG_i^a, VL_i^a, r_1^a, TS_{V_{i_1}}^a\}$. To create request message, the adversary has to perform computations like $VZ_i = VD_i \oplus h(RID_i \| PW_i \| r_i^*)$, $VF_i = RID_i \oplus h(VZ_i \| r_1)$, $VG_i = r_2 \cdot Pub_{TA} + Reg_{ID_i}$, $VL_i = h(r_2 \cdot Pub_{TA} \| RID_i)$. For this the adversary can generate two random nonces r_1, r_2. For computing VZ_i he needs to know VD_i, RID_i, PW_i and r_i^*. Let us also assume that he can extract VD_i from the memory of OBU_i as explained in 2, but he still cannot know RID_i, r_1^* as it depends on secret ID_i, r_1 and PW_i. Therefore it would be impossible for an attacker to create authentication request without knowing the secret values. Hence the scheme is secured against man-in-the-middle attack. □

Proposition 4. *Proposed remote access control scheme is resilient against vehicle impersonation attack.*

Proof. To impersonate a vehicle V_i, and adversary $\mathcal{A}$ might try to intercept the authentication request message $\{TID_i, VF_i, VG_i, VL_i, r_1, TS_{V_{i_1}}\}$ and creates another authentication request message as $\{TID_i^a, VF_i^a, VG_i^a, VL_i^a, r_1^a, TS_{V_{i_1}}^a\}$. To create request message, the adversary has to perform computations like $VZ_i = VD_i \oplus h(RID_i \| PW_i \| r_i^*)$, $VF_i = RID_i \oplus h(VZ_i \| r_1)$, $VG_i = r_2 \cdot Pub_{TA} + Reg_{ID_i}$, $VL_i = h(r_2 \cdot Pub_{TA} \| RID_i)$. For this the adversary can assume r_1, r_2 but the adversary cannot know r_i^*, RID_i, Reg_{ID_i} because the value of r_i^*, RID_i, Reg_{ID_i} depends on the long term secrets like ID_i, PW_i. Therefore an adversary cannot impersonate vehicle V_i as the long term secrets are not known to him. □

Proposition 5. *Proposed remote access control scheme is protected against privileged-insider attack.*

Proof. During the registration phase described in Section 4.2, V_i sends its pseudo identity RID_i to TA via public channel to get Reg_{ID_i}, $RTID_i$, and temporary identity TID_i. To perform insider attack, any privileged user of TA being an attacker gets to know the registration details RID_i. However, even if the attacker gets exposed to RID_i, he/she still does not get to know anything about the real identity of the vehicle. Hence, our scheme is protected against privileged insider attack. □

Proposition 6. *Proposed access control scheme is secured against ephemeral secret leakage (ESL) attack.*

Proof. During authentication, verification and key establishment phase, TA computes a session key as SK_{TA-V_i} as $SK_{TA-V_i} = h(Reg_{ID_i} \| V_1 \| VY_i)$ and the vehicle computes a session key as $SK_{V_i-TA} = h(Reg_{ID_i} \| V_1^* \| (r_2 \cdot Pub_{TA}))$. Both SK_{TA-V_i} and SK_{V_i-TA} depends on Reg_{ID_i} which is computed using long term secrets which are private key pr_{TA} of TA and identity of the vehicle ID_i. The session key also depends on short term secret values like r_3, r_2. Therefore an adversary needs both long term and short term secrets to compute session key. If by any ways, an attacker manages to know short term secret values based on the CK-adversary model by [13] as discussed in the threat model, still he would need to know the long term secrets ID_i, PW_i to acquire the session key. □

Proposition 7. *Proposed access control scheme is secured against masquerading attack.*

Proof. During authentication, verification and key establishment phase, TA sends a message $\{Q_i, V_2, V_3, V_4, TS_{TA_2}\}$ as authentication reply message to vehicle V_i. If an attacker $\mathcal{A}$ tries to launch a masquerade attack he/she would try to forge the valid authentication reply. For that he needs to calculate parameters like Q_i, V_2 etc. All the parameters in the reply message depends on secret values ID_i, pk_{TA}. Moreover the session key is also depended on secret Reg_{ID_i}. Hence it is clear that our scheme can withstand masquerading attack as the attacker is incapable to create a forged reply. □

Proposition 8. *Proposed access control scheme resists off-line identity guessing attack.*

Proof. Let us assume that an attacker $\mathcal{A}$ traps the authentication request message $\{TID_i, VF_i, VG_i, VL_i, r_1, TS_{V_{i_1}}\}$. Now if $\mathcal{A}$ wants to identify ID_i, he needs to compute it having known VZ_i. $\mathcal{A}$ cannot guess identity using VF_i and VL_i as there are two low entropy parameters $< ID_i, r_2 >$ which are impossible to be guessed in polynomial time. So the identity cannot be guessed by trapping log in message. Now let us assume that an attacker traps authentication reply message $\{Q_i, V_2, V_3, V_4, TS_{TA_2}\}$. It is also noticeable from Section 4.4 that the value of Q_i is relied on ID_i which is protected under hash functions. Hence it is impossible for the attacker to guess the identity in polynomial time. □

Proposition 9. *Proposed access control scheme resists vehicle traceability attack.*

Proof. We can easily prove that our scheme provides untraceability as a security requirement. During login phase (Section 4.3), a parameter TID_i is sent in the authentication request message. Then during verification and key establishment phase (in Section 4.4) Step 4, TA generates a new identity TID_i^{new} which is sent as parameter V_4 in authentication reply message to the vehicle. Then in Step 6 the vehicle extracts and updates its old TID_i with TID_i^{new} after verifying the authenticity.

Hence in every session the parameter TID_i is changed. Therefore, dynamic temporary identity supports untraceability in our access control scheme. □

Proposition 10. *Proposed access control scheme provides forward and backward secrecy.*

Proof. During key establishment phase, TA computes a session key as SK_{TA-V_i} as $SK_{TA-V_i} = h(Reg_{ID_i} \| V_1 \| VY_i)$ and the vehicle computes a session key as $SK_{V_i-TA} = h(Reg_{ID_i} \| V_1^* \| (r_2 \cdot Pub_{TA}))$. Both SK_{TA-V_i} and SK_{V_i-TA} depends on short term secret values like r_3, r_2. Therefore an adversary if by any chance gets to know session key for a particular session he still cannot compute session key for next and previous sessions as he needs to know r_3, r_2 to compute the session key. Therefore our scheme offers perfect backward and forward secrecy. □

6.3. Formal security verification using AVISPA tool: Simulation study

To formally analyze the security of the proposed access control scheme we have used the widely accepted simulation tool named as "Automated Validation of Internet Security Protocols and Applications (AVISPA)" [6]. AVISPA has become the common tool that is used to verify the security protocols based on various cryptographic techniques. The simulation process occurs in two steps. First, a formal language is used to specify the protocols and other security properties. Initially the protocol is coded in "High-Level Protocol Specification Language (HLPSL)" which is then transformed in "Intermediate Format (IF)" with the help of HLPSL2IF translator. Following to this in the second step, where the code is provided as input to any back-end of the tool which analyzes the security of the protocol.

The AVISPA tool consist of four back-ends:

- "On-the-fly Model-Checker (OFMC)"
- "Constraint Logic based Attack Searcher (CL-AtSe)"
- "SAT-based Model-Checker (SATMC)"
- "Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP)".

The output or the result from the back-ends is displayed in the "Output Format (OF)" which is comprehended in different sections. In the first section called as "SUMMARY" the output displays whether the protocol is "safe, unsafe, or inconclusive". The second section called as "DETAILS" elaborates on the reason on why the protocol is summarized as "safe, unsafe or inconclusive". The third section is "PROTOCOL" section that defines the "HLPSL specification of the target protocol in intermediate form". Next, section is the "GOAL" which specifies the actual goal of the analysis of the protocol. And the last section displays the name of the back-end that is chosen to process the security analysis.

To analyze the security of our proposed scheme we have coded the HLPSL implementation that consists of two basic roles of TA, V_i, the other compulsory roles of *session* and *goal & environment*. We have considered the registration phase discussed in Section 4.2, log in phase discussed in Section 4.3 and authentication, verification and key establishment phase discussed in Section 4.4 where TA authenticates the vehicle and both TA and vehicle compute a session key.

AVISPA detects the occurrence of attack while simulation by allotting an active role to the intruder (i). All the public parameters are fed into the knowledge of the intruder, and the intruder can even imitate all other roles. According to the "Dolev-Yao (DY) threat model" [21] discussed in Section 2, AVISPA simulation allows the intruder to "eavesdrop, modify, delete, or insert messages during communication". The broadly used "Security Protocol ANimator for AVISPA (SPAN)" tool [7] is used to perform formal security verification simulation under the environment: "Ubuntu 18.04.5 LTS having Memory: 7.7GiB, Processor: Intel®Core^{TM} i7-8565U CPU @ 1.80GHz × 8, OS type: 64-bit, Disk: 966.1 GB". The results of simulation of the proposed scheme is shown in Figure 6 which shows the results using OFMC back-end. Thus we can clearly state that the proposed access control scheme is secured against "replay and man-in-the-middle-attacks".

Table 3
Comparative computational costs analysis

Scheme	Total cost	Estimated time (in milliseconds)
Our scheme	$15T_h + 5T_{ecm} + 5T_{eca} + T_{bp} + T_{exp}$	≈ 173.61 ms
[17]	$10T_h + 6T_{exp}$	≈ 118.40 ms
[38]	$52T_h$	≈ 16.64 ms
[4]	$4T_h + 2T_{ecm} + 2T_{eca}$	≈ 44.28 ms
[2]	$8T_h + 6T_{ecm} + 2T_{enc/dec}$	≈ 105.80 ms
[9]	$10T_h + 9T_{ecm} + 2T_{epa}$	≈ 165.90 ms
[42]	$16T_h$	≈ 5.12 ms

Table 4
Comparative communication costs analysis

Scheme	Number of messages	Number of bits
Our scheme	2	2112
[17]	3	2464
[38]	5	3872
[4]	4	2560
[2]	3	$896n + 1440$
[9]	3	1856
[42]	4	2624

Note: n: number of vehicles in the scheme of [2]

7. Comparative analysis

The efficiency of the scheme can be asserted in terms of computation and communication cost. The computation time is the total time taken by the all cryptographic techniques in the scheme to execute. And the communication cost is defined as the number of bits (messages) exchanged during the execution of any scheme. In this section we calculate the communication, computation of our scheme and also compare it to other existing access control schemes. Later, we also compare all the schemes in terms of security and functionality features.

7.1. Computation costs comparison

The cryptographic techniques which are used in the schemes are "elliptic curve point multiplication", an "elliptic curve point addition", a "bilinear pairing operation", a "modular exponentiation", a "one-way hash function", a "symmetric key encryption/decryption". We use the notation T_{ecm}, T_{epa}, T_{bp}, T_{exp}, T_h and $T_{enc/dec}$ for each respectively. To generalized and fair comparison we have considered specific estimated time for each operation. For T_{ecm}, T_{eca}, T_{bp}, T_{exp}, T_h and $T_{enc/dec}$ the execution time taken is 17.10 ms ([31]), 4.4 ms ([14]), 42.11 ms, 19.2 ms ([31]), 0.32 ms ([14]) and 0.32 ms, respectively.

The cryptographic operations during login, and authentication, verification and key establishment phases (discussed in Sections 4.3 and 4.4) in our scheme, are "elliptic curve point multiplication, elliptic curve point addition, bilinear pairing operation, modular exponentiation, one-way hash function". The total computation cost comes out to be $15T_h + 5T_{ecm} + 3T_{eca} + T_{bp} + T_{exp}$. In Table 3, we have compared the computation costs of our scheme against existing schemes proposed by [17], [38], [4], [2], [42] and [9]. Due to the use of bilinear pairings, our scheme requires more computational cost as compared to other existing schemes except the comparable computation cost as in [9]. However, it can be justified due to superior security and more functionality attributes provided by the proposed scheme as compared to existing competing schemes (see Table 5).

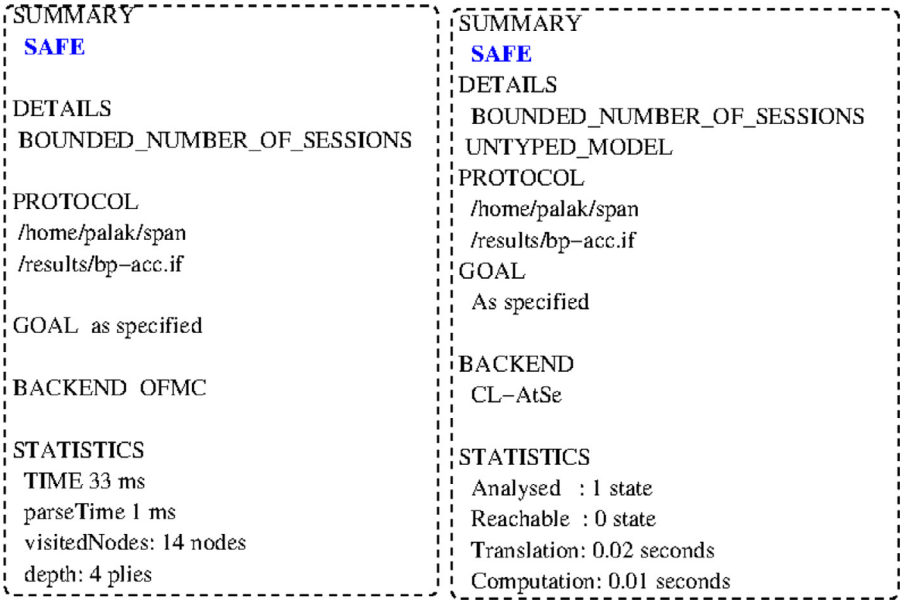

Fig. 6. Simulation results of AVISPA under OFMC and CL-AtSe backends

Table 5
Comparison of functionality & security features

Feature	Chen et al.	Sadri and Rajabzadeh Asaar	Alladi et al.	Al-Shareeda et al.	Vasudev et al.	Bagga et al.	Our
F_1	✓	✓	×	×	✓	✓	✓
F_2	✓	✓	✓	✓	✓	✓	✓
F_3	✓	✓	✓	✓	✓	✓	✓
F_4	✓	✓	✓	✓	✓	✓	✓
F_5	✓	✓	✓	✓	✓	✓	✓
F_6	×	×	×	×	×	×	✓
F_7	✓	×	✓	×	✓	✓	✓
F_8	✓	✓	✓	✓	✓	✓	✓
F_9	×	×	×	×	×	✓	✓
F_{10}	×	×	×	×	×	✓	✓
F_{11}	×	✓	×	×	×	✓	✓

Note: F_1: "resilience against on-broad unit physical capture attack"; F_2: "insider attack"; F_3: "replay attack"; F_4: "man-in-the-middle attack"; F_5: "mutual authentication"; F_6: "remote registration" F_7: "key agreement"; F_8: "impersonation attack"; F_9: "formal security verification using AVISPA tool"; F_{10}: " vehicle addition phase"; F_{11}: "user password and/or biometric update phase".
✓: "a scheme is secure or assists a feature"; ×: "a scheme is insecure or does not assist a feature".

7.2. Communication costs comparison

As stated before the number of messages or number of bits exchanged during the execution of the scheme is said to be its communication overhead. To calculate this, we have considered some standard value to fairly compare all the schemes. The assumed value of "one-way cryptographic hash function" is considered as 256 bits. For ECC techniques we have considered 160 bits cryptosystem. Therefore, an elliptic curve point $P = (P_x, P_y)$ is $(160 + 160) = 320$ bits, where "P_x and P_y are the x and y co-ordinates of the point P". Further, a "vehicle's real identity, random nonce and timestamp" are taken as 160, 160 and 32 bits, respectively. For a "symmetric key encryption/decryption (for example, if the Advanced Encryption Standard (AES-128) is used), the plaintext/ciphertext block size" will become 128 bits.

The authentication process in our scheme, is accomplished by exchanging two messages. The first message is authentication request message $\{TID_i, VF_i, VG_i, VL_i, r_1, TS_{V_{i_1}}\}$ from V_i to TA. This message takes a total of $160 + 256 + 320 + 160 + 32 = 928$ bits. The second message is authentication reply message as $\{Q_i, V_2, V_3, V_4, TS_{TA_2}\}$ to V_i which takes a total of $256 + 320 + 320 + 256 + 32 = 1184$ bits. The total communication overhead of our scheme is 2112 bits.

In Table 4, we have compared the communication costs of our scheme against existing schemes proposed by [17], [38], [4], [2], [42] and [9]. It is noticed that the proposed scheme requires comparable communication cost as in [9]. However, the communication cost in the proposed scheme is low as compared to other remaining existing schemes as shown in Table 4.

7.3. Security and functionality features comparison

The comparative analysis on "security and functionality" features among the proposed scheme and other schemes proposed is provided in Table 5. We have considered few security and functionality features like resilience against "on-broad unit physical capture attack", "insider attack" "replay attack", "man-in-the-middle attack". Other features like "mutual authentication", "remote registration ", "key agreement", impersonation attack", "formal security verification using AVISPA tool, "dynamic vehicle addition phase, " password update phase". And it can be clearly seen that our scheme excels in security and functionality features than other schemes. In Table 5, we have considered ✓: if "a scheme is secure or assists a feature" and ×: if "a scheme is insecure or does not assist a feature".

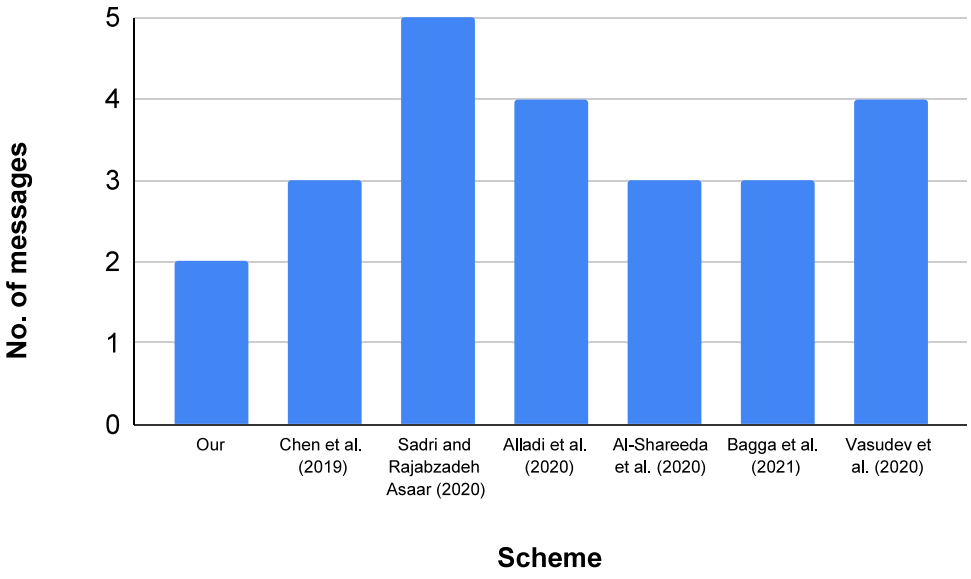

Fig. 7. Performance analysis of all schemes for communication costs in terms of number of messages (assume $n = 1$ in [2])

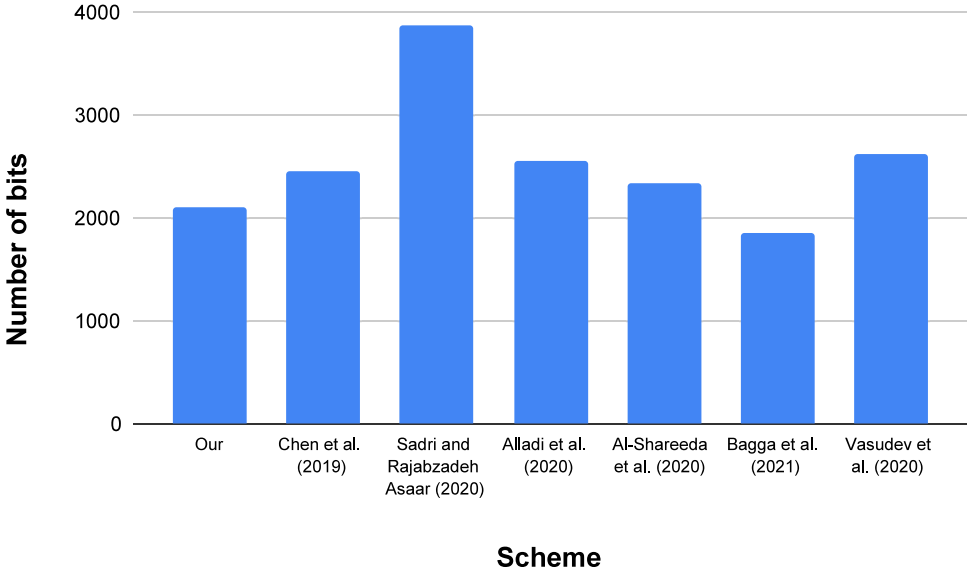

Fig. 8. Performance analysis of all schemes for communication costs in terms of number of bits (assume $n = 1$ in [2])

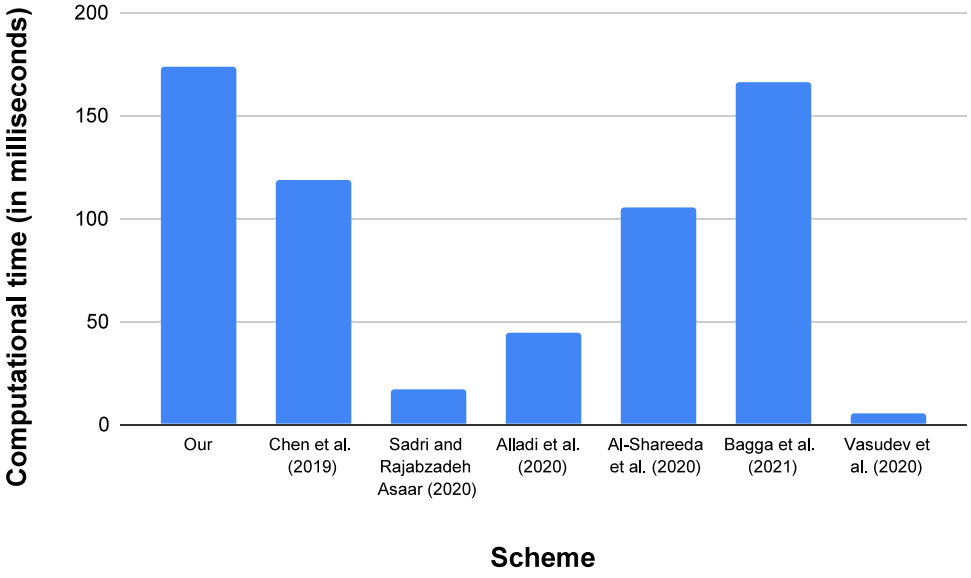

Fig. 9. Performance analysis of all schemes for computational costs

For overall comparison, we present the computation cost, communication costs in bits and number of messages in Figures 7, 8 and 9, respectively. It can be seen that schemes like [38] and [42] have very low computation costs, but the communication cost is too high. In comparison to this, our scheme shows a little more computation cost because of bilinear pairing but it uses minimum number of messages exchange to achieve mutual authentication and thus gives a tough competition in terms of communication cost to other schemes. In addition, our scheme excels in security and functionality features than other schemes.

8. Conclusion and future work

In this paper, we designed a remote access control mechanism as a countermeasure to security issues in smart transportation. According to our scheme TA initially authenticates a vehicle before allowing it to be a part of the network. Further the authenticated vehicle and TA compute a session key to communicate securely. We also propose a vehicle addition phase where any new vehicle can easily be registered via TA. Our scheme also facilitates password update phase which allows vehicles to change their passwords if it is stolen or breached. Later, we analyze the security of our scheme informally and formally using AVISPA simulation to show that it can resist various well known attacks. Finally, a comprehensive performance analysis shows the competency of our scheme against other existing schemes in terms of computation, communication costs. The comparison in security and functionality features shows that our scheme is superior to most of the existing schemes.

In recent years, the lattice-based cryptographic techniques are applied in many networking environments due to its superior security as compared to the traditional public key cryptosystems as they are quantum resistant against various attacks as pointed out by [15] for designing "lattice-based secure cryptosystem for smart healthcare in smart cities". Hence, in future we would like to explore to design more efficient and secure system for IoV based on the lattice-based cryptography.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Palak Bagga: Conceptualization, Methodology, Software, Data curation, Writing – original draft. **Ashok Kumar Das:** Conceptualization, Methodology, Writing – review & editing, Visualization, Supervision, Project administration. **Joel J.P.C. Rodrigues:** Conceptualization, Writing – review & editing, Visualization, Supervision, Funding acquisition.

Acknowledgments

This work was supported by FCT/MCTES through national funds and when applicable co-funded EU funds under the Project UIDB/50008/2020; and by the Brazilian National Council for Research and Development (CNPq) via Grant No. 313036/2020-9. The authors would like to thank the anonymous reviewers, associate editor and editor-in-chief for their valuable feedback on the paper.

References

[1] O.Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, A. Mouzakitis, Intrusion detection systems for intra-vehicle networks: A review, IEEE Access 7 (2019) 21266–21289.
[2] M.A. Al-Shareeda, M. Anbar, I.H. Hasbullah, S. Manickam, S.M. Hanshi, Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks, IEEE Access 8 (2020) 144957–144968, doi:10.1109/ACCESS.2020.3014678.
[3] S.A. Alfadhli, S. Lu, K. Chen, M. Sebai, MFSPV: A multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs, IEEE Access 8 (2020) 142858–142874, doi:10.1109/ACCESS.2020.3014038.
[4] T. Alladi, S. Chakravarty, V. Chamola, M. Guizani, A lightweight authentication and attestation scheme for in-transit vehicles in iov scenario, IEEE Transactions on Vehicular Technology 69 (2020) 14188–14197, doi:10.1109/TVT.2020.3038834.
[5] M.N. Aman, U. Javaid, B. Sikdar, A privacy-preserving and scalable authentication protocol for the internet of vehicles, IEEE Internet of Things Journal 8 (2021) 1123–1139, doi:10.1109/JIOT.2020.3010893.
[6] AVISPA, Automated validation of internet security protocols and applications, 2019a, http://www.avispa-project.org/.Accessed on January 2020.
[7] AVISPA, SPAN, the security protocol ANimator for AVISPA, 2019b, http://www.avispa-project.org/. Accessed on January 2019.
[8] M. Azees, P. Vijayakumar, L.J. Deboarh, EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks, IEEE Transactions on Intelligent Transportation Systems 18 (2017) 2467–2476.
[9] P. Bagga, A.K. Das, M. Wazid, J.J.P.C. Rodrigues, K.K.R. Choo, Y. Park, On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system, IEEE Transactions on Vehicular Technology 70 (2021) 1736–1751, doi:10.1109/TVT.2021.3050614.
[10] P. Bagga, A.K. Das, M. Wazid, J.J.P.C. Rodrigues, Y. Park, Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges, IEEE Access 8 (2020) 54314–54344, doi:10.1109/ACCESS.2020.2981397.
[11] M. Bayat, M. Barmshoory, M. Rahimi, M.R. Aref, A secure authentication scheme for VANETs with batch verification, Wireless Networks 21 (2015) 1733–1743.
[12] D. Boneh, Pairing-based cryptography: Past, present, and future, in: International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'12), Beijing, China, 2012, p. 1.
[13] R. Canetti, H. Krawczyk, Analysis of key-exchange protocols and their use for building secure channels, in: Advances in Cryptology – EUROCRYPT, Springer Berlin Heidelberg, Innsbruck (Tyrol), Austria, 2001, pp. 453–474.
[14] S. Challa, M. Wazid, A.K. Das, N. Kumar, A. Reddy, E.J. Yoon, Y. Kee-Young, Secure signature-based authenticated key establishment scheme for future iot applications, IEEE Access 5 (2017) 3028–3043.
[15] R. Chaudhary, A. Jindal, G.S. Aujla, N. Kumar, A.K. Das, N. Saxena, LSCSH: Lattice-based secure cryptosystem for smart healthcare in smart cities environment, IEEE Communications Magazine 56 (2018) 24–32.
[16] K.K. Chauhan, S. Kumar, S. Kumar, The design of a secure key management system in vehicular ad hoc networks, in: 2017 Conference on Information and Communication Technology (CICT), Gwalior, India, 2017, pp. 1–6.
[17] C.M. Chen, B. Xiang, Y. Liu, K.H. Wang, A secure authentication protocol for internet of vehicles, IEEE Access 7 (2019) 12047–12057, doi:10.1109/ACCESS.2019.2891105.
[18] J. Cui, D. Wu, J. Zhang, Y. Xu, H. Zhong, An efficient authentication scheme based on semi-trusted authority in VANETs, IEEE Transactions on Vehicular Technology 68 (2019) 2972–2986.
[19] A.K. Das, A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks, International Journal of Information Security 11 (2012) 189–211.
[20] A.K. Das, B. Bruhadeshwar, An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system, Journal of Medical Systems 37 (2013) 9969.
[21] D. Dolev, A. Yao, On the security of public key protocols, IEEE Transactions on Information Theory 29 (1983) 198–208.
[22] A. Dua, N. Kumar, A.K. Das, W. Susilo, Secure message communication protocol among vehicles in smart city, IEEE Transactions on Vehicular Technology 67 (2018) 4359–4373.
[23] W. Fu, X. Xin, P. Guo, Z. Zhou, A practical intrusion detection system for internet of vehicles, China Communications 13 (2016) 263–275, doi:10.1109/CC.2016.7733050.
[24] L. Gafencu, L. Scripcariu, Security issues in the internet of vehicles, in: 2018 International Conference on Communications (COMM), Bucharest, Romania, 2018, pp. 441–446.
[25] N.B. Gayathri, G. Thumbur, P.V. Reddy, Z.U.R. Muhammad, Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks, IEEE Access 6 (2018) 31808–31819.
[26] X. Guo, C. Chen, C. Gong, F. Leu, A secure official vehicle communication protocol for VANET, in: 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Fukuoka, Japan, 2016, pp. 482–485.
[27] N. Gupta, R. Manaswini, B. Saikrishna, F. Silva, A. Teles, Authentication-based secure data dissemination protocol and framework for 5g-enabled VANET, Future Internet 12 (2020).
[28] H.J. Jo, I.S. Kim, D.H. Lee, Reliable cooperative authentication for vehicular networks, IEEE Transactions on Intelligent Transportation Systems 19 (2018) 1065–1079.
[29] M.S. Kakkasageri, S.S. Manvi, Multiagent driven dynamic clustering of vehicles in VANETs, Journal of Network and Computer Applications 35 (2012) 1771–1780.
[30] J.B. Kenney, Dedicated short-range communications (DSRC) standards in the united states, Proceedings of the IEEE 99 (2011) 1162–1182.
[31] C.C. Lee, C.T. Chen, P.H. Wu, T.Y. Chen, Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices, IET Computers & Digital Techniques 7 (2013) 48–56.
[32] C. Li, S. Ji, X.Z.H.W.D. Li, H. Liu, An effective and secure key management protocol for message delivery in autonomous vehicular clouds, 2018, 18.
[33] J. Li, H. Lu, M. Guizani, ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs, IEEE Transactions on Parallel and Distributed Systems 26 (2015) 938–948.

[34] K. Lim, K.M. Tuladhar, X. Wang, W. Liu, A scalable and secure key distribution scheme for group signature based authentication in VANET, in: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New york, USA, 2017, pp. 478–483.
[35] J. Liu, Q. Li, R. Sun, X. Du, M. Guizani, An efficient anonymous authentication scheme for internet of vehicles, in: IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1–6.
[36] Y. Liu, Y. Wang, G. Chang, Efficient privacy-preserving dual authentication and key agreement scheme for secure v2v communications in an iov paradigm, IEEE Transactions on Intelligent Transportation Systems 18 (2017) 2740–2749.
[37] A. Menezes, An introduction to pairing-based cryptography, 2013, (????). Accessed on May 2020.
[38] M. Sadri, M. Rajabzadeh Asaar, A lightweight anonymous two-factor authentication protocol for wireless sensor networks in internet of vehicles, International Journal of Communication Systems 33 (2020) e4511, doi:10.1002/dac.4511.
[39] J. Shao, X. Lin, R. Lu, C. Zuo, A threshold anonymous authentication protocol for VANETs, IEEE Transactions on Vehicular Technology 65 (2016) 1711–1720.
[40] S. Sharma, B. Kaushik, A survey on internet of vehicles: Applications, security issues & solutions, Vehicular Communications 20 (2019) 100182, doi:10.1016/j.vehcom.2019.100182.
[41] A.K. Sutrala, P. Bagga, A.K. Das, N. Kumar, J.J.P.C. Rodrigues, P. Lorenz, On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment, IEEE Transactions on Vehicular Technology 69 (2020) 5535–5548, doi:10.1109/TVT.2020.2981934.
[42] H. Vasudev, V. Deshpande, D. Das, S.K. Das, A lightweight mutual authentication protocol for v2v communication in internet of vehicles, IEEE Transactions on Vehicular Technology 69 (2020) 6709–6717.
[43] M. Wazid, P. Bagga, A.K. Das, S. Shetty, J.J.P.C. Rodrigues, Y.H. Park, Akm-iov: Authenticated key management protocol in fog computing-based internet of vehicles deployment, IEEE Internet of Things Journal (2019) 1.
[44] L. Wu, Q. Sun, X. Wang, J. Wang, S. Yu, Y. Zou, B. Liu, Z. Zhu, An efficient privacy-preserving mutual authentication scheme for secure v2v communication in vehicular ad hoc network, IEEE Access 7 (2019) 55050–55063.
[45] B. Ying, A. Nayak, Anonymous and lightweight authentication for secure vehicular networks, IEEE Transactions on Vehicular Technology 66 (2017) 10626–10636, doi:10.1109/TVT.2017.2744182.
[46] S. Yu, J. Lee, K. Lee, K. Park, Y. Park, Secure authentication protocol for wireless sensor networks in vehicular communications, Sensors 18 (2018).
[47] H. Zhong, J. Wen, J. Cui, S. Zhang, Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET, Tsinghua Science and Technology 21 (2016) 620–629, doi:10.1109/TST.2016.7787005.