Complex & Intelligent Systems (2023) 9:2981–2991
https://doi.org/10.1007/s40747-021-00562-z

ORIGINAL ARTICLE

A novel lightweight authentication and privacy-preserving protocol for vehicular ad hoc networks

Shaji K. A. Theodore[1] · K. Rajiv Gandhi[2] · V. Palanisamy[3]

Received: 22 July 2021 / Accepted: 12 October 2021 / Published online: 30 October 2021

Abstract

Vehicular ad hoc network (VANET) is commonly employed in intelligent transportation system (ITS) that allows the exchange of traffic data among vehicles and nearby environment to accomplish effective driving experience. Privacy and security are the challenging issues that exist in the safety needs of the VANET. Any particular leakage of the vehicle details such as route data might result in serious impacts, and therefore, authentication and privacy-preserving protocols are needed to enhance safety in VANET. With this motivation, this paper presents a new lightweight authentication and privacy-preserving protocol using improved timed efficient stream loss-tolerant authentication with cuckoo filter (ITESLA-CF) for VANETs. The proposed model encompasses different stages of operations such as initialization, registration, mutual authentication, broadcast and verification, and vehicle revocation phases. In addition, the ITESLA-CF technique has effective broadcast authentication as TESLA with minimal memory requirement. Besides, the ITESLA-CF technique includes a cuckoo filter to save the authentic information of vehicles that exist in the RSU's range. The proposed model has lightweight mutual authentication among the parties and it offers robust anonymity to accomplish privacy and resists ordinary attacks. To ensure the better performance of the ITESLA-CF technique, an extensive set of simulations take place and the results are assessed in terms of different measures. The resultant experimental values pointed out the supremacy of the ITESLA-CF technique over the recent state of art methods.

Keywords VANET · Intelligent transportation system · Privacy preserving · Security · Authentication · TESLA · Cuckoo filter

Introduction

Vehicular ad hoc network (VANET) is generated by employing the standards of Mobile Ad hoc Network (MANET). It is depending upon the impulsive nature of a wireless network for transferring data [1]. The communications are assisted through the internet with the help of Road-Side Unit (RSU) [2] and On-Board Unit (OBU) [3]. The characteristics of VANET are higher computation capability, predictable mobility, variable network density, available geographic location, quick altering topology, and mobility [4]. Because of these characteristics, it was broadly used for group communication, safety, traffic flow control, and road-side service finder application. In this network, two kinds of wireless transmission occur that consist of V2I [5], and V2V [6]. The V2V is a type of ad hoc transmission which is mostly utilized for collision and obstacle warnings. In this transmission, the single- and multi-hop packet transmissions are executed between the source and destination. The V2I combines the transmission methods of infrastructure and ad hoc, whereas the road side and vehicle base stations are included. The communications in a public access network might create privacy and security crucial and another problem in the VANET. A mismanaging of this communication may generate loss of human lives and traffic accidents; thus, vehicle

✉ Shaji K. A. Theodore
drtheodore7733@hotmail.com

K. Rajiv Gandhi
dr.krajiv.84@gmail.com

V. Palanisamy
vpazhanisamy@yahoo.co.in

[1] Department of Computer Applications, Alagappa University, Karaikudi, Tamil Nadu 630004, India

[2] Department of Computer Science, Alagappa University Model Constituent College, Paramakudi, Tamil Nadu 623707, India

[3] Department of Computer Applications, Alagappa University, Karaikudi, Tamil Nadu 630003, India

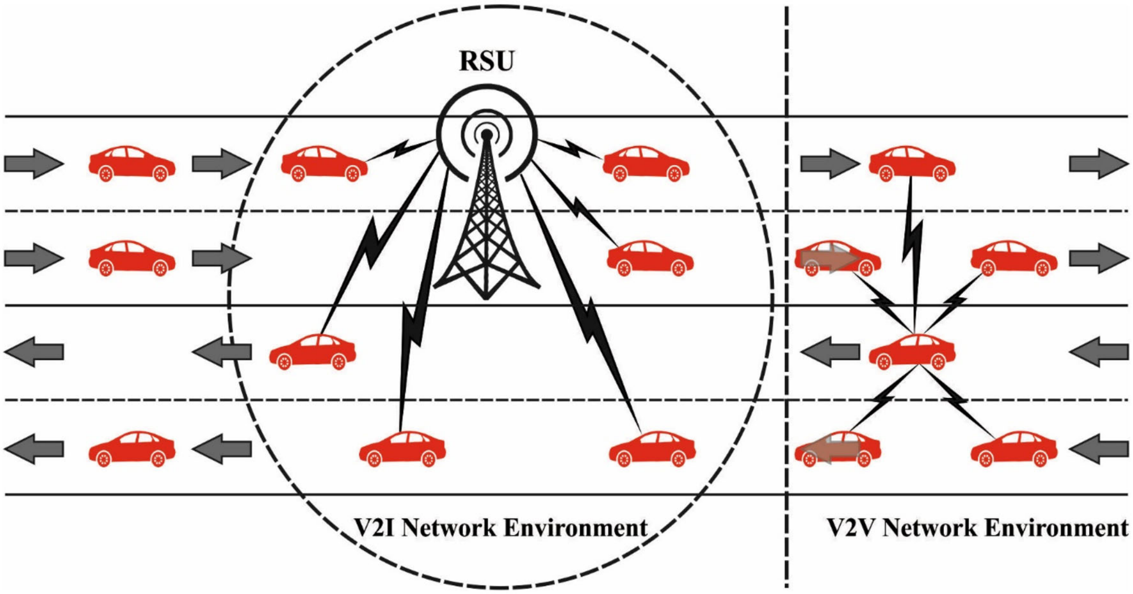


Fig. 1 Overview of VANET

validation is a significant role in this scheme. Thus, the major goal of the designers is to create a VANET highly protected. In validation time, vehicle's privacy correlated data such as private data and data regarding the position should be kept in private. It has Many kinds of validation scheme is available for maintaining the privacy correlated data. Figure 1 showcases the overview of VANET.

Though the benefits of VANETs are significantly increasing, the dynamics of VANET (vehicle could leave and join without restriction) together with a multitude of scheme and application interrelated requirement makes it extremely difficult for designing an effective method to ensure privacy of the vehicle [7]. Simultaneously, guaranteeing privacy of the vehicle (driver) is the most difficult problems where an effective solution should be made or else an adversary can track vehicles traveling routes by analyzing and capturing its message [8] and find the vehicles (drivers) that might contain serious impact for the drivers. To tackle this problem, several scientists have projected procedures where vehicles can utilize pseudonym rather than their real identity in transmission simultaneously allowing authorities for extracting the real identity from pseudonyms to punish and trace mischievous vehicles. This protocol is known as conditional privacy-preserving protocol. Allocating pseudonyms to vehicles and modifying them regularly is another approach utilized for ensuring privacy of the vehicle. For maximizing privacy, vehicles should modify pseudonyms more often though the occurrence of these changes remains uncertain. Features such as storage size and availability play a significant part in defining the rate whereat the pseudonym must be modified. Most of the studies in the survey tackling privacy, security, and authentication utilize TA to obtain and load OBU and RSU by security variables such as pseudonyms, keys, and certificates.

Conventional methods to authenticate and secure message dissemination, mainly depending upon key management and message encryption, could assure secure message interchange among destination pair and known sources. This method cannot directly be employed in terms of VANET because of the dynamics of VANET. Message dissemination in VANET could be susceptible to inside attacks (viz., attacks from valid VANET members), that might damage the content of disseminated message or transmit malicious message. Therefore, guaranteeing the authenticity and integrity of the transferred message in VANET is a significant problem.

This paper presents a new lightweight authentication and privacy-preserving protocol using Improved Timed Efficient Stream Loss-Tolerant Authentication with Cuckoo Filter (ITESLA-CF) for VANETs. The ITESLA-CF technique aims to achieve effective broadcast authentication as TESLA with minimal memory requirement. Moreover, the ITESLA-CF technique comprises a CF to store the authentic data of vehicle that exist in the RSU's range. The presented model has lightweight mutual authentication among the parties and it offers robust anonymity to accomplish privacy and resists ordinary attacks. For ensuring the improved efficiency of the ITESLA-CF technique, a series of experiments were performed and the results are examined in terms of several metrics.

Literature review

Alfadhli et al. [9] proposed a light-weighted system, SD2PA, depending upon a common Hash Function (HF) for VANET. This technique confronts the non-safe driving issue caused by the crucial driving region. Furthermore, the vehicle validation is made using VANET scheme administrator in the vehicles moving; hence, the validation redundancies for the whole systems are deceased and system management efficacy is improved. Yu et al. [10] proposed a privacy-preserving light-weighted authentication protocol for the demand response management in the SG environment for addressing the security limitations. The presented protocol resists several attacks and guarantees secure mutual anonymity and authentication. They calculated the security factors of the projected system by informal security analyses and verified the session key security of projected system by the ROR module.

Sathya Narayanan [11] presents a protocol, i.e., SSVC for enabling reliable and secure transmission in VANET. The aim of this study is to decrease the latency and enhance the transmission efficacy of network. Initially, a network is made by n amount of vehicles, and neighbor finding is executed through WAVE protocol. Alazzawi et al. [12] utilized a novel concept for generating pseudonyms for the vehicles while all the on-board unit (OBU) keeps one pseudonym, called "pseudonym root," and generate each pseudonym from a similar pseudonym. Thus, OBU no needs to expand its storage. In addition, the system does not utilize bilinear pairing process which causes computational overhead, and it has no certification revocation listed which results in computational and transmission overhead. This system has light-weighted mutual validation among the entire parties. Furthermore, it gives stronger anonymity for preserving privacy and resists regular attacks.

Ali and Li [13] proposed an effective ID-CPPA signature system depending upon bilinear map for V2I transmission. This system utilizes common 1 way HF instead of map to point HF. This raises the efficacy by signing and authentication of message at the RSU is executed. In Alfadhli et al. [14], a strong verification solution must deliberate these security problems and the nature of resource-limited nodes. It utilizes an integration of PUF and one-time dynamic pseudo-identity as verification factor. In addition, it removes the heavyweight dependency on the scheme key through decentralizing the broad area of CA to local areas and attains strong controller of the domain key.

Moni and Manivannan [15] proposed a scalable, distributed, privacy-preserving authentication, low overhead system for VANET. This technique utilizes an MHT to authenticate RSU and MMPT vehicles. Feng et al. [16] presented an EPAM, leveraging the asynchronous accumulator for extending the blockchain application. In addition, with the design of mutual authentication protocol, they attain privacy features such as unlinkability and anonymity in the deliberation of semitrust RSU.

Xiong et al. [17] present a CPPA with double insurance support batch authentication for VANET that is created in cyclic group on elliptical curves. Moreover, the master private key or vehicle private key is revealed, it is not possible for forging a valid authenticated message for deceiving the receivers that attain double insurance for the private key. If the multiple messages are attributed, this CPPA-D system permits the recipient to execute batch authentication for improving the efficacy. In Li et al. [18], a light-weighted authentication protocol in a proper transmission module for VANET encounters the privacy protection requirements, using HF and exclusive OR function. Prover if is utilized for verifying the protocol security, and the result shows that privacy could be assured in the simulated attacker.

Problem statement

As displayed in Fig. 2, the VANET framework in this study has fixed RSU at the roadside, trust authority (TA), and OBU fitted on mobile vehicles.

- Trust authority (TA): The TA is a trusted third party that is a registration center for RSU and OBU, and would not compromise [19]. TA and RSU interact by secure communication protocols, like TLS protocol. For avoiding an individual point of failures or bottleneck, redundant TA has similar databases and functionalities that are connected.
- RSUs: The RSU is confidential and difficult that exists compromised. The RVC range is double of the IVC range to guarantee when an RSU obtains a message, each vehicle receives a similar message that exits from the possible range to obtain the notice from the RSU.
- It utilizes traditional public key infrastructure (P-KI) to initiate handshaking. All the vehicles V_i have a traditional private key SK_i and a public key PK_i, and the PK_i is called TA. The public key $\mathrm{PK}_{\mathrm{TA}}$ of TA is called by every person. All the RSU transmits its public key PK_{R} using the message occasionally to the vehicle that is traveling at the RVC range [20]. Thus, PK_{R} is called through the whole vehicles near. It is not necessary for the vehicle to be familiar with the public keys of another vehicle to evade message overhead for swapping certificates. The private keys of TA, RSU and V_i are $\mathrm{SK}_{\mathrm{TA}}$, SK_{R} and SK_{V_i} correspondingly and are saved confidential with the respective parties.

The projected system aims to attain the succeeding security purposes:

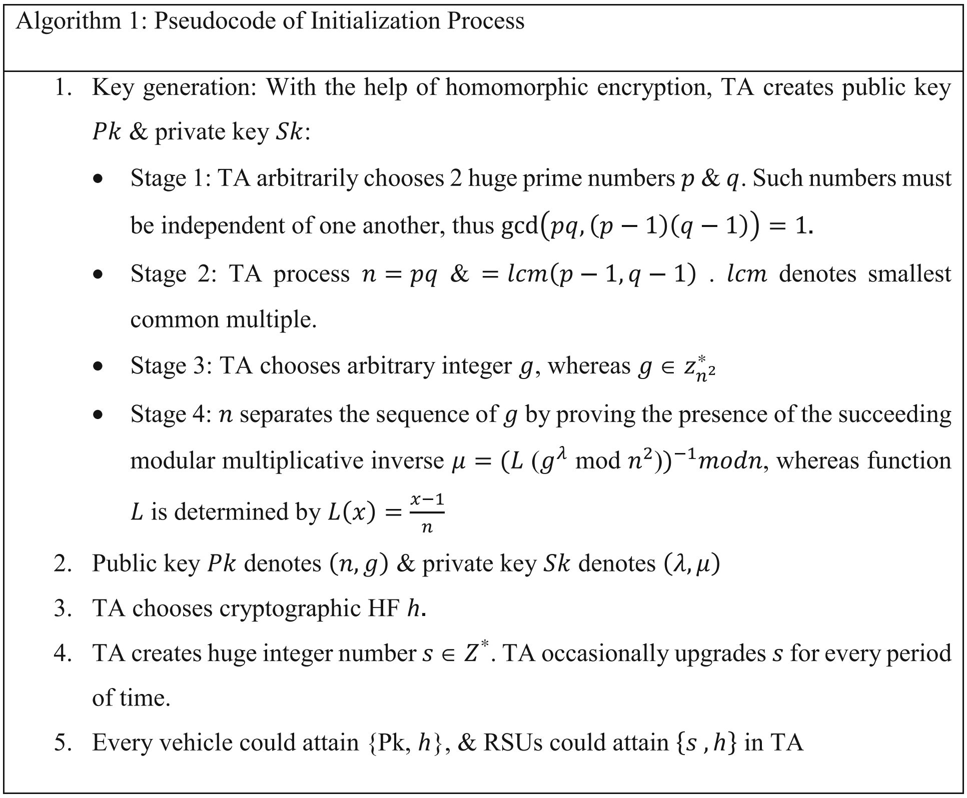
- Message integrity and authentication: The vehicle can authenticate that messages are transmitted and signed with other vehicle with no modification by others.
- Identity privacy preserving: Some third party is not capable to attain the vehicle real identity as examining many messages transmitted with a similar vehicle.
- Traceability and revocability: An id of vehicle must be unseen in usual message receptor in the verification procedure for protecting the transmitter's private data; when it is essential, the TA must have the capability for attaining the vehicle real id and revoke it from upcoming use.
- Collusion resistance: If numerous vehicles get together, they still could not create a valid signature for other vehicles. Noted that, in this study, they do not assume the insider adversary, viz., RSU does not get together by other vehicles to disclose the confidential content.
- Replaying resistance: The malicious vehicle could not store and gather a signed message and try to send it at a late time if the original message is not valid.

The proposed model

The proposed model encompasses different stages of operations such as initialization, registration, mutual authentication, broadcast and verification, and vehicle revocation phases. The detailed working of these processes is neatly explained in the succeeding sections.

Stage I: initialization process

In this section, the TA operates in creating the fundamental scheme variables. This parameter is distributed to the participant of VANETs for facilitating the registration and another procedure or OBU and RSU:



```
Algorithm 1: Pseudocode of Initialization Process

1. Key generation: With the help of homomorphic encryption, TA creates public key $Pk$ & private key $Sk$:
    • Stage 1: TA arbitrarily chooses 2 huge prime numbers $p$ & $q$. Such numbers must be independent of one another, thus $\gcd\big(pq,(p-1)(q-1)\big) = 1$.
    • Stage 2: TA process $n = pq$ & $= lcm(p-1, q-1)$ . $lcm$ denotes smallest common multiple.
    • Stage 3: TA chooses arbitrary integer $g$, whereas $g \in z^*_{n^2}$
    • Stage 4: $n$ separates the sequence of $g$ by proving the presence of the succeeding modular multiplicative inverse $\mu = (L\ (g^{\lambda} \bmod n^2))^{-1} mod n$, whereas function $L$ is determined by $L(x) = \frac{x-1}{n}$
2. Public key $Pk$ denotes $(n, g)$ & private key $Sk$ denotes $(\lambda, \mu)$
3. TA chooses cryptographic HF $h$.
4. TA creates huge integer number $s \in Z^*$. TA occasionally upgrades $s$ for every period of time.
5. Every vehicle could attain {Pk, $h$}, & RSUs could attain $\{s\ , h\}$ in TA
```

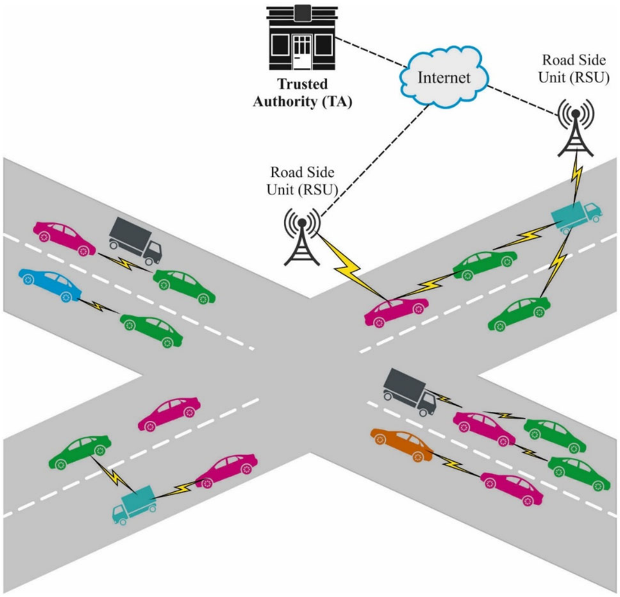


Fig. 2 System model

Stage 2: registration process

A new contributor must endure a registration procedure to be confirmed as trustworthy [12]. This stage has RSU registration and vehicle registration:

1. RSU registration: TA selects the real id of RSU ID_R based on location. Later, it creates arbitrary integer number $m_R \in Z^*$ and find equivalent registration time T_{Reg_R}. Lastly, TA keeps $< \text{ID}_R, m_R, T_{\text{Reg}_R} >$ to registration list $\text{Reg}L_R$ and send the similar data using number s to RSU.
2. OBU registration: During this procedure, OBU would utilize 4G/5G transmission for sending registration requests to TA. First, vehicle drivers select passwordPW, and later OBU would transmit message $\{\text{enc}_{Pk}(\text{ID}_v, \text{PW})\}$. TA decrypt received message $\{\text{dec}_{Sk}(\text{ID}_v, \text{PW})\}$, and later it would authenticate real identityID_v, create arbitrary integer number $m_v \in Z^*$, finds equivalent registration time$T_{\text{Reg}_\mathcal{V}}$, and compute $m_v^* = m_v \oplus h(\text{PW})$ and$\sigma_{\text{TA}} = h\left(T_{\text{Reg}_\mathcal{V}}||ID_v||m_v\right)$. Lastly, it would save $< \text{ID}_R, \text{PW}, m_R, T_{\text{Reg}_R} >$ to registration list $\text{Reg}L_v$ and send $< m_v^*, T_{\text{Reg}_\mathcal{V}}, \sigma_{\text{TA}} >$ to OBU. Afterward obtaining the message, OBU compute $m_v = m_v^* \oplus h(\text{PW})$ and check if$\sigma_{\text{TA}} =? h\left(T_{\text{Reg}_\mathcal{V}}||ID_v||m_v\right)$. When it is similar, then it saves $< \text{ID}_R, \text{PW}, m_\text{R}, T_{\text{Reg}_R} >$ to TPD.

Stage 3: mutual authentication process

In this phase, the ITESLA technique gets executed to achieve effective authentication among every part of the VANET (TA, RSU, and OBU). TESLA utilizes symmetric cryptography and delayed key disclosure for performing transmission verification (the left side represents operation in TESLA). For authenticating a message M, a transmitter broadcast the MAC (Phase 2) of the packet that utilizes the senders key for this interval (K_i). The recipient saves the whole message and MAC (Phase 3) till the transmitter broadcasts the key. Afterward the key revelation period, the transmitter broadcasts the key (Phase 5). For authenticating the message, receiver verifies that the kept message/MAC pairs agree with the transmission key (Phases 6 and 7). Using sufficient pair's malicious transmission, pollution attacks occur while receivers waste a substantial quantity of memory that stores invalid data [21].

ITESLA is designed for preventing memory-based DoS attacks toward TESLA. However, in ITESLA, a receiver stores a self-made MAC for reducing memory needs. A receiver stores shorten form of transmitter's data, the transmitter initially transmissions the MAC and then transmits the equivalent key and message (related to the Guy Fawkes protocol). To validate message$M$, in ITESLA, the transmitter initially broadcast the MAC$\left(\text{MACS} = \text{MAC}_{K_i}(M)\right)$ that is calculated by the present keyK_i, together with key index i (Step 2). Over receptions, by the key index i and the time related to the initial transmitter's key chain, a receiver initially authenticates the security state for ensuring that the key K_i for the transmitter has not been transmitting and yet known by the transmitter. When the security conditions do not hold, the recipient drops the MAC, since an attacker can possibly have attained the equivalent keyK_i. The recipient later re-MACs the attained data by a local secret key K_{Recv} which is known to the recipient $\left(\text{MAC}_R = \text{MAC}_{K_{\text{Recv}}}(\text{MAC}_S)\right)$ (Phase 3) and stores this short MAC(MAC_R) together with the key index (Phase 4).

When the key K_i is revealed, the transmitter would transmit other messages, and the key is utilized for calculating the message' MACs (Step 5). For verifying a message, the recipient initially verifies the authority of K_i by succeeding the one-way key chain back to a confidential key. The recipient later calculates the shorten MAC of the message (Phase 6) and relates it to the MAC and index kept in memory (Phase 7). When the recipient has an equivalent MAC/key index pair in memory, the recipient considers the message authentic (Phase 8).

Eventually, the recipient would save additional MAC and key index pairs from the memory. If a kept MAC effectively authenticates a message, the recipient could open the memory utilized for storing the MAC and key index. However, if the recipient lost legitimate sender messages and key transmission or the malicious node floods the network using MACs in an effort to waste a receiver resource, the recipient would require a policy for determining when to substitute a MAC and key pair. For the substitution policy, receiver stores the transmitter identity and coming timestamp together to shorten MAC and the key index. When memory space becomes inadequate, they utilize subsequent policy for identifying shorten MACs to get rid of:

- Every shorten MACs with key indices are older compared to the latter authentic message attained in that transmitter. The perception is that older shorten MACs are yet saved since an attacker inserted the message or equivalent messages and disclosed key is missing.
- When extra space is required, the message where the verifications are farthest out in the upcoming is removed. This addresses the situation where the attacker tries to trick receiver to store message for longer period by requesting the key index is n if the real transmitter's present key index is j if $j << n$.

Stage 4: broadcast and verification process

RSU occasionally transmits notice message that gave CF. The filter is utilized for storing fingerprints of legitimate pseudonym f(Ps). It can be novel method of probabilistic data structure which is utilized for testing membership of item among the sets. It provides optimum search accuracy and time compared to bloom filters equivalent to save size [22]. It can be included from an array of buckets whereas all the buckets include many entries. It decreases their space by calculating a fingerprint f of the value of the items to be kept in the array. It utilizes smaller f bit fingerprint to represent the data. A CF is utilized as a cuckoo hashing function to discard collision and mainly a compact cuckoo hash table. In cuckoo hashing functions, all the data items are hashed using 2 dissimilar HF for calculating the indices of 2 candidate buckets i_1 and i_2 as $i_1 = h(\text{item})\text{mod}M$ and $\text{i}_2 = i \oplus h$ $(f(\text{item}))\text{mod}M$, whereas M denotes size of CF. Value f could be distributed to most 2 candidate buckets while the candidate bucket i_1 was attempted initially. When the bucket i_1 was empty, then the value was placed in i_1. When it is distributed, then bucket i_2 is attempted. When the bucket i_2 is empty, next the value is placed there. When i_2 is distributed, afterward the occupier of i_2 is removed and the value of f is placed there. For testing the membership of other items from CF, they first calculate the fingerprint of item $f(\text{item})$ and computes i_1, i_2. Later, when the $f(\text{item})$ is discovered i_1 or i_2, the CF is verified correct; or else, the CF is verified incorrect. Figure 3 illustrates the insertion procedure in CF.

1. Broadcast procedure: Afterward the mutual authentication procedure is finished, OBU begins transmitting the beacons. Previously, RSU and OBU perform as follows [12]:

- RSU derives the initial pseudonym level to a novel vehicle in their P_{root} as $Ps = h(P_{\text{root}}|1\text{Lev})$, whereas $\text{Lev} = 1$.
- RSU inserts {Ps, Lev} to PsL.
- RSU inserts f(Ps) for CF with cuckoo hashing, viz., described in sec (3.4), and distributes it using notice message. (Afterward, the whole vehicles from RSU ranges attain the cuckoo; hence, the beacons to a novel vehicle would be verified authentic.)
- OBU derive the initial pseudonym level Ps in P_{root} and $\text{Lev} = 1$. Thus, the beacon would be recognized to the whole contributors and beacon transmitter would be verified as authentic. The beacon derives in $\{T, \text{msg}, \sigma_{\text{msg}}\}$, whereas $\sigma_{\text{msg}} = \text{Ps} \oplus h(T||\text{msg}||s)$. (RSU increase Lev with one for the entire OBUs in its range for deriving the novel Ps for every upgrading procedure to CF. Afterward upgrading the CF, OBU improves Lev with one and derives similar Ps.)

2. Authentication procedure: Once vehicles receive beacon $\{T, \text{msg}, \sigma_{\text{msg}}\}$, it executes the succeeding step:

- Initial step: Verify timestamp T whether it is latest/not. In this case, continue the authentication procedure. Or else, it drops the beacon.
- 2nd step: Calculate $Ps = \sigma_{\text{msg}} \oplus h\ (T||\text{msg}||s)$.
- 3rd step: Check f(Ps) from the 2 hashed i_1, i_2 from the CFs. When unoccupied, latter it drops the beacons.

Stage 5: vehicle revocation process

This stage describes how TA revokes other vehicles which transmit incorrect data. But, all the RSUs have the whole data regarding OBUs within its range in PsL; thus, the culprit vehicle is discovered, and the RSU attains the data of this vehicle in their beacon. Later, it sends the data $\left\{P_{\text{root}}, T_{\text{Reg}_V}\right\}$ to TA. TA retrieves the real identity ID_v from $\text{Reg}L_v$ based on data in the obtained messages. Then, it eliminates the vehicle from $\text{Reg}L_v$, inserts it into the revocation list, and upgrades number$s$. Finally, TA notices that RSU eliminates the vehicle in their PsL and revokes in repeated transmission.

Performance validation

This section examines the performance of the ITESLA-CF technique in terms of different measures under varying vehicle speeds. The proposed model is simulated using MATLAB tool. Table 1 determines the result analysis of ITESLA-CF model with different techniques in terms of PDR, throughput, and Routing Control Overhead (RCO).

Figure 4 investigates the PDR analysis of the ITESLA-CF technique over the other techniques with respect to different vehicle speeds. The figure depicted that the ITESLA-CF

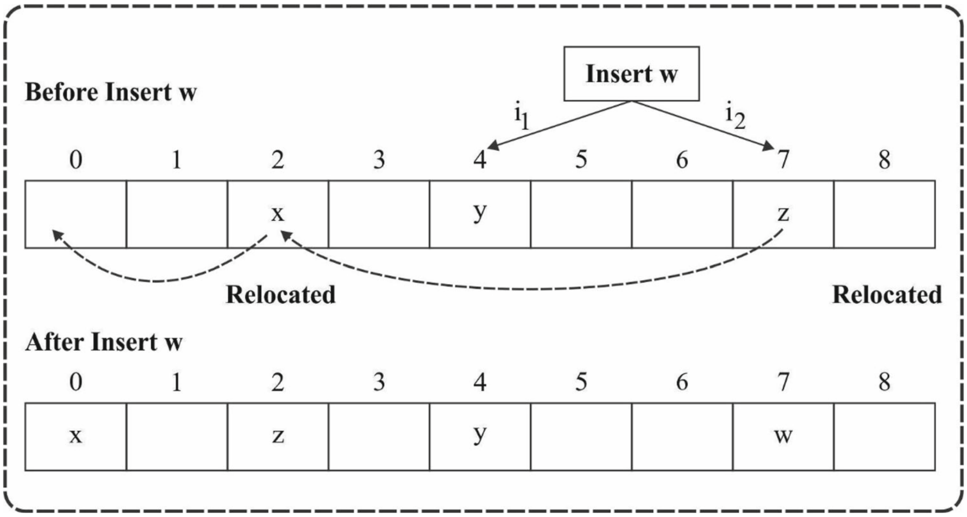


Fig. 3 Insertion process in Cuckoo filter

Table 1 Result analysis of ITESLA-CF model with exiting techniques

Vehicle speed (km/h)	BPAB	3P3B	UMBP	SSVC	ITESLA-CF
Packet delivery ratio (%)					
50	51.55	85.26	90.56	93.53	97.56
60	49.86	82.93	89.29	92.68	96.71
70	43.92	80.17	82.08	84.84	92.26
80	41.59	77.21	82.51	86.75	92.05
90	39.89	74.87	79.75	83.78	90.77
100	38.20	72.97	78.69	82.93	91.20
Throughput (kbps)					
50	85,134.69	85,592.55	86,344.75	90,563.60	90,956.06
60	88,535.94	86,050.41	84,807.65	89,647.88	90,563.60
70	86,279.34	85,134.69	86,148.52	90,759.83	90,825.24
80	85,854.18	84,578.72	86,475.57	89,876.81	90,400.08
90	88,307.01	84,120.86	84,807.65	89,582.48	90,007.63
100	84,055.45	81,962.37	86,671.79	89,615.18	90,105.74
Routing control overhead (%)					
50	36.00	28.26	23.34	16.45	13.64
60	40.08	32.48	27.42	19.40	16.17
70	42.33	35.01	32.20	22.78	18.28
80	45.14	38.95	35.16	27.00	21.51
90	47.25	43.17	37.55	29.11	24.33
100	50.34	45.28	40.78	33.05	27.28

technique has accomplished better performance with the maximum PDR under varying vehicle speeds. For instance, with 50 km/h, the ITESLA-CF technique has obtained a higher PDR of 97.56% whereas the BPAB, 3P3B, UMBP, and SSVC techniques have attained a lower PDR of 51.55%, 85.26%, 90.56%, and 93.53%, respectively. In addition, with 70 km/h, the ITESLA-CF algorithm has gained a superior PDR of 92.26% whereas the BPAB, 3P3B, UMBP, and SSVC manners have attained a lesser PDR of 43.92%, 80.17%, 82.08%, and 84.84%, respectively. Followed by, with 100 km/h, the ITESLA-CF method has obtained a higher PDR of 91.20% whereas the BPAB, 3P3B, UMBP, and SSVC algorithms have attained a minimum PDR of 38.20%, 72.97%, 78.69%, and 82.93% correspondingly.

Figure 5 examines the throughput analysis of the ITESLA-CF method over the other techniques with respect to different vehicle speeds. The figure depicted that the ITESLA-CF technique has accomplished better performance with the maximum throughput under varying vehicle speeds. For instance, with 50 km/h, the ITESLA-CF technique has obtained a higher throughput of 90956.06 whereas the BPAB, 3P3B, UMBP, and SSVC techniques have attained

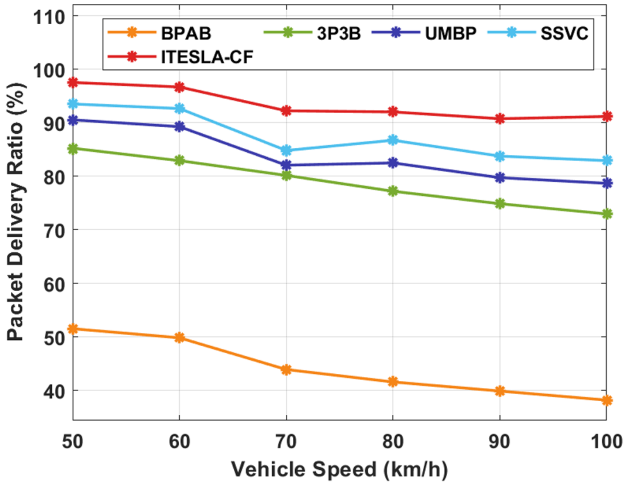


Fig. 4 PDR analysis of ITESLA-CF model

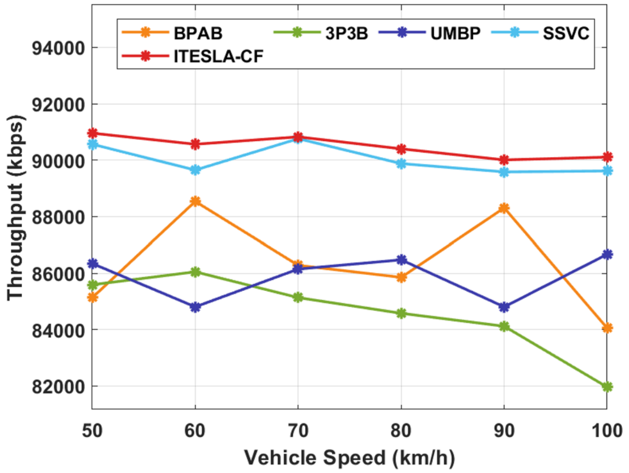


Fig. 5 Throughput analysis of ITESLA-CF model

a lower throughput of 85134.69, 85592.55, 86344.75, and 90563.60 correspondingly. Besides, with 70 km/h, the ITESLA-CF algorithm has obtained a higher throughput of 90825.60 whereas the BPAB, 3P3B, UMBP, and SSVC techniques have attained a lower throughput of 86279.34, 85134.69, 86148.52, and 90759.83 correspondingly. Lastly, with 100 km/h, the ITESLA-CF approach has obtained an improved throughput of 90105.74 whereas the BPAB, 3P3B, UMBP, and SSVC techniques have attained a minimum throughput of 84055.45, 81962.37, 86671.79, and 89615.18, respectively.

A brief RCO analysis of the ITESLA-CF technique under distinct vehicle speed takes place in Fig. 6. The experimental results showcased that the ITESLA-CF technique has gained effective outcomes with the least ROC. For instance, under 50 km/h, the ITESLA-CF technique has achieved a least RCO of 13.64% whereas the BPAB, 3P3B, UMBP, and SSVC techniques have resulted in an increased RCO

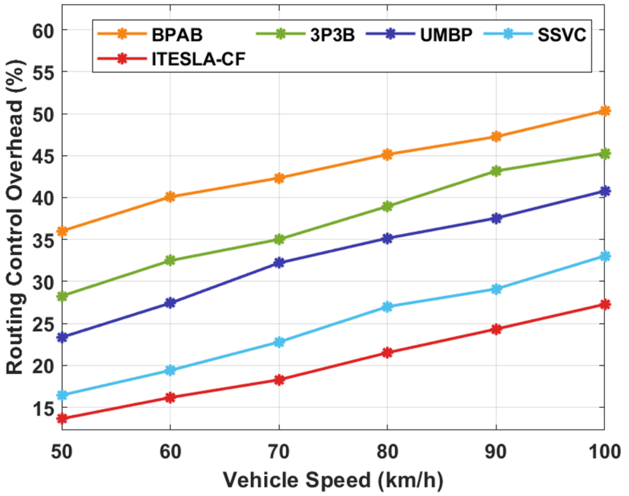


Fig. 6 RCO analysis of ITESLA-CF model

of 36%, 28.26%, 23.34%, and 16.45%, respectively. Eventually, under 70 km/h, the ITESLA-CF manner has reached a lower RCO of 18.28% whereas the BPAB, 3P3B, UMBP, and SSVC methodologies have resulted in an improved RCO of 42.33%, 35.01%, 32.20%, and 22.78% correspondingly. Meanwhile, under 100 km/h, the ITESLA-CF technique has obtained the least RCO of 27.28% whereas the BPAB, 3P3B, UMBP, and SSVC techniques have resulted in a higher RCO of 50.34%, 45.28%, 40.78%, and 33.05% correspondingly.

Table 2 defines the result analysis of ITESLA-CF model with distinct techniques with respect to transmission delay, Key Computation Time (KCT), and Key Recovery Time (KRT). A brief transmission delay analysis of the ITESLA-CF method under different vehicle speed takes place in Fig. 7. The experimental outcomes illustrated that the ITESLA-CF manner has reached effective results with the minimum transmission delay. For sample, under 50 km/h, the ITESLA-CF manner has attained a minimum transmission delay of 161.38 ms whereas the BPAB, 3P3B, UMBP, and SSVC approaches have resulted in an improved transmission delay of 588.9 ms, 391.79 ms, 283.53 ms, and 205.8 ms correspondingly. Likewise, under 70 km/h, the ITESLA-CF technique has attained a minimal transmission delay of 216.9 ms whereas the BPAB, 3P3B, UMBP, and SSVC approaches have resulted in an increased transmission delay of 716.6 ms, 477.85 ms, 347.38 ms, and 266.87 ms correspondingly. Similarly, under 100 km/h, the ITESLA-CF technique has achieved a least transmission delay of 302.96 ms whereas the BPAB, 3P3B, UMBP, and SSVC techniques have resulted in an increased transmission delay of 924.8 ms, 658.3 ms, 430.66 ms, and 364.03 ms, respectively.

A detailed KCT analysis of the ITESLA-CF technique under distinct key size takes place in Fig. 8. The experimental results exhibited that the ITESLA-CF manner has increased effective outcomes with the minimum ROC. For instance,

Table 2 Result analysis of ITESLA-CF method with different techniques

Vehicle speed (km/h)	BPAB	3P3B	UMBP	SSVC	ITESLA-CF
Transmission delay (ms)					
50	588.90	391.79	283.53	205.80	161.38
60	649.97	416.78	308.51	241.89	186.36
70	716.60	477.85	347.38	266.87	216.90
80	783.22	536.15	372.36	300.18	244.66
90	847.07	594.45	405.67	336.27	269.65
100	924.80	658.30	430.66	364.03	302.96
Key size (bits)	NTRU	VGKM	EGKM	SSVC	ITESLA-CF
Key computation time (KCT) (ms)					
64	3558.94	3008.45	2733.21	2090.98	1889.14
128	4054.37	3522.24	3173.60	2402.92	2109.33
256	4531.46	3852.53	3448.84	2696.51	2256.13
512	5081.94	4237.87	3907.58	3081.85	2623.12
Key recovery time (KRT) (ms)					
64	1.43	1.21	1.10	0.84	0.77
128	1.62	1.40	1.28	0.97	0.90
256	1.81	1.55	1.39	1.07	0.97
512	2.01	1.69	1.57	1.23	1.08

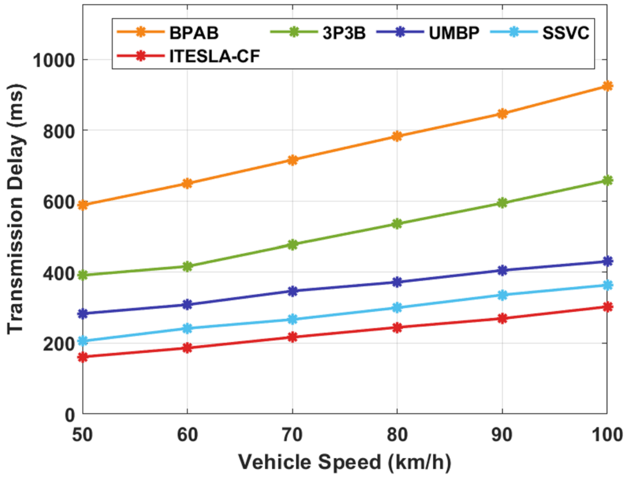


Fig. 7 Transmission delay analysis of ITESLA-CF model

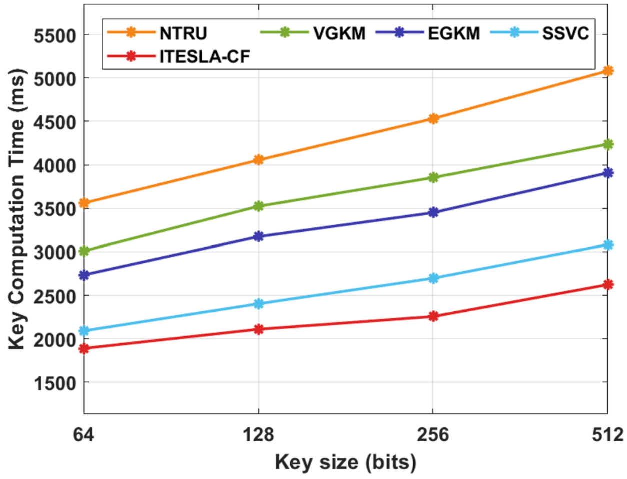


Fig. 8 Key computation time analysis of ITESLA-CF model

under 64 bits, the ITESLA-CF technique has attained a least KCT of 1889.14 ms whereas the NRTU, VGKM, EGKM, and SSVC techniques have resulted in an improved KCT of 3558.94 ms, 3008.45 ms, 2733.21 ms, and 2090.98 ms, respectively. Followed by, under 256 bits, the ITESLA-CF technique has achieved a least KCT of 2256.13 ms whereas the NRTU, VGKM, EGKM, and SSVC techniques have resulted in a maximum KCT of 4531.46 ms, 3852.53 ms, 3448.84 ms, and 2696.51 ms, respectively. Finally, under 512 bits, the ITESLA-CF approach has achieved a lower KCT of 2623.12 ms whereas the NRTU, VGKM, EGKM, and SSVC algorithms have resulted in a maximal KCT of 5081.94 ms, 4237.87 ms, 3907.58 ms, and 3081.85 ms correspondingly.

A briefly KKT analysis of the ITESLA-CF approach in various key size take place in Fig. 9. The experimental outcomes demonstrated that the ITESLA-CF manner has increased effective outcomes with the minimum ROC. For sample, under 64 bits, the ITESLA-CF methodology has attained a worse KKT of 0.77 ms whereas the NRTU, VGKM, EGKM, and SSVC approaches have resulted in an improved KKT of 1.43 ms, 1.21 ms, 1.10 ms, and 0.84 ms correspondingly. At the same time, under 256 bits, the ITESLA-CF technique has attained a least KKT of 0.97 ms whereas the NRTU, VGKM, EGKM, and SSVC techniques have resulted in a higher KKT of 1.81 ms, 1.55 ms, 1.39 ms, and

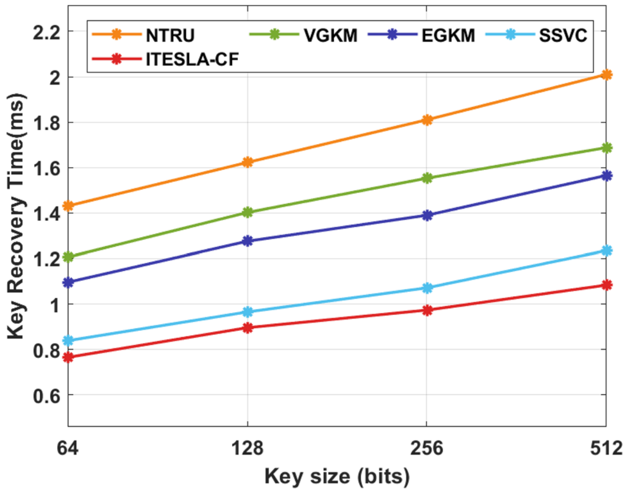


Fig. 9 Key recovery time analysis of ITESLA-CF model

1.07 ms correspondingly. In the meantime, under 512 bits, the ITESLA-CF technique has achieved a lower KKT of 1.08 ms whereas the NRTU, VGKM, EGKM, and SSVC methods have resulted in a maximum KKT of 2.01 ms, 1.69 ms, 1.57 ms, and 1.23 ms correspondingly.

Conclusion

This paper has presented an effective ITESLA-CF technique to achieve authentication and privacy in VANET. The proposed model encompasses different stages of operations such as initialization, registration, mutual authentication, broadcast and verification, and vehicle revocation phases. Furthermore, the ITESLA-CF technique comprises a CF for storing the authentic data of vehicles that exist in the RSU's range. The presented model is lightweight mutual authentication among the parties and it attains robust anonymity to realize privacy and resist ordinary attacks. For ensuring the improved efficiency of the ITESLA-CF technique, a series of experiments were performed and the results are examined in terms of several metrics. The experimental values highlighted the betterment of the proposed ITESLA-CF technique over the existing techniques. In future, the presented model can be extended to the design of energy management and traffic flow predictive techniques in ITS.

Funding The authors received no specific funding for this study.

Declarations

Conflict of interest The authors declare that they have no conflicts of interest to report regarding the present study.

Data availability Available based on request.

Code availability Available based on request.

References

1. Rehman A, Rehman SU, Khan M, Alazab M, Reddy T (2021) CANintelliIDS: detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU. IEEE Transa Netw Sci Eng. https://doi.org/10.1109/TNSE.2021.305988
2. Ali GMN et al (2016) Efficient data dissemination in cooperative multi-RSU vehicular ad hoc networks (VANETs). J Syst Softw 117:508–527
3. Javed AR, Usman M, Rehman SU, Khan MU, Haghighi MS (2020) Anomaly detection in automated vehicles using multistage attention-based convolutional neural network. IEEE Trans Intell Transp Syst. https://doi.org/10.1109/TITS.2020.3025875
4. Singh S, Agrawal S (2014) VANET routing protocols: issues and challenges. In: Engineering and computational sciences (RAECS), 2014 recent advances in, 2014, pp. 1–5
5. Wang W, Xu H, Alazab M, Gadekallu TR, Han Z, Su C (2021) Blockchain-based reliable and efficient certificateless signature for IIoT devices. IEEE Trans Ind Inf. https://doi.org/10.1109/TII.2021.3084753
6. Bitam S et al (2015) VANET-cloud: a generic cloud computing model for vehicular Ad hoc networks. IEEE Wirel Commun 22:96–102
7. Zhang L, Peng M, Wang W, Jin Z, Su Y, Chen H (2021) Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing. Trans Emerg Telecommun Technol. https://doi.org/10.1002/ett.4315
8. Wang W, Huang H, Zhang L, Han Z, Qiu C, Su C (2020) BlockSLAP: Blockchain-based secure and lightweight authentication protocol for smart grid. In 2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom), IEEE. pp. 1332–1338
9. Alfadhli SA, Lu S, Fatani A, Al-Fedhly H, Ince M (2020) SD2PA: a fully safe driving and privacy-preserving authentication scheme for VANETs. HCIS 10(1):1–25
10. Yu S, Park K, Lee J, Park Y, Park Y, Lee S, Chung B (2020) Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment. Appl Sci 10(5):1758
11. SathyaNarayanan PSV (2019) A sensor enabled secure vehicular communication for emergency message dissemination using cloud services. Digit Signal Process 85:10–16
12. Alazzawi MA, Lu H, Yassin AA, Chen K (2019) Robust conditional privacy-preserving authentication based on pseudonym root with cuckoo filter in vehicular ad hoc networks. KSII Trans Internet Inf Syst 13(12):6121–6144

13. Ali I, Li F (2020) An efficient CPPA scheme for vehicle-to-infrastructure communication in VANETs. Veh Commun 22:100228
14. Alfadhli SA, Lu S, Chen K, Sebai M (2020) Mfspv: A multi-factor secured and lightweight privacy-preserving authentication scheme for vanets. IEEE Access 8:142858–142874
15. Moni SS, Manivannan D (2021) A scalable and distributed architecture for secure and privacy-preserving authentication and message dissemination in VANETs. Internet Things 13:100350
16. Feng X, Shi Q, Xie Q, Liu L (2021) An efficient privacy-preserving authentication model based on blockchain for VANETs. J Syst Arch 117:102158
17. Xiong W, Wang R, Wang Y, Zhou F, Luo X (2021) CPPA-D: efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs. IEEE Trans Veh Technol 70(4):3456–3468
18. Li X, Liu T, Obaidat MS, Wu F, Vijayakumar P, Kumar N (2020) A lightweight privacy-preserving authentication protocol for VANETs. IEEE Syst J 14(3):3547–3557
19. Sun Y, Lu R, Lin X, Shen X, Su J (2010) An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. IEEE Trans Veh Technol 59(7):3589–3603
20. Cui J, Zhang J, Zhong H, Xu Y (2017) SPACF: a secure privacy-preserving authentication scheme for VANET with cuckoo filter. IEEE Trans Veh Technol 66(11):10283–10295
21. Wu Z, Zhang Y, Liu L, Yue M (2020) TESLA-based authentication for BeiDou civil navigation message. China Commun 17(11):194–218
22. Bin F, Andersen DG, Kaminsky M, Mitzenmacher MD (2014) Cuckoo filter: practically better than bloom. In: Proc. of the 10th ACM international on conference sydney, Australia, December 2–5, pp. 75–88

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.