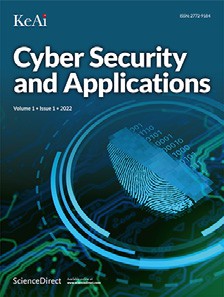
[Cyber Security and Applications 1 (2023) 100001](https://doi.org/10.1016/j.csa.2022.100001)

Contents lists available at [ScienceDirect](http://www.ScienceDirect.com/)

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](#_bookmark0), Ashok Kumar Das [b](#_bookmark1),[∗](#_bookmark4), Joel J.P.C. Rodrigues [c](#_bookmark2),[d](#_bookmark3)

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*

a r t i c l e i n f o a b s t r a c t

*Keywords:*

Internet of Vehicles (IoV) Smart transportation

Intelligent Transportation System (ITS) Authentication

Bilinear pairing Security

Internet of Vehicles (IoV) enabled Intelligent Transportation System (ITS) allows smart vehicles to communi- cate 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, im- personation, 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

it has to register to the nearest trusted authority (*𝑇 𝐴*) in oﬄine or secured channel mode. To make it applica- in an IoV paradigm, that is, they are not under fixed domains. Therefore, whenever a vehicle changes its location ble, we propose *remote registration* of the vehicles via the *𝑇 𝐴*. Access control mechanism occurs in two phases:

1) node authentication phase, where vehicles are remotely authenticated by *𝑇 𝐴* 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.

# Introduction

Internet of Things (IoT) combines various technologies like embed- ded systems, wireless sensors networks, control system appliance au- tomation, 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 cus- tomers. IoV advances to claim a new concept of Intelligent Transporta- tion System (ITS) in smart cities. Smart vehicles (with installed OBU),

vehicle’s intelligence, diverse communication patterns, connection to In- ternet together forms ITS. ITS regulates the coordination between vehic- ular 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 nav- igation, 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 bor- rows its technologies and benefits. But, at the same time it also has to deal with other crucial and strict requirements like limited communica- tion 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](mailto:palak.bagga@research.iiit.ac.in) (P. Bagga), [iitkgp.akdas@gmail.com](mailto:iitkgp.akdas@gmail.com), [ashok.das@iiit.ac.in](mailto:ashok.das@iiit.ac.in) (A.K. Das), [joeljr@ieee.org](mailto: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

2772-9184/© 2022 The Authors. Published by Elsevier B.V. on behalf of KeAi Communications Co., Ltd. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

wireless open channel directly or indirectly through messages or bea- cons. 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 con- trol schemes etc. These mechanisms would provide the required “secu- rity and functionality features to smart transportation”.

The authors in [[10]](#_bookmark41) provided a detailed taxonomy of various secu- rity protocols that are necessary to maintain a secured IoV environment. The basic security protocols related to IoV and other networking envi- ronments are categorized as key management like the schemes of [[19]](#_bookmark48), [[32]](#_bookmark64), [[34]](#_bookmark68), [[16]](#_bookmark45), [[26]](#_bookmark55), [[43]](#_bookmark71), authentication schemes such as [[20]](#_bookmark51), [[39]](#_bookmark74),

[[36]](#_bookmark71), [[28]](#_bookmark58), [[35]](#_bookmark70), [[18]](#_bookmark49), [[44]](#_bookmark72), [[42]](#_bookmark70), privacy preservation schemes such as

[[11]](#_bookmark42), [[33]](#_bookmark66), [[47]](#_bookmark75), [[8]](#_bookmark35), [[25]](#_bookmark56), [[41]](#_bookmark76), intrusion detection systems proposed

by [[1]](#_bookmark62), [[23]](#_bookmark54), [[24]](#_bookmark57), and access control schemes.

In this paper, we focus mainly on access control mechanism. An ac- cess control scheme ensures a secured environment to provide uninter- rupted services. IoV is a dynamic network where the location of the ve- hicle keeps changing every instant so does the nearest neighbors. Also, due to increasing population, the number of vehicles bought and reg- istered are increasing drastically everyday. Therefore, the need of an hour is to have an access control scheme which ensures that the mem- bers 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 differen- tiate between a genuine and a malicious vehicle. Therefore a success- ful access control mechanism controls the flow of false, invalid, illegal and unauthorized information within the network. It also manages ac- cess permissions, monitors the scalable IoV architecture, handles huge amount of data stream, and also keeps a track of allocation and utiliza- tion 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 *𝑇 𝐴*,

after which it is deployed and allowed to communicate and access

the network.

ployed node and the *𝑇 𝐴* compute a secret session key that is used to *• Key establishment:* After the successful authentication, a newly de-

ensure secured communication over a public channel. The key com- puted 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. *Research contributions*

The major contributions of the paper as stated as follows.

between a vehicle and its nearest *𝑇 𝐴*. The vehicles are registered via *•* We propose a remote access control scheme which is implemented the *𝑇 𝐴* over secure channel. The access control mechanism works in

between *𝑇 𝐴* and a vehicle. After successful authentication, a session two phases. In the first phase, a remote mutual authentication occurs

key is computed for future communications in the second phase.

* + - Our proposed scheme facilitates vehicle addition phase and pass- word update phase. The proposed scheme can be also extended in

formed cluster of vehicles with the help of the *𝑇 𝐴*. establishing session keys between any two vehicles in a dynamically

* + - In the later part, we also analyze the security of our scheme. An in- formal 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 Proto- cols and Applications (AVISPA)” [[6]](#_bookmark36) software tool, shows that our scheme can resist passive/active adversarial attacks.

* + - A comprehensive performance analysis evaluates computation, com- munications cost of our scheme in comparison to other existing schemes. We also list down other security and functionality features.
  1. *Paper outline*

The layout of the paper is as follows.

* + - In [Section 2](#_bookmark5) we describe the network and the threat model used in the scheme.
    - Next, in [Section 3](#_bookmark8) 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](#_bookmark11) we describe our proposed scheme in six phases which are defined in [Sections 4.1](#_bookmark9) – [4.6](#_bookmark18). In [Section 5](#_bookmark20), we then extended this basic scheme where any two vehicles in a cluster can establish session key for their secret communication.
    - In [Section 6](#_bookmark21) we provide the security analysis of our scheme. We pro- vide the correctness proof of our verification phase. Severeal propo- sitions 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]](#_bookmark36).
    - In [Section 7](#_bookmark29) we perform a detailed comparative analysis of our scheme against few existing schemes in terms of computation, com- munication costs and other security and functionality features.
    - The conclusion of the paper is presented in [Section 8](#_bookmark40).

# System models

The network and threat model is described as follows.

* 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, mul- timedia 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

ity (*𝑇 𝐴*). They can be single or multiple *𝑇 𝐴*s to supervise a smart city. scheme, a vehicle remotely registers itself to the nearest trusted author- To preserve the identity, the *𝑇 𝐴*s 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 communi- cations like interactions with other vehicles via *Vehicle to Vehicle (V2V) communication*. The vehicles exchange updated traﬃc related informa-

tion. The communication between *𝑇 𝐴* and vehicle occurs via *Vehicle to*

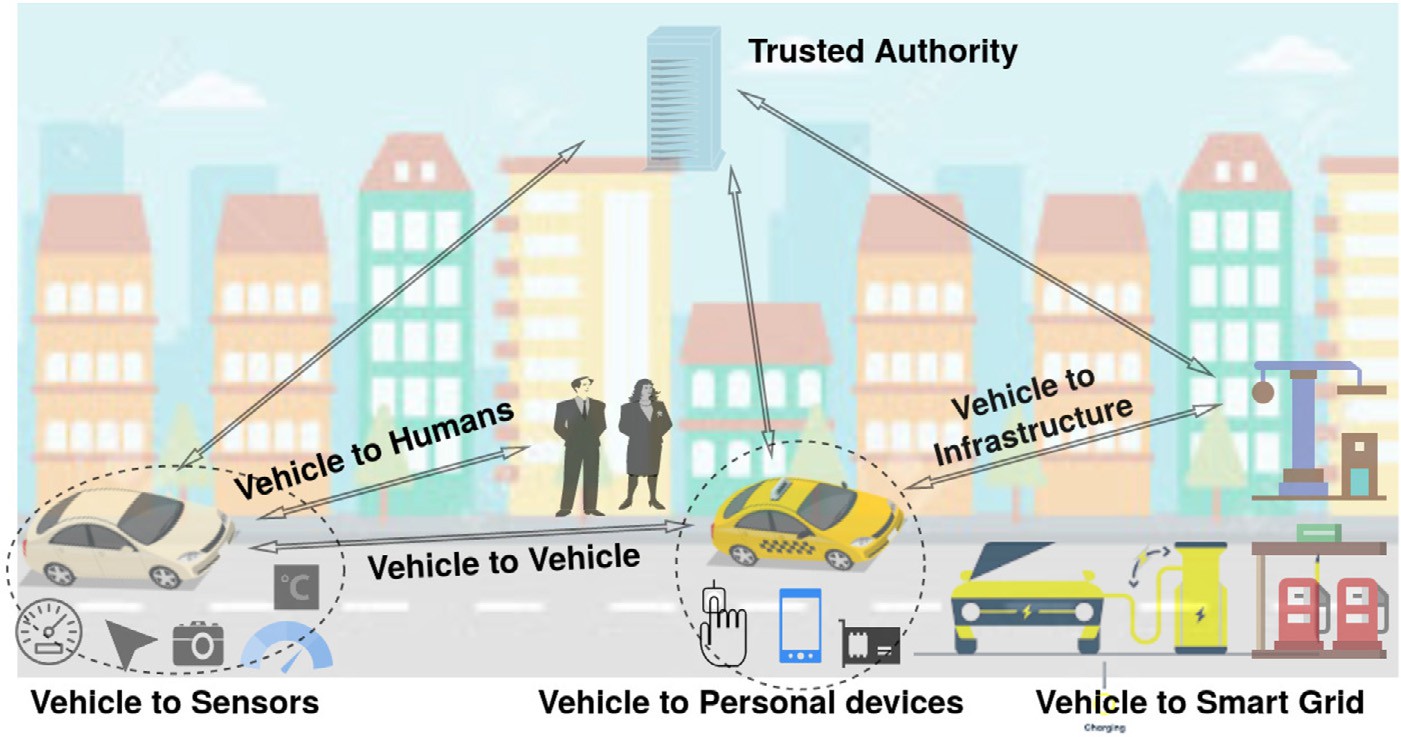
*Infrastructure (V2I) communication*. Vehicle to pedestrian, vehicle to cus-

tomer communication occurs via *Vehicle to Human (V2H) communication* through which vehicle provides user services and safe transportation fa- cilities to passengers and customers. Vehicles can even exchange infor- mation with personal devices through *Vehicle to Personal devices (V2P) communication*. The vehicles are installed with sensors and the commu- nication between them occurs via *Vehicle to Sensor (V2S) communication*

[[40]](#_bookmark75). *𝑇 𝐴* checks the authenticity of the messages flown by the vehicle

therefore, the communication between the vehicle and *𝑇 𝐴* takes place in the network. Our proposed scheme supports remote authentication,

through “wireless medium using the IEEE 802.11p protocol” and “Ded- icated Short-Range Communications (DSRC)” [[30]](#_bookmark59).

**Fig. 1.** IoV network model

[Figure 1](#_bookmark7) shows the architecture of smart transportation network model.

* 1. *Threat model*

We have considered “Dolev-Yao threat (DY) model” [[21]](#_bookmark52) as the threat model for the proposed scheme. The model considers the follow- ing 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 au-

thorities (TAs) are assumed to be fully trusted entities.

* + - Following to this the model considers an adversary A, with enough capabilities such the an adversary can perform fabrication, eaves- dropping, 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]](#_bookmark44); 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.

# Related work

[[45]](#_bookmark73) 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

in their vehicles. Vehicle proves its legitimacy to TA via *𝑅𝑆𝑈* and es- to achieve freshness. Users use their smart card and passwords to log

tablishes 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.

eﬃcient protocol. They assumed a single TA with multiple *𝑅𝑆𝑈* model, [[17]](#_bookmark50) addressed the short comings in ASC by [[45]](#_bookmark73) and proposed an where TA and *𝑅𝑆𝑈* always have secured communications. The vehicle sends a request message to *𝑅𝑆𝑈* which is relayed to *𝑇 𝐴* after checking its authenticity. The reply from the *𝑇 𝐴* is broadcasted to *𝑅𝑆𝑈* and other near by *𝑅𝑆𝑈* s. 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]](#_bookmark74) designed a password based secure authentication protocol for wireless sensor networks (WSNs) in vehicular communications. The pro- tocol 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 col- lected by authenticated vehicles is sent and collected in the sink node, which is accessed to provide user services in future. [[38]](#_bookmark73) claimed that the Yu *et al.*’s scheme cannot resist “sensor capture attack, user trace- ability 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]](#_bookmark73) 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 se- cured 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]](#_bookmark72) proposed an “eﬃcient privacy-preserving mutual authentica-

tion scheme for secure V2V communications” where a vehicle is au- thenticated 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]](#_bookmark70) 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]](#_bookmark70), and [[44]](#_bookmark72), is not secured against CK-adversary attack.

[[3]](#_bookmark67) 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 func- tions (PUF), vehicle’s private key and one time pseudo identity. The mechanism is decentralized and reduces redundant authentications. Af- ter vehicle to central authority mutual authentication phase, a regional key is established which is valid until the vehicle reaches a new region.

[[27]](#_bookmark60) also proposed an authentication-based secure data dissemination protocol and framework for 5G-enabled VANET. The authenticated vehi- cles are allowed to exchange messages only after validating each other. The message integrity is checked by calculating the disparity in the com- munication bits.

[[2]](#_bookmark65) designed an “eﬃcient conditional privacy preservation with mu- tual authentication”. The TA divides the system into domains with speci-

fied number of *𝑅𝑆𝑈* s to cover the region. At the time of authentication,

the RSU provides a pool of pseudo identities and their corresponding

cation within the *𝑅𝑆𝑈* ’s coverage area. OBU uses the pseudo identity secret keys with expiry to the vehicle, that can be used for communi-

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 de- signed in [[9]](#_bookmark37) 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 au-

phase. 3) Log in phase. 4) Authentication and verification phase. 5) Key agreement phase. 6) Password update phase. To avoid replay at- tacks 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 any- time change its password if in case the password is lost or breached. The notations used through out the description of the scheme is de- fined in the [Table 2](#_bookmark13). We now present the proposed scheme in following subsections.

* 1. *Initial setup phase*

The initial set up phase is performed by the *𝑇 𝐴* authorized for a smart city. The *𝑇 𝐴* 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, *𝑇 𝐴* chooses a non-singular elliptic curve

*𝐸𝑞* (*𝑢, 𝑣*) of the form: *𝑦*2 = *𝑥*3 + *𝑢𝑥* + *𝑣* (mod *𝑞*) such that 4*𝑢*3 + 27*𝑣*2 ≠ 0 (mod *𝑞*). *𝑇 𝐴* also picks an additive group *𝐺*1 with point at infinity U 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 bi- linear mapping *𝑒*: *𝐺*1 × *𝐺*1 → *𝐺*2 . The bilinear mapping has following

properties [[12,37]](#_bookmark43):

* + - * **Bilinearity**: For all “*𝑃 , 𝑄, 𝑅* ∈ *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* ∈ *𝑍* ∗ =

*𝑞*

thentication a session key is also established.

Recently, [[5]](#_bookmark38) proposed a “privacy-preserving and scalable authenti- cation protocol for the IoV” which is also based on “physical unclonable function (PUF)”. PUF is installed in the vehicle’s OBU. During registra- tion, vehicles generate crypto identity using PUF, random nonce and hashing, and send it to TA along with few challenge response pairs.

All *𝑅𝑆𝑈* s also store current challenge and nonce. During vehicle to TA

where *𝑅𝑆𝑈* consolidates request messages, creates a reply by encrypt- authentication phase, all vehicles send their crypto identities to RSU

ing and hashing, and forwards to RSU gateway. RSU gateway forwards the request to TA after verification. TA generates a token for each ver- ified vehicle containing a challenge and sends the authorized response

to the gateway. The gateway forwards the reply to all *𝑅𝑆𝑈* s in its re-

gion 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]](#_bookmark69). IoV cloud servers are database that stores the challenge responses and other information. TA

registers vehicles and *𝑅𝑆𝑈* s. A vehicle sends an authentication request

message to *𝑅𝑆𝑈* whenever it comes in range of any *𝑅𝑆𝑈* . *𝑅𝑆𝑈* veri- fies the vehicle by contacting edge servers (attached to *𝑅𝑆𝑈* for stor-

age and computation purposes) for registration details. A session key is established which is used for encryption and for an in-transit attesta- tion 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](#_bookmark12) summarises the characteristics and limitations of the dis- cussed schemes.

# The proposed scheme

In this section, we present a new remote access control scheme for

{1*,* 2*,* ⋯ *, 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* ) ≠ 1*𝐺*1 for all *𝑃* ∈ *𝐺*1 .

“*𝑒*(*𝑃 , 𝑄*) for all *𝑃 , 𝑄* ∈ *𝐺*1”. *•* **Computability**: There exists an eﬃcient algorithm to calculate

* **Step 2:** In the second step, *𝑇 𝐴* randomly selects *𝑝𝑟𝑇 𝐴* ∈ *𝑍* ∗, and sets

*𝑞*

it as its private key. Using its private key *𝑝𝑟𝑇 𝐴*, *𝑇 𝐴* calculates its public key by *𝑃 𝑢𝑏𝑇𝐴* = *𝑝𝑟𝑇 𝐴* ⋅ *𝑃* .

* **Step 3:** Next, *𝑇 𝐴* computes a public verification factor *𝑣𝑒𝑟* as, *𝑣𝑒𝑟* =

*𝑒*(*𝑃 𝑢𝑏𝑇𝐴, 𝑃* ) and also chooses two cryptographic hash functions, de- fined as *ℎ*(⋅): {0*,* 1}∗ → {0*,* 1}∗, and *𝐻* : {0*,* 1}∗ → *𝐺*1 .

* **Step 4:** Finally, *𝑇 𝐴* publicly publishes the system parameters: {*𝐺*1*,*

*𝐺*2 *, 𝑒, 𝑞, 𝑃 , ℎ*(⋅)*, 𝐻* (⋅)*, 𝑃 𝑢𝑏𝑇𝐴, 𝑣𝑒𝑟*} at the end of the set up phase.

* 1. *Registration phase*

The *𝑇 𝐴* is responsible for registering vehicles before their deploy- ment. *𝑇 𝐴* 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 *𝑉𝑖* , following steps are performed between *𝑉𝑖* and *𝑇 𝐴*.

* + - **Step 1:** Vehicle *𝑉𝑖* chooses its unique identity *𝐼𝐷𝑖* and calculates its pseudo identity *𝑅𝐼 𝐷𝑖* as *𝑅𝐼 𝐷𝑖* = *𝐻* (*𝐼𝐷𝑖* ). *𝑉𝑖* sends its pseudo iden- tity *𝑅𝐼 𝐷𝑖* , and hashed unique number *ℎ*(*𝑉 𝑈𝑁𝑖* ) to *𝑇 𝐴* via a secure channel. For instance, the information {*𝑅𝐼 𝐷𝑖* , *ℎ*(*𝑉 𝑈𝑁𝑖* )} can be en- crypted with the help of the public key of the *𝑇 𝐴* and the encrypted credentials can be sent via public channel to the *𝑇 𝐴*, and the *𝑇 𝐴* will decrypt the encrypted credentials using its own private key *𝑝𝑘𝑇 𝐴*.
    - **Step 2:** On receiving *𝑅𝐼 𝐷𝑖* , *ℎ*(*𝑉 𝑈𝑁𝑖* ) from *𝑉𝑖* , *𝑇 𝐴* checks for the

presence of *ℎ*(*𝑉 𝑈𝑁𝑖* ) in its database. If the entry is present in its

of the same vehicle. If *ℎ*(*𝑉 𝑈𝑁𝑖* ) is not present in the database, it database it stops the further process to avoid multiple registration

makes the entry of the vehicle’s number in the table and proceeds the

registration process. *𝑇 𝐴* computes *𝑅𝑒𝑔𝐼𝐷* as, *𝑅𝑒𝑔𝐼𝐷* = *𝑝𝑘𝑇 𝐴* ⋅ *𝑅𝐼 𝐷𝑖* .

*𝑖 𝑖*

smart transportation. The scheme is based on the architecture described in [Section 2.1](#_bookmark6). According to our scheme, initially a vehicle remotely

mutually authenticates *𝑇 𝐴* and then both vehicle and *𝑇 𝐴* compute se-

cret session key for secure communication in future. Our scheme oc-

*𝑇 𝐴* chooses a temporary identity *𝑇 𝐼𝐷𝑖* for vehicle *𝑉𝑖* , and computes

pseudo temporary identity as *𝑅𝑇 𝐼𝐷𝑖* = *ℎ*(*𝑇 𝐼𝐷𝑖* ‖*𝑝𝑘𝑇 𝐴*).

* **Step 3:** Finally, *𝑇 𝐴* generates a current timestamp as *𝑇 𝑆𝑇𝐴*1 , and

sends the registration reply message {*𝑇 𝐼𝐷𝑖 , 𝑅𝑒𝑔𝐼𝐷 , 𝑅𝑇 𝐼𝐷𝑖 , 𝑇 𝑆𝑇𝐴* }

curs in following phases. 1) TA initial set up phase. 2) Registration

to *𝑉𝑖* over secure channel.

*𝑖* 1

**Table 1**

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

|  |  |
| --- | --- |
| Scheme | Description & Limitations/Drawbacks |
| [[45]](#_bookmark73) | 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]](#_bookmark50) | 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]](#_bookmark74) | 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]](#_bookmark73) | 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]](#_bookmark38) | 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]](#_bookmark69) | 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]](#_bookmark72) | 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]](#_bookmark67) | 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]](#_bookmark65) | 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]](#_bookmark60) | 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]](#_bookmark70) | 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]](#_bookmark37) | 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**

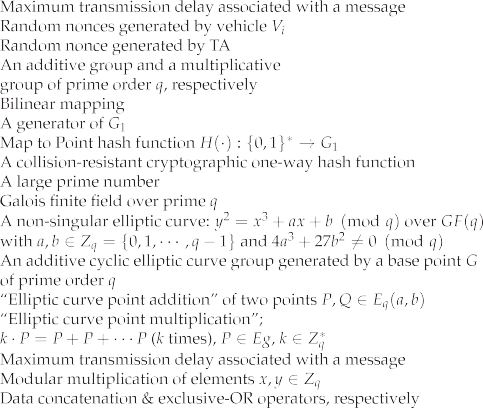
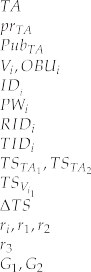
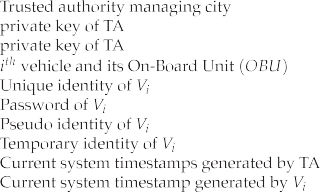
Notations and their meanings

* **Step 5:** *𝑂𝐵𝑈𝑖* of vehicle *𝑉𝑖* stores {*𝑇 𝐼𝐷𝑖*, *𝑉 𝐷𝐼𝐷𝑖*, *𝑉 𝐷𝑖*, *𝑉 𝐴𝑖*, *𝑉 𝐵𝑖*}

in its memory, and deletes {*𝑅𝑒𝑔𝐼𝐷* , *𝑅𝑇 𝐼𝐷𝑖*} permanently from its

*𝑖*

memory.



[Figure 2](#_bookmark16) summarizes the registration phase.

* 1. *Login phase*

In login phase, user of vehicle *𝑉𝑖* inputs its identity *𝐼𝐷𝑖* and pass- word *𝑃 𝑊𝑖* associated with vehicle in the *𝑂𝐵𝑈𝑖*. Then, *𝑂𝐵𝑈𝑖* executes

the following steps.

* + - **Step 1:** *𝑂𝐵𝑈𝑖* computes random nonce *𝑟*∗ as, *𝑟*∗ = *𝑟𝑖 ⊕ ℎ*(*𝐼𝐷𝑖* ‖*𝑃 𝑊𝑖*)

*𝑖 𝑖*

and then computes *𝑅𝑒𝑔*∗

as, *𝑅𝑒𝑔*∗

= *𝑉 𝐷𝐼𝐷𝑖*− *𝐻* (*𝑃 𝑊𝑖* ‖*𝑟*∗), *𝑉 𝐴*∗ =

∗ ∗ *𝐼𝐷𝑖*

*𝐼𝐷𝑖*

*𝑖 𝑖*

∗



* **Step 4:** After receiving registration reply message

{*𝑇 𝐼𝐷𝑖, 𝑅𝑒𝑔𝐼𝐷 , 𝑅𝑇 𝐼𝐷𝑖, 𝑇 𝑆𝑇𝐴* } from *𝑇 𝐴*, *𝑂𝐵𝑈𝑖* of *𝑉𝑖* first veri- fies the received timestamp *𝑇 𝑆𝑇𝐴*1 against the current timestamp

*𝑖* 1

*ℎ*(*𝐼𝐷𝑖* ‖*𝑅𝑒𝑔𝐼𝐷* ‖*ℎ*(*𝑟𝑖* ‖*𝑃 𝑊𝑖*)) and verifies if *𝑉 𝐴𝑖* = *𝑉 𝐴𝑖* 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.

*𝑖*

* + **Step 2:** Following this, *𝑂𝐵𝑈𝑖* generates two random nonces *𝑟*1*, 𝑟*2 ∈

*𝑍*∗, and performs the following computations. It computes *𝑉 𝑍𝑖* =

*𝑉 𝐷𝑖⊕ ℎ*(*𝑅𝐼 𝐷𝑖* ‖*𝑃 𝑊𝑖* ‖*𝑟*∗), *𝑉 𝐹𝑖* = *𝑅𝐼 𝐷𝑖⊕ ℎ*(*𝑉 𝑍𝑖* ‖*𝑟*1), *𝑉 𝐺𝑖* = *𝑟*2 ⋅

*𝑞*

*𝑃 𝑢𝑏𝑇𝐴* +*𝑅𝑒𝑔𝐼𝐷𝑖* , *𝑉 𝐿𝑖* = *ℎ*(*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴* ‖*𝑅𝐼 𝐷𝑖*).

*𝑖*

* + **Step 4:** *𝑉𝑖* generates a current timestamp as *𝑇 𝑆𝑉𝑖*1 and sends au- thentication request message consisting of {*𝑇 𝐼𝐷𝑖, 𝑉 𝐹𝑖, 𝑉 𝐺𝑖, 𝑉 𝐿𝑖,*

*𝑟*1*, 𝑇 𝑆𝑉𝑖*1 } to TA via open public channel.

* 1. *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 *𝑇 𝐴*s. The data shared between

by the condition: |*𝑇 𝑆*∗

*𝑇𝐴*1

– *𝑇 𝑆𝑇𝐴*1 | ≤ Δ*𝑇 𝑆*, where Δ*𝑇 𝑆* is the

them is traﬃc related data which is further used for decision making and

timestamp is valid, *𝑂𝐵𝑈𝑖* of *𝑉𝑖* asks the user of the vehicle to choose “maximum transmission delay associated with a message”. If the and enter password *𝑃 𝑊𝑖* associated with *𝑉𝑖*. Then *𝑂𝐵𝑈𝑖* generates a random nonce *𝑟𝑖* ∈ *𝑍*∗, and computes *𝑉 𝐷𝐼𝐷𝑖*, *𝑉 𝐷𝑖*, *𝑉 𝐴𝑖*, *𝑉 𝐵𝑖* as,

*𝑞*

*𝑉 𝐷𝐼𝐷𝑖* = *𝑅𝑒𝑔𝐼𝐷* + *𝐻* (*𝑃 𝑊𝑖* ‖*𝑟𝑖*), *𝑉 𝐷𝑖* = *𝑅𝑇 𝐼𝐷𝑖⊕ ℎ*(*𝐼𝐷𝑖* ‖*𝑃 𝑊𝑖* ‖*𝑟𝑖*),

*𝑉 𝐴𝑖* = *ℎ*(*𝐼𝐷𝑖* ‖*𝑅𝑒𝑔𝐼𝐷* ‖*ℎ*(*𝑟𝑖* ‖*𝑃 𝑊𝑖*)), *𝑉 𝐵𝑖* = *ℎ*(*𝐼𝐷𝑖* ‖*𝑟𝑖* ‖*𝑃 𝑊𝑖*) *⊕𝑅𝐼𝐷𝑖*.

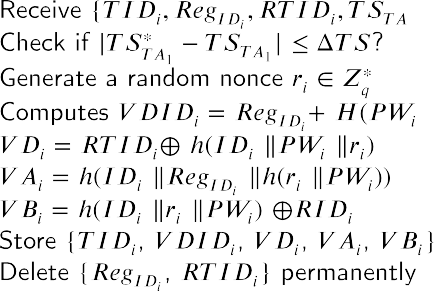
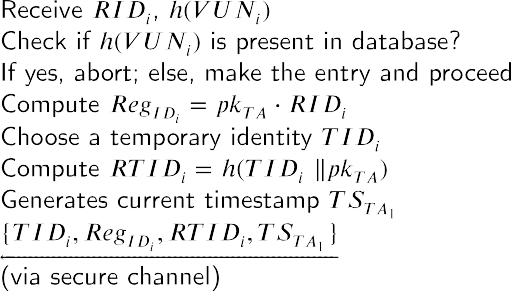
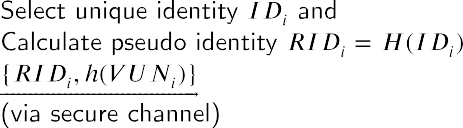
*𝑖*

*𝑖*

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

{*𝑇 𝐼𝐷𝑖, 𝑉 𝐹𝑖, 𝑉 𝐺𝑖, 𝑉 𝐿𝑖, 𝑟*1*, 𝑇 𝑆𝑉𝑖*1 } from *𝑉𝑖*, *𝑇 𝐴* first verifies the



**Fig. 2.** Summary of vehicle registration phase

received timestamp *𝑇 𝑆**𝑉𝑖*1 against the current timestamp by the

condition: |*𝑇 𝑆* ∗ − *𝑇 𝑆𝑉* | ≤ Δ*𝑇 𝑆*. If the timestamp is valid, it

[Figure 3](#_bookmark17) summarizes the log in, authentication, verification and key establishment phases.

∗ *𝑉𝑖*1

*𝑖*1 ∗ ∗

computes *𝑉 𝑍𝑖* = *ℎ*(*𝑇 𝐼𝐷𝑖* ‖*𝑝𝑘𝑇 𝐴*), *𝑅𝐼 𝐷𝑖* = *𝑉 𝐹𝑖⊕ ℎ*(*𝑉 𝑍𝑖* ‖*𝑟*1 ).

*𝑖*

* + - **Step 2:** After computing *𝑅𝐼 𝐷*∗, *𝑇 𝐴* checks its validity against the stored *𝑅𝐼 𝐷𝑖* by the equation *𝑅𝐼 𝐷𝑖* = *𝑅𝐼 𝐷*∗? If it is valid, *𝑇 𝐴* com-

putes *𝑅𝑒𝑔*∗ = *𝑝𝑘𝑇 𝐴* ⋅ *𝑅𝐼 𝐷*∗, *𝑉 𝑌𝑖* = *𝑉 𝐺𝑖* − *𝑅𝑒𝑔*∗ . Then *𝑇 𝐴* uses the

*𝑖*

* 1. *Vehicle addition phase*

With the increase in number of vehicles every day, a new vehicle

*𝑖 𝑖*

*𝐼 𝐷 𝑖 𝐼 𝐷*

bilinear pairing equation: *𝑒*(*𝑝𝑟𝑇 𝐴*⋅ (*𝑅𝐼 𝐷*∗) ⋅ *𝑃 , 𝑃* ) = *𝑣𝑒𝑟*

*𝑖*

∗

*𝑖* to verify

*𝑅𝐼 𝐷*

may wish to join the network. Also, there can be a possibility where an existing vehicle might get physically captured or may stop working

the authenticity of the vehicle. It the equation is valid, *𝑇 𝐴* computes

*𝑉 𝐿*∗ = *ℎ*(*𝑉 𝑌𝑖* ‖*𝑅𝐼 𝐷*∗) for the corresponding authorized vehicle.

for some reason. Therefore, a flexible access control scheme should only

allow authenticated vehicle to be deployed in the network. Following

*𝑖 𝑖*

* **Step 3:** In the next step, *𝑇 𝐴* computes a session key. For this, it

generates a random nonce *𝑟*3 ∈ *𝑍* ∗, and computes *𝑉*1 = *𝑟*3 ⋅ *𝑃* , *𝑉*2 =

*𝑞*

steps are performed between new vehicle *𝑉 𝑛𝑒𝑤* and *𝑇 𝐴*.

* + **Step 1:** Vehicle *𝑉 𝑛𝑒𝑤* chooses its unique identity *𝐼𝐷𝑛𝑒𝑤* and calcu-

*𝑖*

*𝑉*1 − *𝑅𝑒𝑔𝐼𝐷𝑖* . Finally it computes the session key between *𝑇 𝐴* and *𝑉𝑖* ,

*𝑖*

*𝑛𝑒𝑤*

*𝑛𝑒𝑤*

*𝑖*

*𝑛𝑒𝑤*

as *𝑆𝐾*

= *ℎ*(*𝑅𝑒𝑔*

‖*𝑉*

‖*𝑉 𝑌* ).

lates its pseudo identity *𝑅𝐼 𝐷𝑖* as *𝑅𝐼 𝐷𝑖* = *𝐻* (*𝐼𝐷𝑛𝑒𝑤*). *𝑉𝑖* sends

*𝑇𝐴*−*𝑉𝑖*

*𝐼𝐷𝑖* 1 *𝑖*

its pseudo identity

*𝑛𝑒𝑤*

*𝑖*

( *𝑛𝑒𝑤* ) to

* **Step 4:** To ensure the integrity of the session key *𝑆𝐾𝑇𝐴*−*𝑉* , while

*𝑅𝐼 𝐷𝑖* , hashed unique number *ℎ 𝑉 𝑈𝑁𝑖*

sending it on an open channel, *𝑇 𝐴* computes *𝑄* = *ℎ*(

∗ *𝑖*

*𝑇 𝐴* via a secure channel.

*𝑖 𝑅𝐼 𝐷𝑖* ‖*𝑆𝐾𝑇𝐴*−*𝑉𝑖*

*𝑛𝑒𝑤*

*𝑛𝑒𝑤*

*𝑛𝑒𝑤*

‖*𝑉*1 ). It generates a new temporary identity *𝑇 𝐼𝐷𝑛𝑒𝑤*, and computes

* + **Step 2:** On receiving *𝑅𝐼 𝐷𝑖* , *ℎ*(*𝑉 𝑈𝑁𝑖* ) from *𝑉𝑖* , the *𝑇 𝐴* checks

*𝑖*

*𝑛𝑒𝑤*

*𝑛𝑒𝑤*

for the presence of *ℎ*(*𝑉 𝑈𝑁𝑛𝑒𝑤*) in its database. If the entry is present

new pseudo temporary identity by *𝑅𝑇 𝐼𝐷𝑖* = *ℎ*(*𝑇 𝐼𝐷𝑖* ‖*𝑝𝑘𝑇 𝐴*).

It computes *𝑉*3 = *𝑅𝑇 𝐼𝐷𝑛𝑒𝑤⊕ 𝑆𝐾𝑇𝐴*−*𝑉* and *𝑉*4 = *𝑇 𝐼𝐷𝑛𝑒𝑤⊕ ℎ*(*𝑉*1 ). Fi-

*𝑖 𝑖 𝑖*

*𝑖*

in its database it stops the further process to avoid multiple reg-

istration of the same vehicle. If *ℎ*(*𝑉 𝑈𝑁𝑛𝑒𝑤*) is not present in the

nally, *𝑇 𝐴* generates another timestamp *𝑇 𝑆𝑇𝐴*2 and sends the authen-

tication reply message as {*𝑄𝑖, 𝑉*2 *, 𝑉*3 *, 𝑉*4 *, 𝑇 𝑆𝑇𝐴*2 } to *𝑉𝑖* on an open

*𝑖*

database, it makes the entry of the vehicle’s number in the table and

proceeds the registration process. *𝑇 𝐴* computes *𝑅𝑒𝑔𝑛𝑒𝑤* as, *𝑅𝑒𝑔𝑛𝑒𝑤* =

public channel.

*𝐼𝐷𝑖*

*𝐼𝐷𝑖*

* **Step 5:** On receiving the authentication reply message from *𝑇 𝐴*, *𝑉*

*𝑝𝑘𝑇 𝐴* ⋅ *𝑅𝐼 𝐷𝑛𝑒𝑤*. *𝑇 𝐴* chooses a temporary identity *𝑇 𝐼𝐷𝑛𝑒𝑤* for vehi-

*𝑖*

cle

*𝑖*

*𝑛𝑒𝑤*

*𝑖*

*𝑛𝑒𝑤*

checks the freshness of the message by checking the time delay us-

ing the condition: |*𝑇 𝑆* ∗ − *𝑇 𝑆* | ≤ Δ*𝑇 𝑆*. Then, *𝑉* calculates *𝑉* ∗ =

*𝑉𝑖* , and computes pseudo temporary identity by *𝑅𝑇 𝐼𝐷𝑖* =

*ℎ*(*𝑇 𝐼𝐷𝑛𝑒𝑤* ‖*𝑝𝑘𝑇 𝐴*).

*𝑇𝐴*2

*𝑇𝐴*2

*𝑖* 1 *𝑖*

*𝑉*2 + *𝑅𝑒𝑔*

. It uses the value of *𝑉* ∗ to compute session key *𝑆𝐾*

* + **Step 3:** Finally, *𝑇 𝐴* generates a current timestamp

*𝐼𝐷𝑖* ∗ 1

*𝑉𝑖* −*𝑇𝐴*

as *𝑇 𝑆*

, and sends the registration reply message

as *𝑆𝐾𝑉* −*𝑇𝐴* = *ℎ*(*𝑅𝑒𝑔𝐼𝐷*

‖*𝑉*1 ‖(*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴*)). To ensure the integrity

*𝑇𝐴*1

{

*𝑖 𝑖*

∗ ∗ *𝑇 𝐼𝐷𝑛𝑒𝑤, 𝑅𝑒𝑔𝑛𝑒𝑤, 𝑅𝑇 𝐼𝐷𝑛𝑒𝑤, 𝑇 𝑆𝑇𝐴* } to *𝑉𝑖* on a secure channel.

of the calculated session key, *𝑉𝑖* calculates *𝑄𝑖* = *ℎ*(*𝑅𝐼 𝐷𝑖* ‖*𝑆𝐾𝑉𝑖* −*𝑇𝐴*

*𝑖 𝐼𝐷𝑖 𝑖* 1

‖*𝑉* ∗) and checks if *𝑄*∗ = *𝑄𝑖* ?

* + **Step 4:** After receiving registration reply message

1 *𝑖* ∗

{*𝑇 𝐼𝐷𝑛𝑒𝑤, 𝑅𝑒𝑔𝑛𝑒𝑤, 𝑅𝑇 𝐼𝐷𝑛𝑒𝑤, 𝑇 𝑆*

} from *𝑇 𝐴*, *𝑂𝐵𝑈 𝑛𝑒𝑤*

of *𝑉 𝑛𝑒𝑤*

* **Step 6:** If the equation *𝑄𝑖* = *𝑄𝑖* is valid, *𝑉𝑖* extracts the cre-

*𝑖 𝐼𝐷𝑖*

*𝑖 𝑇𝐴*1

*𝑖 𝑖*

dentials by, *𝑅𝑇 𝐼𝐷𝑛𝑒𝑤* = *𝑉*3 *⊕ 𝑆𝐾𝑉* −*𝑇𝐴*, *𝑇 𝐼𝐷𝑛𝑒𝑤* = *𝑉*4 *⊕ ℎ*(*𝑉* ∗) and

first verifies the received timestamp *𝑇 𝑆𝑇𝐴*1 against the current

*𝑛𝑒𝑤*

*𝑖*

*𝑛𝑒𝑤*

*𝑖 𝑖* 1

timestamp by the condition: |*𝑇 𝑆* ∗

– *𝑇 𝑆*

| ≤ Δ*𝑇 𝑆*. If the times-

*𝑉 𝐷𝑖* = *𝑅𝑇 𝐼 𝐷𝑖 ⊕ ℎ*(*𝐼 𝐷𝑖* ‖*𝑃 𝑊𝑖* ‖*𝑟𝑖* ). Subsequently, after success-

*𝑇𝐴*1

*𝑇𝐴*1

ful authentication and session key establishment, *𝑂𝐵𝑈𝑖* of vehicle tamp is valid, *𝑂𝐵𝑈 𝑛𝑒𝑤* requests the user of *𝑉 𝑛𝑒𝑤* to choose and

*𝑖 𝑖*

*𝑉𝑖* replaces {*𝑇 𝐼𝐷𝑖 , 𝑉 𝐷𝑖* } with {*𝑇 𝐼𝐷𝑛𝑒𝑤, 𝑉 𝐷𝑛𝑒𝑤*} for availing further

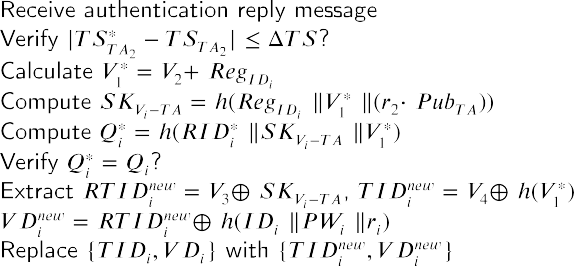
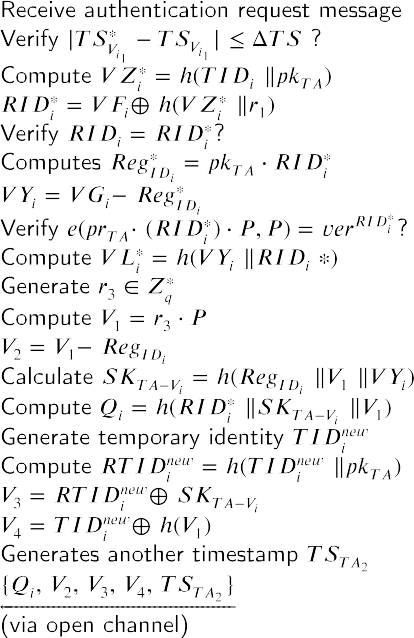
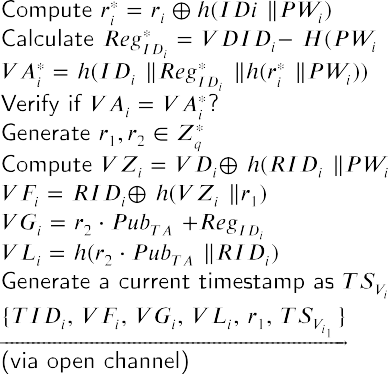
enter a password *𝑃 𝑊 𝑛𝑒𝑤* associated with *𝑉 𝑛𝑒𝑤*. *𝑂𝐵𝑈 𝑛𝑒𝑤* gener-

*𝑖 𝑖 𝑖 𝑖 𝑖*

services.

ates a random nonce *𝑟𝑛𝑒𝑤* ∈ *𝑍* ∗, and computes *𝑉 𝐷𝐼𝐷𝑛𝑒𝑤*, *𝑉 𝐷𝑛𝑒𝑤*,

*𝑖 𝑞 𝑖 𝑖*



**Fig. 3.** Authentication and key establishment phase

*𝑉 𝐴𝑛𝑒𝑤*, *𝑉 𝐵𝑛𝑒𝑤* as, *𝑉 𝐷𝐼𝐷𝑛𝑒𝑤* = *𝑅𝑒𝑔𝑛𝑒𝑤*+ *𝐻* (*𝑃 𝑊 𝑛𝑒𝑤* ‖*𝑟𝑛𝑒𝑤*), *𝑉 𝐷𝑛𝑒𝑤* =

change or update the password. Following steps are executed by the

*𝑖 𝑖*

*𝑖 𝐼𝐷𝑖*

*𝑖 𝑖 𝑖*

*𝑅𝑇 𝐼 𝐷𝑛𝑒𝑤⊕ ℎ*(*𝐼 𝐷𝑛𝑒𝑤*

‖*𝑃 𝑊 𝑛𝑒𝑤*

‖*𝑟𝑛𝑒𝑤*), *𝑉 𝐴𝑛𝑒𝑤* = *ℎ*(*𝐼𝐷𝑛𝑒𝑤*

‖*𝑅𝑒𝑔𝑛𝑒𝑤*

*𝑂𝐵𝑈𝑖* of the vehicle to update the password.

*𝑖 𝑖*

*𝑖 𝑖 𝑖*

*𝑖 𝐼𝐷𝑖*

‖*ℎ*(*𝑟𝑛𝑒𝑤* ‖*𝑃 𝑊 𝑛𝑒𝑤*)), *𝑉 𝐵𝑛𝑒𝑤* = *ℎ*(*𝐼𝐷𝑛𝑒𝑤* ‖*𝑟𝑛𝑒𝑤* ‖*𝑃 𝑊 𝑛𝑒𝑤*) *⊕𝑅𝐼𝐷𝑛𝑒𝑤*.

*𝑖 𝑖 𝑖*

*𝑖 𝑖 𝑖 𝑖*

* + **Step 1:** Vehicle *𝑉𝑖* enters its identity *𝐼𝐷𝑖* and old password *𝑃 𝑊𝑖* .
* **Step 5:** *𝑂𝐵𝑈 𝑛𝑒𝑤* of vehicle *𝑉 𝑛𝑒𝑤* stores {*𝑇 𝐼 𝐷𝑛𝑒𝑤*, *𝑉 𝐷𝐼 𝐷𝑛𝑒𝑤*, *𝑉 𝐷𝑛𝑒𝑤*,

*𝑖 𝑖*

*𝑛𝑒𝑤*

*𝑖 𝑖 𝑖*

Now, the *𝑂𝐵𝑈𝑖* , executes the **Step 1** of log in phase (described in

*𝑉 𝐴𝑖* , *𝑉 𝐵𝑛𝑒𝑤*} in its memory, and deletes {*𝑅𝑒𝑔𝑛𝑒𝑤*, *𝑅𝑇 𝐼𝐷𝑛𝑒𝑤*} per-

[Section 4.3](#_bookmark14)) to check the authenticity of the vehicle.

*𝑖*

manently from its memory.

*𝐼𝐷𝑖 𝑖*

* + **Step 2:** A valid vehicle enters the new password *𝑃 𝑊 𝑛𝑒𝑤*. Then,

For better understanding, [Figure 4](#_bookmark19) shows the complete phases of ex-

*𝑖*

*𝑂𝐵𝑈𝑖* computes *𝑉 𝑍𝑖* = *𝑉 𝐷𝑖⊕ ℎ*(*𝑅𝐼 𝐷𝑖* ‖*𝑃 𝑊𝑖* ‖*𝑟*∗), *𝑅𝑒𝑔𝐼𝐷* = *𝑉 𝐷𝐼𝐷𝑖* −

ecution of our scheme.

*𝐻* (*𝑃 𝑊𝑖* ‖*𝑟*∗).

*𝑖 𝑖*

* 1. *Password change phase*

*𝑖*

* + - **Step 3:** Using the new password *𝑃 𝑊 𝑛𝑒𝑤*, *𝑂𝐵𝑈𝑖* calculates

*𝑉 𝐷𝐼𝐷𝑛𝑒𝑤* = *𝑅𝑒𝑔𝐼𝐷* + *𝐻* (*𝑃 𝑊 𝑛𝑒𝑤* ‖*𝑟*∗), *𝑉 𝐷𝑛𝑒𝑤* = *𝑉 𝑍𝑖⊕ ℎ*(*𝐼𝐷𝑖* ‖*𝑃 𝑊𝑖*

*𝑖*

*𝑖 𝑖 𝑖 𝑖 𝑖*

‖*𝑟*∗), *𝑉 𝐴𝑛𝑒𝑤* = *ℎ*(*𝐼𝐷𝑖* ‖*𝑅𝑒𝑔𝐼𝐷* ‖*ℎ*(*𝑟*∗ ‖*𝑃 𝑊 𝑛𝑒𝑤*)), *𝑉 𝐵𝑖* = *ℎ*(*𝐼𝐷𝑖* ‖*𝑟*∗

*𝑖 𝑖 𝑖 𝑖 𝑖 𝑖*

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

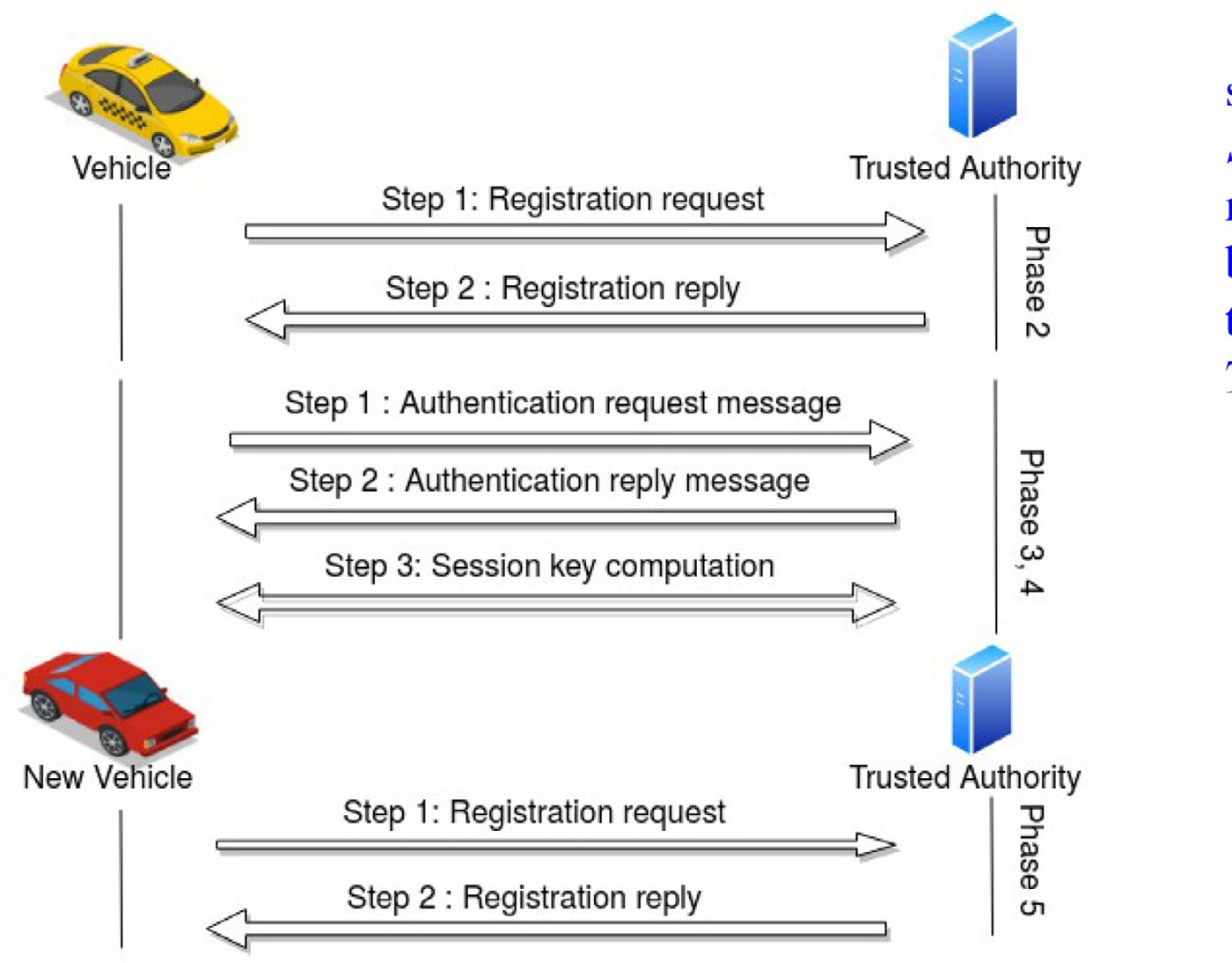
‖*𝑃 𝑊 𝑛𝑒𝑤*) *⊕𝑅𝐼𝐷𝑖* .

* + - **Step 4:** *𝑂𝐵𝑈𝑖* of vehicle *𝑉𝑖* replaces the old {*𝑉 𝐷𝐼𝐷𝑖* , *𝑉 𝐷𝑖* , *𝑉 𝐴𝑖* , *𝑉 𝐵𝑖* }

*𝑖*

with new values {*𝑉 𝐷𝐼𝐷𝑛𝑒𝑤*, *𝑉 𝐷𝑛𝑒𝑤*, *𝑉 𝐴𝑛𝑒𝑤*, *𝑉 𝐵𝑛𝑒𝑤*}.

*𝑖 𝑖 𝑖 𝑖*

**Fig. 4.** Overview of the proposed access control scheme

# The extended scheme

In this section, we provide an extended scheme from the basic scheme discussed in [Section 4](#_bookmark11) for an IoV application.

the *𝑇 𝐴* fetches the already established session keys *𝑆𝐾𝑇𝐴,𝑉𝑖* and

*𝑆𝐾𝑇𝐴*−*𝐶𝐻* corresponding to *𝑇 𝐼𝐷𝑖* and *𝑇 𝐼𝐷𝐶𝐻* respectively, and generates a current timestamp *𝑇 𝑆𝑇𝐴* and a random secret *𝑟𝑇𝐴* ∈

*𝑍* ∗. The *𝑇 𝐴* computes a shared session key *𝑆𝐾𝑉 ,𝐶𝐻* between *𝑉𝑖*

*𝑞 𝑖*

In IoV environment, we consider a dynamic clustering mechanism for the vehicles proposed by [[29]](#_bookmark61) and [[22]](#_bookmark53) to creating different clus-

ters of vehicles on the fly. The dynamic clustering can be considered as

and *𝐶𝐻* as *𝑆𝐾𝑉 ,𝐶𝐻* = *ℎ*(*𝑟𝑇𝐴* ||*𝑟𝐶𝐻* ||*𝑇 𝑆𝑖* ||*𝑇 𝑆𝐶𝐻* ||*𝑇 𝐼𝐷𝑖* ||*𝑇 𝐼𝐷𝐶𝐻*

||*𝑆 𝐾𝑇𝐴,𝑉𝑖* ||*𝑆 𝐾𝑇𝐴,𝐶𝐻* ). The *𝑇 𝐴* also generates new temporary iden-

*𝑖*

tities *𝑇 𝐼𝐷𝑛𝑒𝑤* and *𝑇 𝐼𝐷𝑛𝑒𝑤* to compute *𝑇 𝐼 𝐷*∗ = *𝑇 𝐼 𝐷𝑛𝑒𝑤 ⊕ℎ*(*𝑇 𝑆𝑇𝐴*

*𝑖 𝐶𝐻 𝑖 𝑖*

follows. The vehicles moving on a same lane segment that ends at the

||*𝑆 𝐾𝑇𝐴,𝑉*

||*𝑆 𝐾𝑉 ,𝐶𝐻* ) and *𝑇 𝐼𝐷*∗ = *𝑇 𝐼𝐷𝑛𝑒𝑤 ⊕ℎ*(*𝑇 𝑆𝑇𝐴* ||*𝑆𝐾𝑇𝐴,𝐶𝐻*

*𝑖 𝑖*

*𝐶𝐻*

*𝐶𝐻*

intersection with the other lane are included in a cluster. Thus, a vehicle

||*𝑆𝐾𝑉 ,𝐶𝐻* ). Once these parameters are calculated, the *𝑇 𝐴* sends

needs to find its neighboring vehicles moving on the same lane segment

*𝑖*

the messages

*𝑀𝑠𝑔*3

= {*𝑇 𝐼𝐷*∗*, 𝑇 𝑆*

*𝑇𝐴, 𝐸*

*𝑆𝐾𝑇𝐴,𝑉*

(*𝑆𝐾𝑉 ,𝐶𝐻*

*, 𝑇 𝑆*

*𝑇𝐴*)} and

towards the same direction almost with the same speed. In this way, a

*𝑀 𝑠𝑔*

= {*𝑇 𝐼 𝐷*∗

*, 𝑇 𝑆*

*, 𝐸*

*𝑖*

(*𝑆𝐾*

*𝑖*

*𝑖*

)} to *𝑉* and *𝐶𝐻*,

4 *𝐶𝐻*

*𝑇𝐴*

*𝑆𝐾𝑇𝐴,𝐶𝐻*

*𝑉𝑖 ,𝐶𝐻 , 𝑇 𝑆𝑇𝐴 𝑖*

cluster head (*𝐶𝐻*) will be selected among the members in each cluster. dynamic cluster will have a group of members as the vehicles. Next, a Now, every vehicle needs to securely communicate with their *𝐶𝐻* in a

respectively, over the public channel.

* **Step 4:** After receiving the message *𝑀𝑠𝑔*3 from the *𝑇 𝐴*, *𝑉𝑖* checks the timeliness of received timestamp *𝑇 𝑆𝑇𝐴* and if it is valid, *𝑉𝑖* decrypts

cluster.

*𝐸𝑆𝐾*

(*𝑆𝐾𝑉 ,𝐶𝐻 , 𝑇 𝑆𝑇𝐴*) using the shared key *𝑆𝐾𝑇𝐴,𝑉*

with the *𝑇 𝐴*

Note that both the cluster head (*𝐶𝐻*) and a vehicle, say *𝑉*

in each

*𝑇𝐴,𝑉𝑖 𝑖* ′ *𝑖* ′

*𝑖* as (*𝑆𝐾𝑉𝑖 ,𝐶𝐻 , 𝑇 𝑆𝑇𝐴*) = *𝐷𝑆𝐾𝑇𝐴,𝑉* [*𝐸𝑆𝐾𝑇𝐴,𝑉* (*𝑆𝐾𝑉𝑖 ,𝐶𝐻 , 𝑇 𝑆𝑇𝐴*)]. If *𝑇 𝑆𝑇𝐴* =

cluster have already established session keys *𝑆𝐾𝑇𝐴,𝐶𝐻* and *𝑆𝐾𝑇𝐴,𝑉* , re-

*𝑖*

*𝑛𝑒𝑤*

∗ *𝑖* ′

spectively, for their secure communication with the *𝑇 𝐴*

*𝑖*

. For establishing

*𝑇 𝑆𝑇𝐴*, *𝑉𝑖* calculates *𝑇 𝐼𝐷𝑖* = *𝑇 𝐼𝐷𝑖 ⊕ℎ*(*𝑇 𝑆𝑇𝐴* ||*𝑆𝐾𝑇𝐴,𝑉𝑖* ||*𝑆𝐾𝑉𝑖 ,𝐶𝐻* ).

Next, *𝑉𝑖* updates *𝑇 𝐼𝐷𝑖* by the calculated *𝑇 𝐼𝐷𝑛𝑒𝑤* in its database and

a session key between the cluster head (*𝐶𝐻*) and its member vehicle *𝑉𝑖* ,

the following steps need to be executed with the help of the *𝑇 𝐴*:

also stores the session key communication.

*𝑖*

*𝑆𝐾𝑉𝑖 ,𝐶𝐻* shared with the *𝐶𝐻* for secret

* + **Step 1:** The initiator vehicle *𝑉𝑖* generates a current timestamp *𝑇 𝑆𝑖*

and sends a session key request message *𝑀𝑠𝑔*1 = {*𝑇 𝐼𝐷𝑖 , 𝑇 𝑆𝑖* } to its cluster head *𝐶𝐻* via a public channel.

* + **Step 5:** After receiving the message *𝑀𝑠𝑔*4 from the *𝑇 𝐴*, *𝐶𝐻*

also checks the timeliness of received timestamp *𝑇 𝑆𝑇𝐴* and

if it is valid, *𝐶𝐻* decrypts *𝐸𝑆𝐾* (*𝑆𝐾𝑉 ,𝐶𝐻 , 𝑇 𝑆𝑇𝐴*) using

*𝑇𝐴,𝐶𝐻 𝑖* ∗

* + **Step 2:** After receiving the message *𝑀𝑠𝑔*1, the *𝐶𝐻* validates the

timeliness of the received timestamp *𝑇 𝑆𝑖* . If it is valid, *𝐶𝐻* gener-

the shared key *𝑆𝐾𝑇𝐴,𝐶𝐻* with the *𝑇 𝐴* as (*𝑆𝐾𝑉𝑖 ,𝐶𝐻 , 𝑇 𝑆𝑇𝐴*)

= *𝐷𝑆𝐾* [*𝐸𝑆𝐾* (*𝑆𝐾𝑉 ,𝐶𝐻 , 𝑇 𝑆𝑇𝐴*)]. If *𝑇 𝑆* ∗ = *𝑇 𝑆𝑇𝐴*, *𝐶𝐻*

*𝑇𝐴,𝐶𝐻*

*𝑇𝐴,𝐶𝐻 𝑖*

*𝑇𝐴*

ates a current timestamp *𝑇 𝑆𝐶𝐻* and a random secret *𝑟𝐶𝐻* ∈ *𝑍* ∗, and

proceeds to compute *𝑇 𝐼𝐷𝑛𝑒𝑤* = *𝑇 𝐼𝐷*∗

*⊕ℎ*(*𝑇 𝑆* ∗

||*𝑆𝐾𝑇𝐴,𝐶𝐻*

*𝑞 𝐶𝐻*

*𝐶𝐻*

*𝑇𝐴*

encrypts (*𝑇 𝐼𝐷𝑖, 𝑇 𝐼𝐷𝐶𝐻 , 𝑇 𝑆𝑖 , 𝑟𝐶𝐻 , 𝑇 𝑆𝐶𝐻* ) using the shared session ||*𝑆𝐾𝑉 ,𝐶𝐻* ). Finally, *𝐶𝐻* updates *𝑇 𝐼𝐷𝐶𝐻* by the calculated *𝑇 𝐼𝐷𝑛𝑒𝑤*

*𝑖 𝐶𝐻*

key *𝑆𝐾𝑇𝐴𝐶𝐻* with the *𝑇 𝐴*. After that *𝐶𝐻* sends a request message

*𝑀𝑠𝑔*2 = {*𝑇 𝑆𝐶𝐻 , 𝐸𝑆𝐾𝑇𝐴,𝐶𝐻* (*𝑇 𝐼 𝐷𝑖 , 𝑇 𝐼 𝐷𝐶𝐻 , 𝑇 𝑆𝑖 , 𝑟𝐶𝐻 , 𝑇 𝑆𝐶𝐻* )} to the

*𝑇 𝐴* via public channel, where *𝐸𝐾* (⋅) denotes the symmetric encryp- tion using the shared key *𝐾*.

* + **Step 3:** Once the message *𝑀𝑠𝑔*2 is received by the *𝑇 𝐴*, it checks the timeliness of timestamp *𝑇 𝑆**𝐶𝐻* . If it is valid, the *𝑇 𝐴* de-

in its database and also stores the session key *𝑆𝐾𝑉𝑖 ,𝐶𝐻* shared with

*𝑉𝑖* for secret communication.

The summary of the extended scheme is briefed in [Figure 5](#_bookmark22).

# Security analysis

crypts *𝐸𝑆𝐾*

(*𝑇 𝐼𝐷𝑖 , 𝑇 𝐼𝐷𝐶𝐻 , 𝑇 𝑆𝑖 , 𝑟𝐶𝐻 , 𝑇 𝑆𝐶𝐻* ) using the shared

key *𝑆𝐾*

*𝑇𝐴,𝐶𝐻*

(*𝑇 𝐼𝐷 , 𝑇 𝐼𝐷*

*, 𝑇 𝑆 , 𝑟*

*, 𝑇 𝑆* ′

) = *𝐷*

In this section we analyze the security of proposed scheme. We show

*𝑇𝐴,𝐶𝐻* as

[ *𝑆𝐾*

*𝑖 𝐶𝐻*

*𝑖 𝐶𝐻*

*𝐶𝐻*

*𝑆𝐾𝑇𝐴,𝐶𝐻*

*𝐸*

*𝑇𝐴,𝐶𝐻*

(*𝑇 𝐼𝐷𝑖 , 𝑇 𝐼𝐷𝐶𝐻 , 𝑇 𝑆𝑖 , 𝑟𝐶𝐻 , 𝑇 𝑆𝐶𝐻* )], where *𝐷𝐾* (⋅) denotes

the correctness of bilinear pairing based verification equation used in

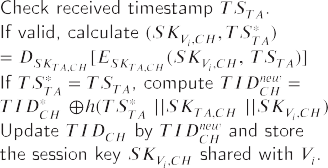
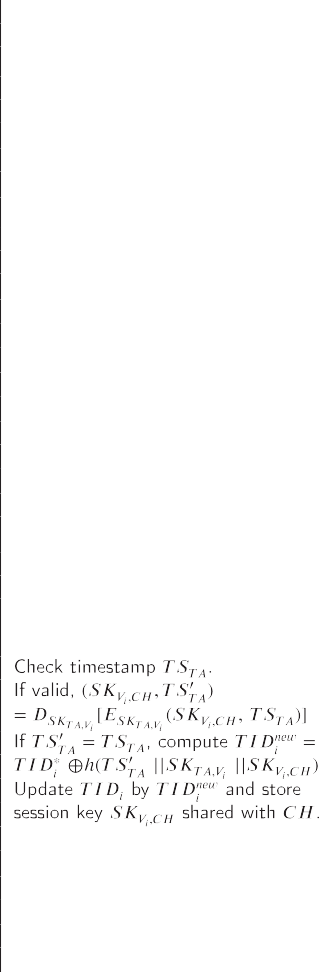
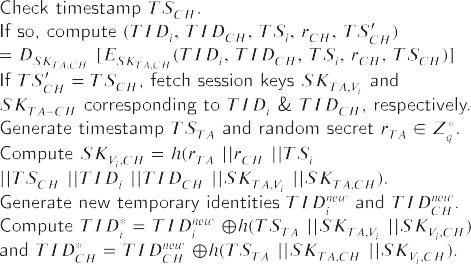
the symmetric decryption using the shared key *𝐾*. Next, the

*𝑇 𝐴* checks the validity of *𝑇 𝑆* ′ = *𝑇 𝑆𝐶𝐻* , and if this is valid,

*𝐶𝐻*

[section 4.4](#_bookmark15) and the correctness of session key computed by vehicle *𝑉𝑖*

and *𝑇 𝐴*. In the next subsection, we present an informal security analysis



**Fig. 5.** Summary of the extended scheme

of the scheme. And later, a formal security analysis using AVISPA is provided in [6.3](#_bookmark28).

* 1. *Correctness proof*

We provide below the correctness proof of our authentication, verifi- cation and key establishment phase that is described in [Section 4.4](#_bookmark15) using the [theorems 1](#_bookmark24) and [2](#_bookmark23).

Since the above equation holds, the message received from *𝑉𝑖* is valid.

Hence, the theorem follows. □

*session key computed by 𝑇 𝐴* ∶ *𝑆𝐾𝑇𝐴*−*𝑉𝑖 , is same as the session key computed* **Theorem 2.** *During the key establishment phase, described in* [*Section 4.4*](#_bookmark15)*, by vehicle 𝑉𝑖* ∶ *𝑆𝐾𝑉𝑖* −*𝑇𝐴.*

**Proof.** The session key computed by *𝑇 𝐴* after successful authentication is *𝑆𝐾𝑇𝐴*−*𝑉𝑖* = *ℎ*(*𝑅𝑒𝑔𝐼𝐷𝑖* ‖*𝑉*1 ‖*𝑉 𝑌𝑖* ). And the session key computed by *𝑉𝑖*

after receiving authentication reply message is *𝑆𝐾𝑉* −*𝑇𝐴* = *ℎ*(*𝑅𝑒𝑔𝐼𝐷* ‖*𝑉* ∗

**Theorem 1.** *During the authentication phase described in*

[*Section 4.4*](#_bookmark15)*, a vehicle 𝑉𝑖 sends authentication request message*

‖(*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴*)).

*𝑖 𝑖* 1

{*𝑇 𝐼𝐷𝑖 , 𝑉 𝐹𝑖 , 𝑉 𝐺𝑖 , 𝑉 𝐿𝑖 , 𝑟*1 *, 𝑇 𝑆𝑉*

*𝑖*1

} *to 𝑇 𝐴. Authentication and verifica-*

Now, we have,

*tion is successful, if and only if the received message is valid.*

**Proof.** *𝑇 𝐴* receives the authentication request message

{*𝑇 𝐼𝐷𝑖 , 𝑉 𝐹𝑖 , 𝑉 𝐺𝑖 , 𝑉 𝐿𝑖 , 𝑟*1 *, 𝑇 𝑆𝑉𝑖*1 } from vehicle *𝑉𝑖* . Vehicle *𝑉𝑖* is au-

thenticated if the following equation holds:

*𝑆𝐾𝑇𝐴*−*𝑉𝑖* = *ℎ*(*𝑅𝑒𝑔𝐼𝐷𝑖* ‖*𝑉*1 ‖*𝑉 𝑌𝑖* )

= *ℎ*(*𝑅𝑒𝑔𝐼𝐷𝑖* ‖*𝑉*1 ‖(*𝑉 𝐺𝑖* − *𝑅𝑒𝑔𝐼𝐷𝑖* ))

= *ℎ*(*𝑅𝑒𝑔𝐼𝐷𝑖* ‖*𝑉*1 ‖(*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴*

+*𝑅𝑒𝑔𝐼𝐷* − *𝑅𝑒𝑔𝐼𝐷* ))

∗ *𝑅𝐼 𝐷*∗

*𝑖 𝑖*

*𝑒*(*𝑝𝑟𝑇 𝐴* ⋅ (*𝑅𝐼 𝐷𝑖* ) ⋅ *𝑃 , 𝑃* ) = *𝑣𝑒𝑟 𝑖*

Now,

= *ℎ*(*𝑅𝑒𝑔𝐼𝐷𝑖* ‖*𝑉*1 ‖*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴*)*.*

*𝑣𝑒𝑟 𝑖* = *𝑒*(*𝑃 𝑢𝑏𝑇𝐴, 𝑃* )

*𝑅𝐼 𝐷*∗

*𝑅𝐼 𝐷*∗

*𝑅𝐼 𝐷*∗

*𝑖*

*𝑆𝐾𝑉* −*𝑇𝐴* = *ℎ*(*𝑅𝑒𝑔𝐼𝐷* ‖*𝑉* ∗‖(*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴*))

= *𝑒*(*𝑝𝑟𝑇 𝐴* ⋅ *𝑃 , 𝑃* )

= *𝑒*(*𝑝𝑟𝑇 𝐴* ⋅ *𝑃 , 𝑃* )

*𝑖*

*𝑅𝐼 𝐷*∗ ⋅1

*𝑖*

= *ℎ*(*𝑅𝑒𝑔𝐼𝐷𝑖* ‖(*𝑉*2 + *𝑅𝑒𝑔𝐼𝐷𝑖* )‖(*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴*))

= *ℎ*(*𝑅𝑒𝑔𝐼𝐷𝑖* ‖(*𝑉*1 − *𝑅𝑒𝑔𝐼𝐷𝑖* + *𝑅𝑒𝑔𝐼𝐷𝑖* )

*𝑖 𝑖* 1

= *𝑒*(*𝑝𝑟𝑇 𝐴* ⋅ *𝑃* ⋅ *𝑅𝐼 𝐷*∗*, 𝑃* ⋅ 1)

*𝑖*

= *𝑒*(*𝑝𝑟𝑇 𝐴* ⋅ (*𝑅𝐼 𝐷*∗) ⋅ *𝑃 , 𝑃* )*.*

*𝑖*

‖(*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴*))

= *ℎ*(*𝑅𝑒𝑔𝐼𝐷𝑖* ‖*𝑉*1 ‖*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴*)*.*

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

‖*𝑅𝐼 𝐷𝑖* ). For this the adversary can assume *𝑟*1 *, 𝑟*2 but the adversary can-

not know *𝑟*∗, *𝑅𝐼 𝐷𝑖* , *𝑅𝑒𝑔𝐼𝐷* because the value of *𝑟*∗, *𝑅𝐼 𝐷𝑖* , *𝑅𝑒𝑔𝐼𝐷* de-

*𝑖 𝑖 𝑖 𝑖*

* 1. *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 au- thentication and session key establishment. The first message is a regis-

tration reply message {*𝑇 𝐼𝐷𝑖 , 𝑅𝑒𝑔𝐼𝐷 , 𝑅𝑇 𝐼𝐷𝑖 , 𝑇 𝑆𝑇𝐴* } which is sent from

pends on the long term secrets like *𝐼𝐷𝑖* , *𝑃 𝑊𝑖* . Therefore an adversary

cannot impersonate vehicle *𝑉𝑖* 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](#_bookmark10), *𝑉𝑖* sends its pseudo identity *𝑅𝐼 𝐷𝑖* to *𝑇 𝐴* via public channel to get *𝑅𝑒𝑔𝐼𝐷𝑖* , *𝑅𝑇 𝐼𝐷𝑖* , and temporary identity *𝑇 𝐼𝐷𝑖* . To perform insider attack, any privileged user of *𝑇 𝐴* being an attacker gets to know the registration details *𝑅𝐼 𝐷𝑖* . However, even if the attacker gets exposed to *𝑅𝐼 𝐷𝑖* , he/she still does

not get to know anything about the real identity of the vehicle. Hence,

*𝑖* 1

*𝑇 𝐴* to *𝑉𝑖* . The second is during log in phase, where a vehicle sends an

authentication request message {*𝑇 𝐼𝐷𝑖 , 𝑉 𝐹𝑖 , 𝑉 𝐺𝑖 , 𝑉 𝐿𝑖 , 𝑟*1 *, 𝑇 𝑆𝑉𝑖*1 } to TA and third is an authentication reply message as {*𝑄𝑖, 𝑉*2 *, 𝑉*3 *, 𝑉*4 *, 𝑇 𝑆𝑇𝐴*2 } sent to *𝑉𝑖* from *𝑇 𝐴*. All the messages include the current timestamp

*𝑇 𝑆𝑇𝐴*1 *, 𝑇 𝑆𝑉𝑖*1 *, 𝑇 𝑆𝑇𝐴*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 re-

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,

*𝑇 𝐴* computes a session key as *𝑆𝐾𝑇𝐴*−*𝑉𝑖* as *𝑆𝐾𝑇𝐴*−*𝑉𝑖* = *ℎ*(*𝑅𝑒𝑔𝐼𝐷𝑖* ‖*𝑉*1 ‖*𝑉 𝑌𝑖* )

and the vehicle computes a session key as *𝑆𝐾𝑉* −*𝑇𝐴* = *ℎ*(*𝑅𝑒𝑔𝐼𝐷* ‖*𝑉* ∗ ‖(*𝑟*2 ⋅

ceived timestamp and the current timestamp. To avoid replay attacks,

*𝑃 𝑢𝑏*

)). Both *𝑆𝐾*

and *𝑆𝐾*

*𝑖*

*𝑅𝑒𝑔*

*𝑖* 1

*𝑇𝐴*

*𝑇𝐴*−*𝑉𝑖*

*𝑉𝑖* −*𝑇𝐴* depends on

*𝐼𝐷𝑖* which is com-

we have considered a very small value Δ*𝑇 𝑆* as the difference in times-

tamp 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](#_bookmark10),

*𝑂𝐵𝑈𝑖* stores the credentials {*𝑇 𝐼 𝐷𝑖* , *𝑉 𝐷𝐼 𝐷𝑖* , *𝑉 𝐷𝑖* , *𝑉 𝐴𝑖* , *𝑉 𝐵𝑖* } in its mem- ory, and deletes {*𝑅𝑒𝑔𝐼𝐷* , *𝑅𝑇 𝐼𝐷𝑖* } permanently from its memory. So if the adversary has physically stolen *𝑂𝐵𝑈𝑖* of vehicle *𝑉𝑖* , he/she can extract all the credentials from *𝑂𝐵𝑈𝑖* using power analysis attack. As

*𝑖*

seen in the registration phase, *𝑉 𝐷𝐼𝐷𝑖* = *𝑅𝑒𝑔𝐼𝐷* + *𝐻* (*𝑃 𝑊𝑖* ‖*𝑟𝑖* ), *𝑉 𝐷𝑖* =

puted using long term secrets which are private key *𝑝𝑟𝑇 𝐴* of *𝑇 𝐴* and identity of the vehicle *𝐼𝐷𝑖* . 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]](#_bookmark44) as discussed in the threat model, still he would need to

know the long term secrets *𝐼𝐷𝑖* , *𝑃 𝑊𝑖* to acquire the session key. □

**Proposition 7.** *Proposed access control scheme is secured against mas- querading attack.*

**Proof.** During authentication, verification and key establishment phase,

*𝑅𝑇 𝐼 𝐷 ⊕ ℎ*(*𝐼 𝐷*

‖*𝑃 𝑊*

*𝑖*

‖*𝑟* ), *𝑉 𝐴* = *ℎ*(*𝐼𝐷* ‖*𝑅𝑒𝑔*

‖*ℎ*(*𝑟*

‖*𝑃 𝑊* )), *𝑉 𝐵* =

*𝑇 𝐴* sends a message {*𝑄𝑖, 𝑉*2 *, 𝑉*3 *, 𝑉*4 *, 𝑇 𝑆𝑇𝐴*2 } as authentication reply mes-

*𝑖 𝑖*

*𝑖 𝑖 𝑖*

*𝑖 𝐼𝐷𝑖 𝑖 𝑖 𝑖*

sage to vehicle *𝑉𝑖* . If an attacker A tries to launch a masquerade attack

*ℎ*(*𝐼𝐷𝑖* ‖*𝑟𝑖* ‖*𝑃 𝑊𝑖* ) *⊕𝑅𝐼𝐷𝑖* . However, to retrieve secrets like *𝑅𝑒𝑔𝐼𝐷* , *𝑅𝑇 𝐷𝑖*

the adversary needs to know *𝑟𝑖* , *𝐼𝐷𝑖* , *𝑃 𝑊𝑖* . Therefore it can clearly be

*𝑖*

concluded that the adversary cannot know any secret credentials by

*𝑂𝐵𝑈𝑖* physical capture attack. □

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

message {*𝑇 𝐼𝐷𝑖 , 𝑉 𝐹𝑖 , 𝑉 𝐺𝑖 , 𝑉 𝐿𝑖 , 𝑟*1 *, 𝑇 𝑆𝑉𝑖*1 } and tries to create another **Proof.** Assume that an adversary intercepts the authentication request

needs to calculate parameters like *𝑄𝑖 , 𝑉*2 etc. All the parameters in the he/she would try to forge the valid authentication reply. For that he reply message depends on secret values *𝐼𝐷𝑖* , *𝑝𝑘𝑇 𝐴*. Moreover the session key is also depended on secret *𝑅𝑒𝑔𝐼𝐷𝑖* . 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.*

authentication request message as {*𝑇 𝐼𝐷𝑎, 𝑉 𝐹 𝑎, 𝑉 𝐺𝑎, 𝑉 𝐿𝑎, 𝑟𝑎, 𝑇 𝑆 𝑎* }.

*𝑖 𝑖*

*𝑖 𝑖* 1

*𝑉𝑖*1

**Proof.** Let us assume that an attacker A traps the authentication request

To create request message, the adversary has to perform computations

like *𝑉 𝑍𝑖* = *𝑉 𝐷𝑖⊕ ℎ*(*𝑅𝐼 𝐷𝑖* ‖*𝑃 𝑊𝑖* ‖*𝑟*∗), *𝑉 𝐹𝑖* = *𝑅𝐼 𝐷𝑖⊕ ℎ*(*𝑉 𝑍𝑖* ‖*𝑟*1 ), *𝑉 𝐺𝑖* =

message {*𝑇 𝐼𝐷𝑖 , 𝑉 𝐹𝑖 , 𝑉 𝐺𝑖 , 𝑉 𝐿𝑖 , 𝑟*1 *, 𝑇 𝑆𝑉𝑖*1 }. Now if A wants to identify

*𝐼𝐷* , he needs to compute it having known *𝑉 𝑍* . A cannot guess identity

*𝑖 𝑖 𝑖*

*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴* +*𝑅𝑒𝑔𝐼𝐷𝑖* , *𝑉 𝐿𝑖* = *ℎ*(*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴* ‖*𝑅𝐼 𝐷𝑖* ). For this the adversary

can generate two random nonces *𝑟*1 *, 𝑟*2 . For computing *𝑉 𝑍𝑖* he needs to know *𝑉 𝐷𝑖* , *𝑅𝐼 𝐷𝑖* , *𝑃 𝑊𝑖* and *𝑟*∗. Let us also assume that he can extract

*𝑖*

*𝑉 𝐷𝑖* from the memory of *𝑂𝐵𝑈𝑖* as explained in [2](#_bookmark25), but he still cannot

using *𝑉 𝐹𝑖* and *𝑉 𝐿𝑖* as there are two low entropy parameters *< 𝐼𝐷𝑖 , 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 {*𝑄𝑖, 𝑉*2 *, 𝑉*3 *, 𝑉*4 *, 𝑇 𝑆𝑇𝐴*2 }.

know *𝑅𝐼 𝐷𝑖* , *𝑟*∗ as it depends on secret *𝐼𝐷𝑖* , *𝑟*1 and *𝑃 𝑊𝑖* . Therefore it

1

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 *𝑉𝑖* , and adversary A might try to in- tercept the authentication request message {*𝑇 𝐼𝐷𝑖 , 𝑉 𝐹𝑖 , 𝑉 𝐺𝑖 , 𝑉 𝐿𝑖 , 𝑟*1 *,*

It is also noticeable from [Section 4.4](#_bookmark15) that the value of *𝑄𝑖* is relied on

*𝐼𝐷𝑖* 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](#_bookmark14)), a parameter

*𝑇 𝐼𝐷* is sent in the authentication request message. Then during verifica-

*𝑇 𝑆*

*𝑖*

*𝑉𝑖*1

} and creates another authentication request message as {*𝑇 𝐼𝐷𝑎,*

*𝑖*

tion and key establishment phase (in [Section 4.4](#_bookmark15)) Step 4, *𝑇 𝐴* generates

*𝑉 𝐹 𝑎, 𝑉 𝐺𝑎, 𝑉 𝐿𝑎, 𝑟𝑎, 𝑇 𝑆 𝑎*

}. To create request message, the adversary

a new identity *𝑇 𝐼𝐷𝑛𝑒𝑤* which is sent as parameter *𝑉*

in authentica-

*𝑖 𝑖*

*𝑖* 1

*𝑉𝑖*1

*𝑖* 4

has to perform computations like *𝑉 𝑍𝑖* = *𝑉 𝐷𝑖⊕ ℎ*(*𝑅𝐼 𝐷𝑖* ‖*𝑃 𝑊𝑖* ‖*𝑟*∗),

*𝑖*

*𝑉 𝐹𝑖* = *𝑅𝐼 𝐷𝑖⊕ ℎ*(*𝑉 𝑍𝑖* ‖*𝑟*1 ), *𝑉 𝐺𝑖* = *𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴* +*𝑅𝑒𝑔𝐼𝐷𝑖* , *𝑉 𝐿𝑖* = *ℎ*(*𝑟*2 ⋅ *𝑃 𝑢𝑏𝑇𝐴*

*𝑖*

and updates its old *𝑇 𝐼𝐷𝑖* with *𝑇 𝐼𝐷𝑛𝑒𝑤* after verifying the authenticity. tion reply message to the vehicle. Then in Step 6 the vehicle extracts

Hence in every session the parameter *𝑇 𝐼𝐷𝑖* is changed. Therefore, dy-

namic 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, *𝑇 𝐴* computes a session key as

|  |  |  |
| --- | --- | --- |
| Scheme | Total cost | Estimated time |
|  |  | (in milliseconds) |
| Our scheme | 15*𝑇ℎ* + 5*𝑇𝑒𝑐𝑚* + 5*𝑇𝑒𝑐𝑎* + *𝑇𝑏𝑝* + *𝑇𝑒𝑥𝑝* | ≈ 173*.*61 ms |
| [[17]](#_bookmark50) | 10*𝑇ℎ* + 6*𝑇𝑒𝑥𝑝* | ≈ 118*.*40 ms |
| [[38]](#_bookmark73) | 52*𝑇ℎ* | ≈ 16*.*64 ms |
| [[4]](#_bookmark69) | 4*𝑇ℎ* + 2*𝑇𝑒𝑐𝑚* + 2*𝑇𝑒𝑐𝑎* | ≈ 44*.*28 ms |
| [[2]](#_bookmark65) | 8*𝑇ℎ* + 6*𝑇𝑒𝑐𝑚* + 2*𝑇𝑒𝑛𝑐*∕*𝑑𝑒𝑐* | ≈ 105*.*80 ms |
| [[9]](#_bookmark37) | 10*𝑇ℎ* + 9*𝑇𝑒𝑐𝑚* + 2*𝑇𝑒𝑝𝑎* | ≈ 165*.*90 ms |
| [[42]](#_bookmark70) | 16*𝑇ℎ* | ≈ 5*.*12 ms |

**Table 3**

Comparative computational costs analysis

*𝑆𝐾*

*𝑇𝐴*−*𝑉𝑖*

as *𝑆𝐾*

*𝑇𝐴*−*𝑉𝑖*

= *ℎ*(*𝑅𝑒𝑔*

*𝐼𝐷𝑖*

‖*𝑉*1

‖*𝑉 𝑌𝑖*) and the vehicle computes

∗

a session key as *𝑆𝐾𝑉𝑖* −*𝑇𝐴* = *ℎ*(*𝑅𝑒𝑔𝐼𝐷𝑖* ‖*𝑉*1 ‖(*𝑟*2⋅ *𝑃 𝑢𝑏𝑇𝐴*)). Both *𝑆𝐾𝑇𝐴*−*𝑉𝑖*

and *𝑆𝐾𝑉𝑖* −*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

as he needs to know *𝑟*3, *𝑟*2 to compute the session key. Therefore our session he still cannot compute session key for next and previous sessions

scheme offers perfect backward and forward secrecy. □

* 1. *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]](#_bookmark36). AVISPA has become the common tool that is used to ver- ify 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 “Out- put Format (OF)” which is comprehended in different sections. In the first section called as “SUMMARY” the output displays whether the pro- tocol is “safe, unsafe, or inconclusive”. The second section called as “DE- TAILS” elaborates on the reason on why the protocol is summarized as “safe, unsafe or inconclusive”. The third section is “PROTOCOL” sec- tion that defines the “HLPSL specification of the target protocol in inter- mediate 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.

HLPSL implementation that consists of two basic roles of *𝑇 𝐴*, *𝑉𝑖*, the To analyze the security of our proposed scheme we have coded the

other compulsory roles of *session* and *goal & environment*. We have con- sidered the registration phase discussed in [Section 4.2](#_bookmark10), log in phase dis- cussed in [Section 4.3](#_bookmark14) and authentication, verification and key establish-

ment phase discussed in [Section 4.4](#_bookmark15) where *𝑇 𝐴* authenticates the vehicle

and both *𝑇 𝐴* and vehicle compute a session key.

ting an active role to the intruder (*𝑖*). All the public parameters are AVISPA detects the occurrence of attack while simulation by allot-

fed into the knowledge of the intruder, and the intruder can even im- itate all other roles. According to the “Dolev-Yao (DY) threat model”

[[21]](#_bookmark52) discussed in [Section 2](#_bookmark5), 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]](#_bookmark39) 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](#_bookmark30) which shows the results using OFMC back-end. Thus we can

**Table 4**

Comparative communication costs analysis

|  |  |  |
| --- | --- | --- |
| Scheme | Number of messages | Number of bits |
| Our scheme | 2 | 2112 |
| [[17]](#_bookmark50) | 3 | 2464 |
| [[38]](#_bookmark73) | 5 | 3872 |
| [[4]](#_bookmark69) | 4 | 2560 |
| [[2]](#_bookmark65) | 3 | 896*𝑛* + 1440 |
| [[9]](#_bookmark37) | 3 | 1856 |
| [[42]](#_bookmark70) | 4 | 2624 |

*Note: 𝑛*: number of vehicles in the scheme of [[2]](#_bookmark65)

clearly state that the proposed access control scheme is secured against “replay and man-in-the-middle-attacks”.

# Comparative analysis

The eﬃciency of the scheme can be asserted in terms of computa- tion 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) ex- changed 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.

* 1. *Computation costs comparison*

The cryptographic techniques which are used in the schemes are “el- liptic 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 *𝑇𝑒𝑐𝑚*, *𝑇𝑒𝑝𝑎*, *𝑇𝑏𝑝*, *𝑇𝑒𝑥𝑝*, *𝑇ℎ* and *𝑇𝑒𝑛𝑐*∕*𝑑𝑒𝑐* for each respectively. To

time for each operation. For *𝑇𝑒𝑐𝑚*, *𝑇𝑒𝑐𝑎*, *𝑇𝑏𝑝*, *𝑇𝑒𝑥𝑝*, *𝑇ℎ* and *𝑇𝑒𝑛𝑐*∕*𝑑𝑒𝑐* the exe- generalized and fair comparison we have considered specific estimated

cution time taken is 17.10 ms ([[31]](#_bookmark63)), 4.4 ms ([[14]](#_bookmark46)), 42.11 ms, 19.2 ms

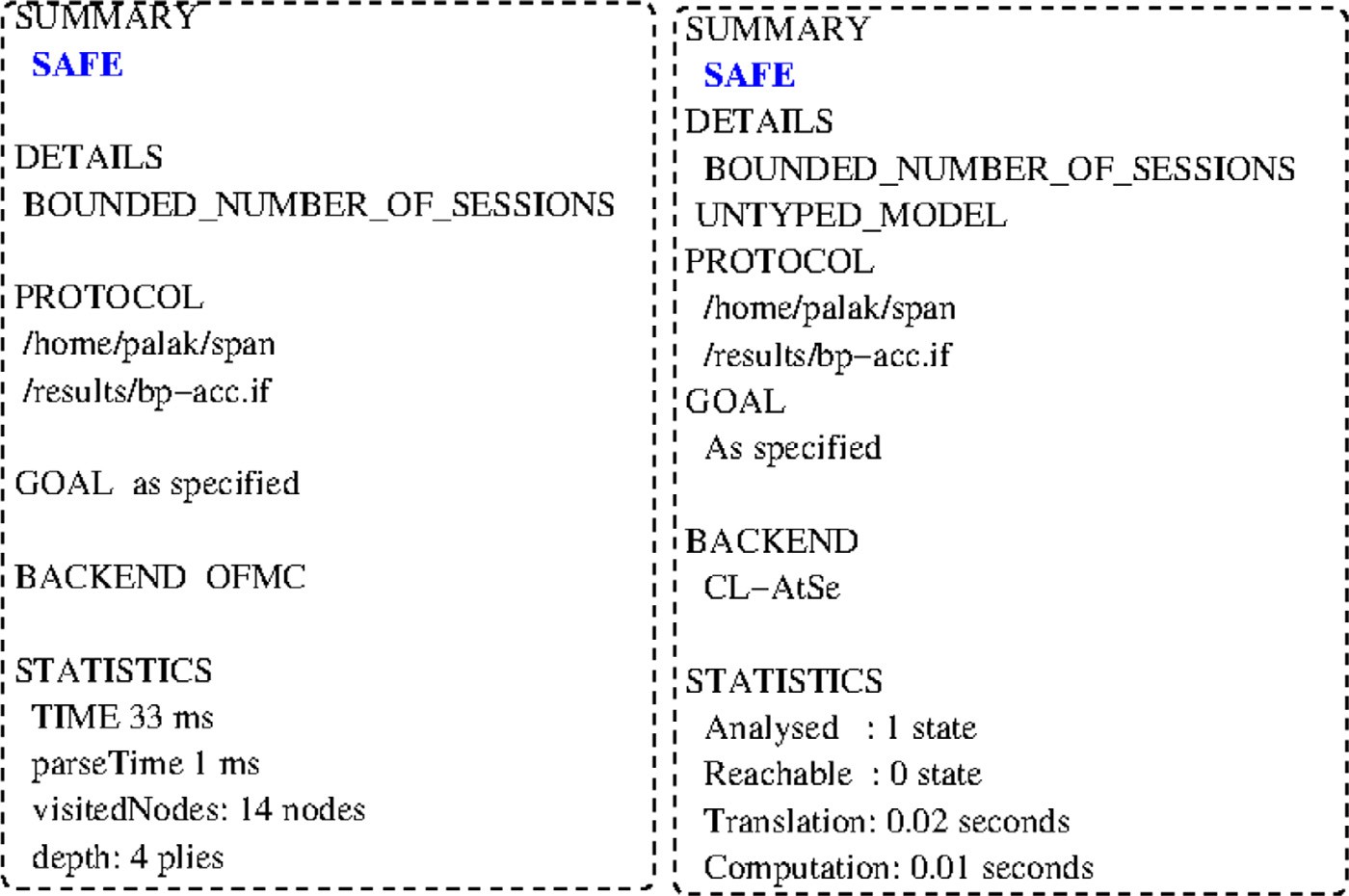
([[31]](#_bookmark63)), 0.32 ms ([[14]](#_bookmark46)) and 0.32 ms, respectively.

The cryptographic operations during login, and authentication, ver- ification and key establishment phases (discussed in [Sections 4.3](#_bookmark14) and [4.4](#_bookmark15)) in our scheme, are “elliptic curve point multiplication, elliptic curve

way hash function”. The total computation cost comes out to be 15*𝑇ℎ*+ point addition, bilinear pairing operation, modular exponentiation, one- 5*𝑇𝑒𝑐𝑚*+ 3*𝑇𝑒𝑐𝑎*+ *𝑇𝑏𝑝*+ *𝑇𝑒𝑥𝑝*. In [Table 3](#_bookmark26), we have compared the computa-

tion costs of our scheme against existing schemes proposed by [[17]](#_bookmark50),

[[38]](#_bookmark73), [[4]](#_bookmark69), [[2]](#_bookmark65), [[42]](#_bookmark70) and [[9]](#_bookmark37). 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]](#_bookmark37). However, it can be justified due to superior security and more functionality at- tributes provided by the proposed scheme as compared to existing com- peting schemes (see [Table 5](#_bookmark31)).



**Table 5**

Comparison of functionality & security features

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Feature | Chen | Sadri and Rajabzadeh | Alladi | Al-Shareeda | Vasudev | Bagga | Our |
|  | et al. | Asaar | et al. | et al. | et al. | et al. |  |
| *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”.
  1. *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 cryp- tographic hash function” is considered as 256 bits. For ECC techniques we have considered 160 bits cryptosystem. Therefore, an elliptic curve

point *𝑃* = (*𝑃𝑥, 𝑃𝑦*) is (160 + 160) = 320 bits, where “*𝑃𝑥* and *𝑃𝑦* are the

*𝑥* and *𝑦* co-ordinates of the point *𝑃* ”. Further, a “vehicle’s real iden-

tity, random nonce and timestamp” are taken as 160, 160 and 32 bits,

respectively. For a “symmetric key encryption/decryption (for exam- ple, if the Advanced Encryption Standard (AES-128) is used), the plain- text/ciphertext block size” will become 128 bits.

The authentication process in our scheme, is accomplished by ex- changing two messages. The first message is authentication request mes-

In [Table 4](#_bookmark27), we have compared the communication costs of our scheme against existing schemes proposed by [[17]](#_bookmark50), [[38]](#_bookmark73), [[4]](#_bookmark69), [[2]](#_bookmark65),

[[42]](#_bookmark70) and [[9]](#_bookmark37). It is noticed that the proposed scheme requires compa- rable communication cost as in [[9]](#_bookmark37). However, the communication cost in the proposed scheme is low as compared to other remaining existing schemes as shown in [Table 4](#_bookmark27).

* 1. *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](#_bookmark31). 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”, im-

sage {*𝑇 𝐼𝐷𝑖, 𝑉 𝐹𝑖, 𝑉 𝐺𝑖, 𝑉 𝐿𝑖, 𝑟*1*, 𝑇 𝑆𝑉*

*𝑖*1

} from *𝑉𝑖* to *𝑇 𝐴*. This message takes

personation attack”, “formal security verification using AVISPA tool,

“dynamic vehicle addition phase, “ password update phase”. And it can

a total of 160 + 256 + 320 + 160 + 32 = 928 bits. The second message is authentication reply message as {*𝑄𝑖, 𝑉*2*, 𝑉*3*, 𝑉*4*, 𝑇 𝑆𝑇𝐴*2 } to *𝑉𝑖* which takes a total of 256 + 320 + 320 + 256 + 32 = 1184 bits. The total communica-

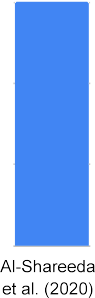
tion overhead of our scheme is 2112 bits.

be clearly seen that our scheme excels in security and functionality fea- tures than other schemes. In [Table 5](#_bookmark31), 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



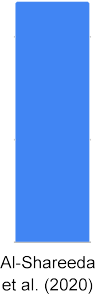
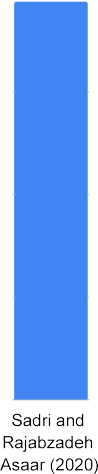
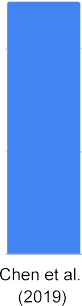
messages (assume *𝑛* = 1 in [[2]](#_bookmark65))







**Fig. 8.** Performance analysis of all schemes for



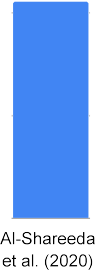
(assume *𝑛* = 1 in [[2]](#_bookmark65)) communication costs in terms of number of bits







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





For overall comparison, we present the computation cost, commu- nication costs in bits and number of messages in [Figures 7](#_bookmark32), [8](#_bookmark33) and [9](#_bookmark34), respectively. It can be seen that schemes like [[38]](#_bookmark73) and [[42]](#_bookmark70) have very low computation costs, but the communication cost is too high. In com- parison 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.

# Conclusion and future work

In this paper, we designed a remote access control mechanism as a

our scheme *𝑇 𝐴* initially authenticates a vehicle before allowing it to be a countermeasure to security issues in smart transportation. According to part of the network. Further the authenticated vehicle and *𝑇 𝐴* compute

tion phase where any new vehicle can easily be registered via *𝑇 𝐴*. Our a session key to communicate securely. We also propose a vehicle addi-

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 com- prehensive 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 ap- plied in many networking environments due to its superior security as compared to the traditional public key cryptosystems as they are quan- tum resistant against various attacks as pointed out by [[15]](#_bookmark47) 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 cu- ration, Writing – original draft. **Ashok Kumar Das:** Conceptualiza- tion, Methodology, Writing – review & editing, Visualization, Supervi- sion, Project administration. **Joel J.P.C. Rodrigues:** Conceptualization, Writing – review & editing, Visualization, Supervision, Funding acqui- sition.

# 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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0001)
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 net- works, IEEE Access 8 (2020) 144957–144968, doi:[10.1109/ACCESS.2020.3014678](https://doi.org/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](https://doi.org/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 Ve- hicular Technology 69 (2020) 14188–14197, doi:[10.1109/TVT.2020.3038834](https://doi.org/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](https://doi.org/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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0008)
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](https://doi.org/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](https://doi.org/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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0011)
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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0012)
13. [R. Canetti, H. Krawczyk, Analysis of key-exchange protocols and their use for build- ing secure channels, in: Advances in Cryptology – EUROCRYPT, Springer Berlin Hei- delberg, Innsbruck (Tyrol), Austria, 2001, pp. 453–474.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0013)
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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0014)
15. [R. Chaudhary, A. Jindal, G.S. Aujla, N. Kumar, A.K. Das, N. Saxena, LSCSH: Lat- tice-based secure cryptosystem for smart healthcare in smart cities environment, IEEE Communications Magazine 56 (2018) 24–32.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0015)
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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0016)
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/AC- CESS.2019.2891105.](https://doi.org/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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0018)
19. [A.K. Das, A random key establishment scheme for multi-phase deployment in large-s- cale distributed sensor networks, International Journal of Information Security 11 (2012) 189–211.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0019)
20. [A.K. Das, B. Bruhadeshwar, An improved and effective secure password-based au- thentication and key agreement scheme using smart cards for the telecare medicine information system, Journal of Medical Systems 37 (2013) 9969.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0020)
21. [D. Dolev, A. Yao, On the security of public key protocols, IEEE Transactions on Information Theory 29 (1983) 198–208.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0021)
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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0022)
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.](https://doi.org/10.1109/\penalty%20-\%40M%20CC.2016.7733050)
24. [L. Gafencu, L. Scripcariu, Security issues in the internet of vehicles, in: 2018 In- ternational Conference on Communications (COMM), Bucharest, Romania, 2018,](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0024)

[pp. 441–446.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0024)

1. [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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0025)
2. [X. Guo, C. Chen, C. Gong, F. Leu, A secure oﬃcial vehicle communication proto- col for VANET, in: 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Fukuoka, Japan, 2016, pp. 482– 485.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0026)
3. [N. Gupta, R. Manaswini, B. Saikrishna, F. Silva, A. Teles, Authentication-based se- cure data dissemination protocol and framework for 5g-enabled VANET, Future In- ternet 12 (2020).](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0027)
4. [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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0028)
5. [M.S. Kakkasageri, S.S. Manvi, Multiagent driven dynamic clustering of vehicles in VANETs, Journal of Network and Computer Applications 35 (2012) 1771– 1780.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0029)
6. [J.B. Kenney, Dedicated short-range communications (DSRC) standards in the united states, Proceedings of the IEEE 99 (2011) 1162–1182.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0030)
7. [C.C. Lee, C.T. Chen, P.H. Wu, T.Y. Chen, Three-factor control protocol based on ellip- tic curve cryptosystem for universal serial bus mass storage devices, IET Computers & Digital Techniques 7 (2013) 48–56.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0031)
8. 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.
9. [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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0033)
10. [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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0034)
11. [J. Liu, Q. Li, R. Sun, X. Du, M. Guizani, An eﬃcient anonymous authentication scheme for internet of vehicles, in: IEEE International Conference on Communica- tions (ICC), Kansas City, MO, USA, 2018, pp. 1–6.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0035)
12. [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–](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0036)

[2749.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0036)

1. A. Menezes, An introduction to pairing-based cryptography, 2013, (????). Accessed on May 2020.
2. 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](https://doi.org/10.1002/dac.4511).
3. [J. Shao, X. Lin, R. Lu, C. Zuo, A threshold anonymous authentication protocol for VANETs, IEEE Transactions on Vehicular Technology 65 (2016) 1711–1720.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0039)
4. S. Sharma, B. Kaushik, A survey on internet of vehicles: Applications, se- curity issues & solutions, Vehicular Communications 20 (2019) 100182, doi:[10.1016/j.vehcom.2019.100182](https://doi.org/10.1016/j.vehcom.2019.100182).
5. 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 Tech- nology 69 (2020) 5535–5548, doi:[10.1109/TVT.2020.2981934](https://doi.org/10.1109/TVT.2020.2981934).
6. [H. Vasudev, V. Deshpande, D. Das, S.K. Das, A lightweight mutual authentication protocol for v2v communication in internet of vehicles, IEEE Transactions on Vehic- ular Technology 69 (2020) 6709–6717.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0042)
7. [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.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0043)
8. [L. Wu, Q. Sun, X. Wang, J. Wang, S. Yu, Y. Zou, B. Liu, Z. Zhu, An eﬃcient privacy-p- reserving mutual authentication scheme for secure v2v communication in vehicular ad hoc network, IEEE Access 7 (2019) 55050–55063.](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0044)
9. B. Ying, A. Nayak, Anonymous and lightweight authentication for secure vehicu- lar networks, IEEE Transactions on Vehicular Technology 66 (2017) 10626–10636, doi:[10.1109/TVT.2017.2744182](https://doi.org/10.1109/TVT.2017.2744182).
10. [S. Yu, J. Lee, K. Lee, K. Park, Y. Park, Secure authentication protocol for wireless sensor networks in vehicular communications, Sensors 18 (2018).](http://refhub.elsevier.com/S2772-9184(22)00001-7/sbref0046)
11. 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](https://doi.org/10.1109/TST.2016.7787005).