IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received 16 December 2023, accepted 19 February 2024, date of publication 20 February 2024, date of current version 29 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3368393

RESEARCH ARTICLE

FC-LSR: Fog Computing-Based Lightweight Sybil Resistant Scheme in 5G-Enabled Vehicular Networks

ABDULWAHAB ALI ALMAZROI[1], MONAGI H. ALKINANI[2], MAHMOOD A. AL-SHAREEDA[3], MOHAMMED A. ALQARNI[4], ALAA ATALLAH ALMAZROEY[5], AND TAREK GABER[6], (Member, IEEE)

[1]Department of Information Technology, College of Computing and Information Technology at Khulais, University of Jeddah, Jeddah 23218, Saudi Arabia
[2]Department of Computer Science and Artificial Intelligence, College of Computer Science and Engineering, University of Jeddah, Jeddah 23218, Saudi Arabia
[3]Department of Communication Engineering, Iraq University College, Basra 11800, Iraq
[4]Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 23218, Saudi Arabia
[5]Modern Aljazeera Company, Khulais 25503, Saudi Arabia
[6]School of Science, Engineering and Environment, University of Salford, M5 4WT Manchester, U.K.

Corresponding authors: Abdulwahab Ali Almazroi (aalmazroi@uj.edu.sa) and Mahmood A. Al-Shareeda (alshareeda022@gmail.com)

This work was supported by the University of Jeddah, Jeddah, Saudi Arabia, under Grant UJ-23-SRP-4.

ABSTRACT Vehicular networks with Fifth-Generation (5G) are a new form of wireless communication that could greatly benefit society by lowering the number of preventable car accidents and entertaining passengers in a variety of ways. Security threats can compromise the communications transmitted by a vehicle in a vehicular network because of the open nature of these networks. This means that there are potential security and privacy concerns with VANET. Many methods for fixing VANET's issues have been offered recently. Unfortunately, most of them suffer from significant overhead and security concerns such as Sybil attacks. Therefore, this paper proposes a novel fog computing-based lightweight Sybil resistant attacks, called FC-LSR in 5G-enabled vehicular networks. The proposed FC-LSR scheme makes use of Modified Merkle Patricia Trie (MMPT) in conjunction with Merkle Hash Tree (MHT) to securely store the 'current status' values of cars while protecting the anonymity of the data. In the proposed FC-LSR scheme, vehicles inside the same fog server's region are more likely to update their anonymity at the same time and on a regular basis when anonymous expiration is enabled.

INDEX TERMS Fog server, fog computing, fifth-generation (5G), Sybil attacks, vehicular network.

I. INTRODUCTION

Research and development into automotive-related technologies has often been regarded as one of the most promising. When human well-being rises, the field of automobile engineering rises with it [1]. Congestion of urban traffic and traffic jam are only two of the many issues that have put the spotlight on today's automobile networks. Rapid alerts, cornering, data of traffic status, street conditions, warnings of intersection, and pedestrian crossing alerts are just a few of the many important traffic issues that can be transmitted to users via car networks [2], [3].

To improve driver safety and better manage increasingly unpredictable traffic patterns [4], [5], transportation systems in several countries have lately introduced widespread deployments of 5G technology, vehicle networks, and fog computing. Wireless equipment fitted in vehicles (termed onboard units, or OBUs) gather, operation, and distribute road information in the context of networked autos [6].

Although 5G-enabled vehicular network have promising applications, widespread adoption faces significant obstacles. 5G-enabled vehicular network communication is susceptible to a wide variety of threats since it is wireless. Authentication is crucial for sending messages over a secure channel. Adversaries can easily compromise other users on 5G-enabled vehicular networks without a strong

The associate editor coordinating the review of this manuscript and approving it for publication was Miguel López-Benítez.

authentication system. A traffic delay could be caused, for instance, if malignant vehicles circulate false data about an incident and then block the traffic. It can impersonate a roadside unit (RSU) or electronic toll booth to gain access to other drivers' private data. In addition, drivers may be hesitant to join 5G-enabled vehicular network out of concern for their own safety and security.

As a result, there is a pressing need for the development and deployment of authentication and message distribution techniques that respect users' right to privacy. Anonymous-based authentication and message propagation is one of the most widely presented techniques in the literature to safeguard cars' and drivers' privacy. In this authentication method, vehicles utilize anonymous IDs in place of their true IDs wherever possible. To facilitate interaction between vehicles and RSUs, each one is fitted with an OBU. Anonymous-based approaches involve a Trusted Authority loading a list of aliases into an OBU installed in a vehicle. To prevent being tracked, vehicles must constantly adopt new aliases. Anonymous linking attacks can be avoided, but only if the vehicle's anonymous is constantly being changed. Let's say only one car out of a hundred has a name change. In that instance, an intruder can simply trace the vehicle's route by associating two messages with the same vehicle and linking the previous and new anonymous used by the vehicle. Furthermore, more study is required to develop an effective strategy for managing vehicle anonymity. Nevertheless, the vehicular system is susceptible to a variety of attacks [7], including the Sybil attack, in which the intruder pretends to be numerous vehicles by using forged identities [8]. Therefore, this paper proposes a novel fog computing-based lightweight Sybil-resistant attack, called FC-LSR in 5G-enabled vehicular networks. To protect user anonymity, the proposed FC-LSR scheme only requires vehicles to request a pool of anonymous ones with fog server by 5G-base station (5G-BS)'s communication area, after which they can select and utilise a single anonymous at random. The MHT and MMPT data structures are useful for efficiently managing and storing these anonymous, which are used to validate the legitimacy of cars while protecting their owners' anonymity. To efficiently authenticate fog servers without certificates, MHT of public keys is also helpful. The major contributions of this paper are provided as follows.

- This paper proposes an FC-LSR scheme based on fog computing and 5G technology to resist Sybil attacks for vehicular networks. The proposed FC-LSR scheme uses Modified Merkle Patricia Trie (MMPT) combined with Merkle Hash Tree (MHT) for saving vehicles' anonymous and their efficient matching values of 'status of current'.
- The proposed FC-LCR uses MHT to ensure that only legitimate fog servers are used in a vehicle. In addition, certificates are not required for authentication when using our method.
- To prevent the tracking of cars' journeys, fog servers help vehicles in their region change their anonymous concurrently by giving each vehicle's anonymous the same expired period. When a vehicle's anonymous expires, it will re-establish contact with an RSU to select a fresh anonymous from the grouping provided by the vehicle's home RTA at registration.
- We suppose that a car always has enough anonymous such that it never has to recycle one within a year. Anonymous expiration encourages cars within the same fog server's region to change their anonymous concurrently and frequently, making it more difficult to correlate messages from the same vehicle with two different anonymous.
- Finally, the signature verification overhead of the proposed FC-LSR technique is observed to be significantly lower than that of related research.

The reminder of this paper is structured as follows. In Section II, this paper reviews the related work for vehicular networks. In Section III, this paper provides preliminary of this work in detail. In Section IV, this paper describes the phases of the proposed FC-LSR scheme. Security analysis and performance evaluation are introduced In Section V and Section VI, respectively. Lastly, conclusion of this paper is introduced in Section VII.

II. RELATED WORK

The academic and business communities are both interested in vehicular system's security and privacy problems. To address these problems, this section reviews some authentication schemes as follows. Xie et al. [9] were proposed that ECC be used to create a lightweight anonymous authentication method with verification of batch. To prevent RSU capture attacks and OBU intrusion assaults, they employed physical unclonable function and biological keys, and we devise a advantage embedding technique with dynamic pseudonym-ID to allow the TA to restore the identity of a compromised vehicle. Zhang et al. [10] suggested a novel authentication mechanism based on bilinear pairings and short-lived pseudonyms, which the suggested authentication protocol can include features like authenticating the vehicle's identification and validating its sent messages. In order to solve the escrow issue and make certificates unnecessary, Imghoure et al. [11] proposed an authentication with a privacy system that uses elliptic curve cryptography (ECC) instead of the more conventional Map-to-Hash function and bilinear pairing. Chen et al. [12] developed a conditional privacy-preserving scheme using ECC and functions of secure hash in place of the more expensive bilinear pairings and function of map-to-point hash operations. Ali et al. [13] prepared a bilinear pairing-based signcryption scheme to ensure heterogeneous V2I mode in the vehicular system. Haider et al. [14] developed an original lightweight encryption-enabled CPPA method (LWE-CPPA) using form of the Diffie-Hellman method, nodes exchange one-of-a-kind symmetric keys to send and receive alerts securely and to provide a secure cipher for hiding messages from potential threats.

Recently, Genc et al. [15] offered ELCPAS, ECC based pairing-free, energy-efficient, lightweight, certificateless conditional privacy preserving authentication (CL-CPPA) system for the internet of vehicles (IoV). Farooqi et al. [16] created a model for priority-established fog server to lessen the latency and delay of fog server in the context of intelligent urban vehicle transportation. Latency and delay have been drastically reduced thanks to the incorporation of 5G localised Multi-Access Edge Computing (MEC) servers into the fog computing infrastructure in order to fulfil QoS and latency criteria. For VANET communication, Bouakkaz e al. [17] offered a certificateless ring signature (BV-CLRS) with batch verification to guarantee conditional privacy preservation authentication. For vehicular system, Zhu et al. [18] presented a novel CLAS-based authentication strategy that makes use of CPP. The scheme's superior security is demonstrated by rigorous security proofs that are based on the default cryptographic assumption. Cahyadi et al. [19] proposed an authentication method with the potential to boost safety, confidentiality, and productivity by employing the certificateless aggregate signature approach to ensure that no private data is divulged during message transmissions from devices onboard the unit. Nath et al. [20] proposed a reciprocal authentication technique for group communication in VANET that protects users' privacy without requiring them to establish a direct connection to a central authority.

The suggested approach also encrypts all messages before transmission and makes use of pseudonyms to protect users' identities. Wang and Yuo [21] suggested a bilinear-paired local identity-based anonymous message authentication protocol (LIAP). Long-term certifications are issued by the CA at the time of registration for both the vehicle and the RSU. When entering the area serviced by an RSU, a vehicle must authenticate itself using its long-term certificate. In order to verify a vehicle's legitimacy, RSUs consult the VCRL. Vehicles employ the RSU certificate revocation list (RCRL) in a similar fashion. After successfully authenticating with RSUs, vehicles are given keys to use in order to create pseudonyms for use in V2V communication. Even yet, in this design the CA must still disperse RCRL and VCRL. A pseudonym-based authentication approach was developed by Ali et al. [22], which would allow only cars having a valid pseudonym to communicate with one another. First, the Vehicular Manufacturing Corporation (VMC) uses its own secret key embedded in each car to provide a unique initial pseudonym to each vehicle. After obtaining an LTC from the CA, the LTC Authority can then utilise that information to create a PC to the vehicle. Subsequent, the vehicle submits a request to the PP for pseudonyms, either directly or via RSUs. All of the aliases that PP provides the car with will work for the same amount of time. Since numerous pseudonyms for the same car are active at the same time, this technique is vulnerable to Sybil attacks. Furthermore, CA utilises CRL for vehicle authentication. Bilinear pairing and Map-To-Point operation were proposed by Bayat et al. [23] as a practical RSU-based authentication technique. To participate in VANET communication, a vehicle would register with a certain RSU's area. RSU creates a set of pseudonyms and the secret keys that go along with them for each node in its zone after mutual authentication. In this technique, authentic vehicle identifiers are added to CRLs to prevent eavesdropping. There is an added cost to authenticating all RSUs because of this. The lack of timestamps on each message's production also leaves it open to replay assaults.

When all the anonymous in a certain scheme have been used, the plan often requires a vehicle to obtain a fresh set of anonymous [24], [25]. There's no reason to do this. When a car needs to change its anonymous, it can simply request a big pool of anonymous all at once, and then choose one at random. Our plan does exactly that. This, however, requires effective management of the aliases for a given vehicle. In order to accomplish this, the proposed FC-LSR scheme makes use of the efficient and secure MHT and MMPT data structures for saving and switching anonymously and resisting Sybil attacks. Additionally, MHT and MMPT data structures aid fog servers in efficiently authenticating vehicles for changing anonymously. Vehicles can use MHT to efficiently authenticate fog servers without certificates or CRLs thanks to MHT's assistance.

III. BACKGROUND

A. DESIGN ARCHITECTURE

The design architecture of the proposed FC-LSR scheme is depicted in its entirety in Figure 1. There are two levels: the top level includes of the Trusted Authority (TA) and the Regional Trusted Authorities (RTAs), while the lowest level consists of the Fifth-Generation-Base Stations (5G-BSs), fog servers and the Onboard Units (OBUs) that located each vehicle. Each RTA serves as a decentralised branch of the TA for its respective region.

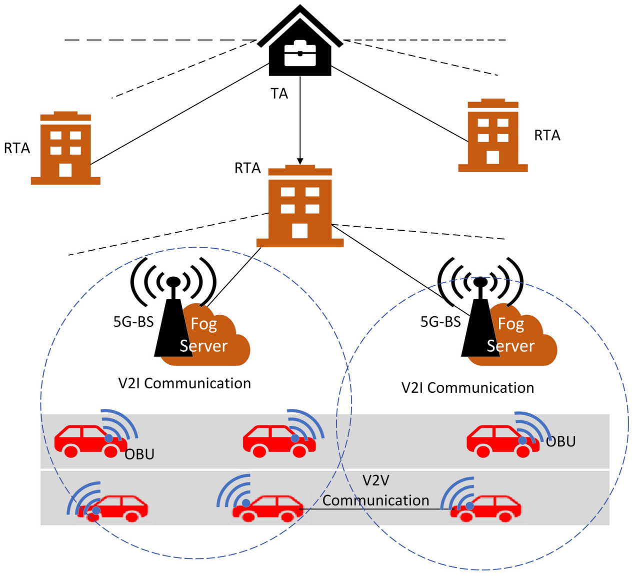


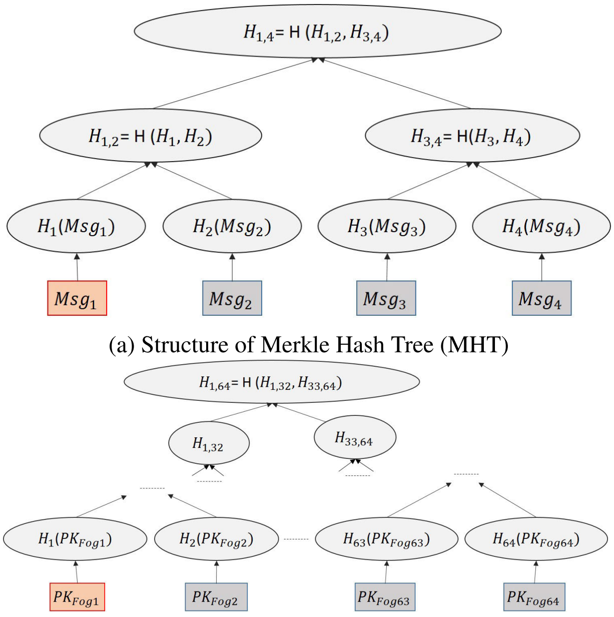
FIGURE 1. System model of proposal.

- Trusted Authority (TA): TA is fully trued component in the vehicle system and has huge resources in terms of storage and computation. Anonymous for vehicles are created and issued by the vehicle's home RTA at the time of registration.
- Regional Trusted Authorities (RTAs): The RTA generates an MHT containing the keys of public related to the fog servers that have been registered with it. The appropriate Missing Hash Values (MHVs) are subsequently distributed to each fog server in the region.
- Fifth-Generation-Base Stations (5G-BSs): 5G-BS is wireless infrastructure tha located along side road. The FC-LSR scheme assumes that 5G-BS that only forward the message between vehicles and fog servers and vice versa, which doesn't measurement any secret information.
- Fog Servers: Fog server is wireless node that located behind 5G-BSs to serve large number of vehicle and communicate with RTA. Each fog server has its own copy of the MHT and MMPT to keep track of all the aliases for each vehicle. For secure two-way communication between the fog server and each car within 5G-BS communication area, the fog server will distribute a symmetric key *SK* and group key *GK* to all vehicles in the area covered by 5G-BS. All fog servers with the same RTA have access to each other's public keys.
- Onboard Units (OBUs): OBU is wireless equipment installed each node for transceiver the messages among vehicles or fog servers via 5G-BSs. Each car knows both the public key (PK_{TA}) of the TA under which it is registered and the public key (PK_{RTA}P) of the RTA under which it is garaged. These are programmed into the OBU at the time of the vehicle's initial registration with its home RTA. The OBU in the car is programmed with these anonymous. The OBU in the vehicle is secure enough to keep a large value of anonymous safe. Taking into account the capabilities of modern hardware, this is not a significant limitation.

B. DESIGN GOAL

The major design purpose of the proposed FC-LSR scheme is to secure Sybil attacks and achieving the following requirements of privacy and security in 5G-based vehicular system.

- Message Authentication and Integrity: Message authentication, also known as data origin authentication, is a security feature that lets a recipient confirm the message's original sender and ensures the message's integrity during transit (data integrity) among vehicles.
- Anonymity Identity-privacy: The real identity of the vehicle cannot be retrieved by fog servers or any other vehicles. The real identity of the vehicle cannot be determined by a third party through analysis of intercepted communications.



(a) Structure of Merkle Hash Tree (MHT)

(b) The public key-based MHT of fog servers that are RTA-registered

FIGURE 2. Example of merkle hash tree (MHT).

- Unlinkability: Fog servers and bad cars can't use the messages a vehicle sends to track its location or determine what it's doing.
- Non-repudiation: There should be no way for the sender to claim they did not transmit information.
- Resistance to replay attacks: A replay attack is a malicious attempt to trick a network into thinking that an incident is actually taking place by retransmitting previously acquired data or duplicating it illegally.
- Resistance to Sybil attacks: is a method of attacking a service on the Internet by generating a large number of anonymous identities and then using those accounts to exert undue influence.
- Resistance to message injection attack: is the taking advantage of a flaw in a vehicular system brought on by processing incorrect data. An attacker can utilise the injection to alter the behaviour of a vehicular network that is susceptible to code injection.

C. FOUNDATION OF MERKLE HASH TREE (MHT)

A Merkle Hash Tree (MHT) [26] uses a hash [27]-established tree structure to ensure the integrity of information in a big information structure. Each leaf node in an MHT holds information, whereas all other nodes store their children's hashes.

In Figure 2a, we see an example of an MHT with four leaf nodes. Leaf nodes are where data are stored, whereas values in other nodes are calculated using a hash of the offspring of that node. We just require the relative Missing Hash Values (MHVs) of MHT (H_2, $H_{3,4}$) and the root value $H_{1,4}$ to show the integrity of Data1 in Figure 2a. Recalculating the root hash value with the MHVs involves first computing $H_{1,2} = \text{H}(\text{H}(Msg_1\ ), H_2)$, and then computing $H'_{1,4} = \text{H}(H_{1,2}, H_{3,4})$. If the result of the calculation, $H'_{1,4}$, is the same as the original root value, $H_{1,4}$, then Data1 can be trusted.

Each RTA builds an MHT that includes the public keys of all fog servers that are registered to it. Figure 2b shows an instance of an MHT made up of public keys for 64 fog servers enrolled under an RTA. The MHT is structured so that each leaf node keeps the public key of a fog server enrolled with the RTA, and each non-leaf node holds the offspring of the hash. Each RTA communicates the following to all fog servers in its zone [28]: (1) the TA's signature on its own public key; (2) the RTA's signature on the MHT's root value; and (3) the MHVs (explained above) that correspond to nodes in path of authentication of that fog server's public key.

TABLE 1. Matched fog servers at missing hash values (MHVs).

Fog_i	MHVs
Fog_1	H_2, $H_{3,4}$, $H_{5,8}$, $H_{9,16}$, $H_{17,32}$, $H_{33,64}$
Fog_2	H_1, $H_{3,4}$, $H_{5,8}$, $H_{9,16}$, $H_{17,32}$, $H_{33,64}$
Fog_3	H_4, $H_{1,2}$, $H_{5,8}$, $H_{9,16}$, $H_{17,32}$, $H_{33,64}$
....	....
Fog_{33}	H_{34}, $H_{35,36}$, $H_{37,40}$, $H_{41,48}$, $H_{49,64}$, $H_{1,32}$
....	....
Fog_{64}	H_{63}, $H_{61,62}$, $H_{57,60}$, $H_{49,56}$, $H_{33,48}$, $H_{1,32}$

The public keys of the various fog servers that have been registered with an RTA are shown in Table 1, along with their matching MHVs. When an RTA builds or reconstructs the MHT (when a fog server is added or removed, or when a compromised fog server is discovered), it communicates the time at which the MHT's root was generated (T^{mht}_{Root}) to the TA. To identify malicious fog servers or automobiles, an RTA can employ either previously developed algorithms [29], [30] or brand-new algorithms. The TA updates all RTAs with the current value of (T^{mht}_{Root}, and each RTA in turn updates all fog servers within its region. Fog servers also send the information out to nearby vehicles. Let's pretend Fog_p is linked to RTA_x and Fog_q is associated with RTA_y. When a new Fog_r is introduced to the system under RTA_x, a fresh MHT root is created for the system and the timestamp of the MHT root's creation is sent to the TA as the $T^{mht}_{Root_x}$. Also, if RTA_y determines that Fog_q is malicious, it will remove the public key from the MHT and recreate the MHT. RTA_y additionally transmits the $T^{mht}_{Root_y}$ timestamp, which is the time at which the root MHT was generated, to the TA. The TA will check $T^{mht}_{Root_x}$ and $T^{mht}_{Root_y}$ and only send the more recent timestamp to the other RTAs. In the case where $T^{mht}_{Root_x}$ and $T^{mht}_{Root_y}$ are identical, a random one will be chosen for transmission. Each RTA updates its own timestamp and broadcasts it to its associated fog server, so that all cars can keep accurate time. When an RTA detects a new or malicious fog server, it updates the MHT of the public keys corresponding to those fog servers, the root amount, and the root reproduction timestamp. This means that the only thing that changes at every other RTA is the MHT's root generation timestamp, and not the values themselves. When a car drives under a different fog server, it checks the difference between the current time, $T^{mht}_{Root_y}$, and the one that the fog server transmits, $T^{mht}_{Root_n}$. The car will not accept the connection request from that fog server if $T^{mht}_{Root_n} < T^{mht}_{Root_y}$. Fog servers are less vulnerable because of their stability and permanence. As a result, these transmissions are extremely rare. Thus, the proposed FC-LRS scheme offers a practical means of cancelling an fog server without the need for a CRL database.

D. FOUNDATION OF MODIFIED MERKLE HASH TREE (MMHT)

Modified Merkle Patricia Trie (MMPT) is an optimisation of Merkle Tree and Patricia Trie tailored to Ethereum's specific needs [31]. The time required to perform an insert, lookup, or delete operation in an MMPT is exponentially worse than log(n), where n is the number of leaf nodes in the tree. The fictitious names for cars are stored in an MMPT. All MMPT nodes are represented by a set of keys and values [32]. In an MMPT, there are three distinct kinds of nodes.

- Node of Leaf: There is no parent node for a leaf node. Nodes are classified by their prefixes, with prefix 2 designating a leaf node. Whether or not a given pseudonym is in use by the vehicle is indicated by its status (1 or 0), which is stored in each leaf node as a (key, value) pair (anonymous, status).
- Node of Branch: The number 1 denotes a node in a branch. There is a maximum of 16 child nodes that a branch node can have. These represent the hexadecimal values 0 through f.
- Node of Extension: Prefix 0 is used for extension nodes. It's like a streamlined version of a branch node, with a pointer to the following node and a partial path (shared nibble) that lets us skip forward.

In order to securely store vehicle authentication certificates in BPPA, MMPT is integrated with traditional blockchain [33]. Each fog server in the proposed FC-LSR uses a combination of a master hash table (MHT) and a master password table (MMPT), as shown in Figure 3, to save and achieve vehicle anonymous for efficient authentication with privacy-preserving. Public vehicle key (PK_v), set of anonymous ($AID_1, \ldots, AID_n$), and matching MHVs are all stored in a database that is updated and maintained by each fog server. The MHT MHVs are used by fog servers to check for the existence or non-attendance of the alias in the MMPT. Vehicle aliases and the most up-to-date active/inactive status are saved in each MMPT. By using the MMPT lookup method, an fog server can quickly verify and update the status of a given vehicle alias.

IV. THE PROPOSED FC-LSR SCHEME

To access 5G-enabled vehicular networks, each vehicle must first provide its true *TID* value to its local RTA. During the automobile registration process, the home RTA creates and issues a pool of anonymous. At the time of registration, the

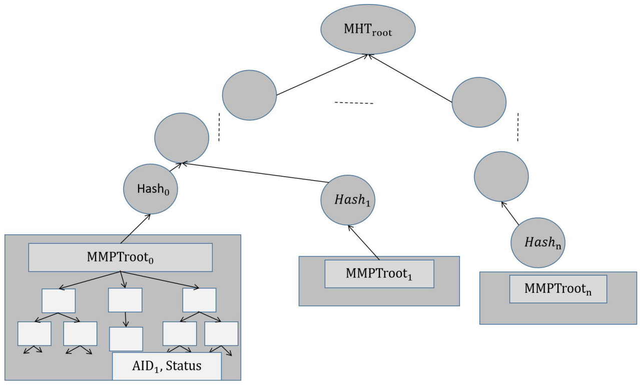


FIGURE 3. Vehicle anonymous storage using mmpt and merklel hash tree.

OBU is programmed with the vehicle's pair(public/private keys), the set of anonymous, and an first anonymous signed by the vehicle's home RTA. As an additional security measure, RTAs use a protected protocol like Transport Layer Security (TLS) to transmit the enrolled uses's pseudonyms to all fog servers in its territory via 5G-BS. To efficiently handle and authenticate vehicle anonymously, fog servers keep an MHT mixed with MMPT. A vehicle utilizes the credentials in the fog server's beacon message to verify the fog server's public key upon its first post-registration visit to the area serviced by 5G-BS through the fog server. After the fog server's public key has been verified, the vehicle will provide its own public key and an initial anonymous that has been signed by the RTA it is registered with. After both the vehicle and the fog server have authenticated each other, the fog server will change the anonymous's expiration time and create a symmetric key to use for exchanging encrypted data. The fog server also creates a group key for V2V communication between all cars in its area. The fog server then uses a trusted transport layer protocol to send the vehicle the updated anonymous expiration time, symmetric key, and group key. fog servers help cars in their area make a new anonymous by giving each one a unique anonymous expiration time. When a car's existing anonymous's validity time runs out, it contacts its fog server to request a new anonymous from the pool provided by the home RTA during first registration. This method of evading vehicle tracking involves increasing the rate at which pseudonyms are used. Figure 4 depicts the steps involved in a verified communication.

A. ANONYMOUS DISTRIBUTION PHASE

The primary goal of this phase is for RTAs to establish anonymity that can be utilised by any vehicles enrolled with them.

- During registration, each vehicle V_i obtains a legitimate driver's license from its local RTA.
- After registering a vehicle, the OBU is programmed with the owner's public-private key pair (PK_V, Pri_V) and a series of anonymous (AID_1,..., AID_n), with the first pseudonym being given the special designation $AID_{v_{first}}$ for communicating with fog servers as the first time, where $AID_{v_{first}} \in \{AID_1, \ldots, AID_n\}$.
- Local RTA assigns $(E(H(AID_{v_{first}})||t_{exp}), Pri_{RTA}$, where t_{exp} is the expired periodic of $AID_{v_{first}}$.
- Using a trusted transport layer protocol (TLS), the RTA communicates with all fog servers in its territory by broadcasting their $\{AID_1, \ldots, AID_n\}$, $AID_{v_{first}}$, and PK_v of vehicle V.
- When fog servers receive this information, they join the PK_v with the anonymous and store the whole thing in the MMPT along with their status. Except for $AID_{v_{first}}$, all other anonymity begin with a status of 0 (inactive). As a result, all fog servers inside an RTA share the anonymity of all vehicles within the RTA.

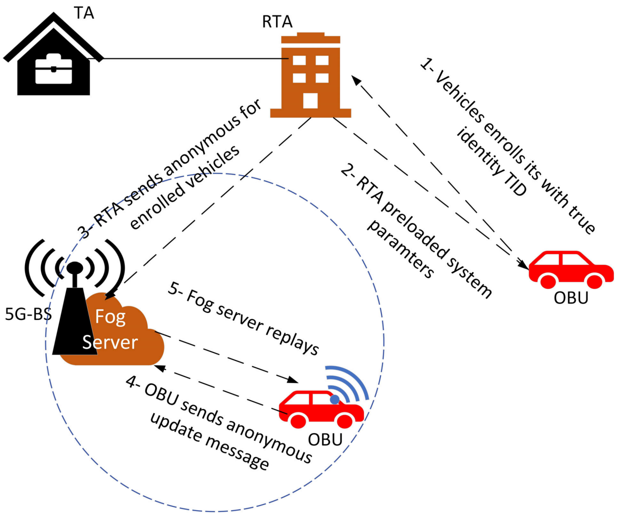

TA
RTA
1- Vehicles enrolls its with true identity TID
2- RTA preloaded system paramters
3- RTA sends anonymous for enrolled vehicles
5G-BS
Fog Server
5- Fog server replays
4- OBU sends anonymous update message
OBU
OBU

FIGURE 4. The proposed FC-LSR scheme.

B. JOINING PHASE

- Vehicle V receives the beacon message from the fog server, which includes the fog server's true ID TID_{Fog}, public key PK_{Fog}, PK_{RTA} signed by TA $PK_{RTA(signbyTA)}$, root value of the MHT signed by RTA $root_{signbyRTA}$ (where $root_{signbyRTA}$ contains (MHT root||signature of RSA$||T_{mhtRoot}$)), MHVs corresponding to the fog server's public key PK_{Fog}, and timestamp ts.
- The fog server beacon message's freshness is verified using ts. Then, vehicle V checks that the TA and RTA are legitimately signed. A vehicle is able to travel through many RTA zones. Note that it doesnt mandate that drivers keep every RTA's public key in their cars. The proposed FC-LSR scheme just needs vehicle V to keep the PK_{TA} in order to retrieve the PK_{Fog}, which may then be used to validate the fog server's public key.
- After confirming PK_{TA} and PK_{Fog}, vehicle V checks the $T_{mhtRoot}$ value in the beacon message against the previously recorded value. If the value of $T_{mhtRoot}$ in

the beacon message is larger than or equal to the value previously saved, the vehicle will recalculate the root of MHT based on the MHVs and the hash value of the public key PK_{Fog} of the sender fog server. The root value of MHT is then compared by V with the one it has just calculated. PK_{Fog} is legitimate if and only if the two values are the same.

- After verifying the fog server's identity, vehicle V relays the following transmission to it: $(E(AID_{v_{first}}, (E(H(AID_{v_{first}})t_{exp}), Pri_{RTA}), PK_{v}, ts), PK_{Fog})$, where $(E(H(AID_{v_{first}})t_{exp}), Pri_{RTA})$ is the first anonymous of vehicle signed by its local RTA.
- When fog server receives the preceding message, it checks the received ts to ensure the message is current. The RTA's signature is then checked by fog server. The t_{exp}, or time until anonymous expiration, is then retrieved. If t_{exp} is correct, then the initial anonymous $(AID_{v_{first}}$ is hashed and compared to the hash value H$((AID_{v_{first}})$ obtained. If the hash values are the same, the $(AID_{v_{first}}$ status in the MMPT is set to 1 and the fog server appends the public key of the vehicle PK_{V} to the $(AID_{v_{first}}$. $(AID_{v_{first}}$ has a new expiration date established by fog server, and the document has been signed.
- The fog server creates a symmetric key SK for use in encrypting and decrypting communications between the vehicle V and the fog server. After that, the following data is transmitted to the vehicle V: $(E(TID_{Fog}, (E(H((AID_{v_{first}})t_{new}), Pri_{Fog}), SK, Gk, ts), PK_{V})$, where $(E(H(AID_{v_{first}})\, t_{new}), Pri_{Fog})$ is the first anonymity with new expired periodic signed by the fog server and GK is the group key to be utilized by all vehicles registered by the same fog server.
- Vehicles that are part of an fog server can securely communicate with one another by using the group key Gk. For fog server-signed messages, a vehicle appends its current anonymity AID_{Vcurr} $(E(H(AID_{Vcurr})t_{exp}), Pri_{Fog})$ to the message m before broadcasting it to other vehicles.
- In order to resist replay assaults, it also appends a timestamp ts to messages generated by the system. When a vehicle needs to send a message m to other vehicles in the area covered by the current fog server, it encrypts m in the following way: $(E(AID_{Vcurr}, (E(H(AID_{Vcurr})||t_{new}, Pri_{Fog}, m, ts), GK)$.
- By comparing the received H$AID_{Vcurr})$ to the computed hash of received AID_{Vcurr}, the recipients can determine whether or not the message they received was sent before or after the current anonymity expired periodic t_{new}. If both checks pass, then the received message can be trusted. If this is not the case, the message is ignored by the receiving cars.

C. UPDATING STATUS ANONYMOUS OF VEHICLE PHASE

For security reasons, it is recommended that each vehicle periodically switch between anonymous. Anonymous should be changed at least once every five minutes, as per the European standard ETSI TS 102 867 [34] and once every 120 seconds or after one km of travel, whichever comes first. The American standard SAE J2735 [35] supports the latter. It's generally unnecessary to use a different anonymous every few minutes while a car is parked. In order to meet the requirements of the American SAE J2735 standard, a vehicle needs 720 anonymous per 24 hours and 262,800 every year. We presume that the OBU in the proposed FC-LSR scheme's car has a large enough cache of anonymity that the vehicle won't have to recycle for at least a year. Each anonymizing token is 16 bytes in size. To keep track of all of its anonymity, a car needs about 4 MB of space. For the sake of argument, let's say that the cars' existing hardware allows for sufficient storing of its anonymity.

- In the proposed FC-LSR scheme, fog servers provide assistance to nearby vehicles in changing anonymous by tagging each one with an expiration time. A car's current anonymity will need to be updated at the end of the given time period.
- After the allotted period has passed, the car will contact its fog server to have a new anonymous assigned to it from the pool provided by the home RTA during initial registration. Since fog servers are assumed to have more robust computational and storage capabilities than vehicles, we expect them to efficiently compute each request message.
- All cars in the fog server's area must update their anonymous at the time specified by the fog server. As a result, the possibility of linking a new anonymous to an old one is reduced when cars within the same fog server's region all change their anonymity at the same time.
- We suppose that the TA, RTAs, fog servers, and vehicles' (OBUs) clocks are only somewhat in sync with one another. If a vehicle's current anonymous AID_{Vcurr} is about to expire, it will choose a new anonymous AID_{Vcurr} at random from the pool of anonymous given to it and send a secure message to the fog server letting it know which anonymous it has chosen. The fog server then appends the new anonymous to the vehicle's public key PK_{v} together with AID_{Vcurr} and AID_{Vnew} in order to access the vehicle's MMPT. After verifying the message's authenticity, fog server makes the v AID_{Vcurr} and AID_{Vnew} MMPT statuses of 0 and 1, respectively. The fog server also transmits vehicle V an updated TID_{V} expiration date of t' new for AID_{Vnew}.

D. HANDOVER PHASE

Whenever a vehicle V travels from an area serviced by a fog server Fog_{i} via 5G-BS to an area serviced by a fog server Fog_{j} via another 5G-BS, vehicle V must first confirm the validity of the Fog_{j} as follows.

- To verify its identity before initiating contact with Fog_{j}, vehicle V sends the following message: $(E(AID_{Vcurr})||t_{new}, Pri_{Fog_{i}}), PK_{Fog_{j}})$. There are two possible scenarios.

  - Scenarios (1): When Fog_j receives the aforesaid message, it checks the message's validity and the Fog_i's signature by using the ts it received. Fog_j is registered with V's home RTA. If the check is good, Fog_j confirms the validity of the V's current anonymous, AID_{Vcurr}.
  - Scenarios (2): The service area of V's home RTA does not include Fog_j. The Fog_j uses ts to determine if the received message is still current. Assuming that other fog servers registered under the same RTA also know each other's public keys, Fog_j will deliver the received message to its own RTA. Then, the Fog_i local RTA exchanges information with the V home RTA to obtain V's public key PK_v, as well as the Fog_i public key PK_{Fog_i}. Using a trusted transport such as TLS, Fog_j's primary RTA communicates with all other fog servers in its area to distribute the necessary credentials.
- Fog server Fog_j validates V's hash value after receiving Fog_i's public key. Then, Fog_j appends the status and the set of V anonymous formed by appending PK_v to the end of the MMPT.
- After verifying V's identity, Fog_j updates AID_{Vcurr} to a new expired periodic of t' new and notifies V of the change. $(E(TID_{Vcurr})||t'_{new})$, $Pri_{Fog_j})$, SK', GK', $ts)$, $PK_v)$, where GK' is the group key shared by all authorized vehicles in the region of Fog_j and SK' is the shared symmetric key between V and Fog_j, and ts is the time stamp.

V. SECURITY ANALYSIS

This section analyses the security and privacy requirements for the proposed FC-LSR scheme as follows.

- Message Authentication and Integrity: The FC-LSR scheme requires a vehicle V and fog server to verify each other's identities before exchanging data. The root value of the MHT is recalculated and compared with the received $root_{signbyRTA}$ after the vehicle obtains the Missing Hash Values (MHVs), MHT root signed by RTA $root_{signbyRTA}$, public key of RTA signed by TA $PK_{RTAsignbyTA}$, and public key of the fog server PK_{Fog}. PK_{Fog} is legitimate if and only if the two values are the same. The vehicle then transmits a message bearing its initial anonymous AID_{Vfirst} and the RTA's signature, as well as the anonymous expired periodic $E((H(AID_{Vfirst})t_{exp}), Pri_{RTA})$. The fog server then compares its calculated hash of the received AID_{Vfirst} with the received hash value H(AID_{Vfirst}). If these two hashes are the same, fog server will search them up in the MMPT and make AID_{Vfirst} active. Following successful two-way authentication, the fog server will transmit a symmetric key SK and a group key GK to the car. All cars authenticated by the same fog server utilise the group key GK to communicate securely with one another. Since the group key GK is being used by all cars under an fog server, we don't have to worry about forward and backward secrecy. The group key is distributed to all vehicles in the region authenticated by the fog server.
- Anonymity Identity-privacy: If a sender always employs an anonymity, the recipients will never learn who the sender really is. Temporary credentials are used for sender authentication at the receiving end. When communicating using the proposed FC-LSR scheme, cars do so under a anonymity and with an associated time limit. Based on the anonymity and its expired period, receivers verify the sender's vehicle. No one ever refers to a car by its true name in a message. Only the RTA has access to the vehicle's true identification. Conditional privacy is maintained because only the car's local RTA can resolve the anonymity to the true identify of the vehicle.
- Unlinkability: For communications to be unlinkable, an adversary must be unable to correlate two anonymous sends from the same vehicle. After signing up for the proposed FC-LSR scheme, vehicles use their first anonymity AID_{Vfirst} to authenticate with the first fog server they come across. The fog server will change AID_{Vfirst}'s expired periodic to t_{new} at that point. In order to use a new anonymity from the pool of anonymous allotted to it after the current one expires, vehicle V must interact with the fog server using the symmetric key SK established between the vehicle and fog server during the mutual authentication procedure. By making the anonymity expiration time the same for all cars in its region, fog server makes it easier for them to change their anonymous regularly and in unison. Due to the fact that vehicles change anonymous simultaneously, the proposed FC-LSR scheme lessens the likelihood that two communications delivered by the same vehicle under different anonymous can be linked.
- Non-repudiation: A vehicle's fog server signs off on its communications with the anonymous's expired periodic, $E((H(AID_{Vcurr})t_{new}), Pri_{Fog})$, and the vehicle's current anonymous, AID_{Vcurr}, and its hash, AID_{VcurrH}, in the proposed FC-LSR scheme. The fog server recipient must first confirm the authenticity of the signature. Then, the time remaining on the anonymous is examined. For verification, it compares the received $H(AID_{Vcurr})$ with the computed hash of the received anonymous. Having identical hash values verifies the legitimacy of the sender. Since a vehicle utilises a pre-registered anonymous from its cache to send and receive messages, it cannot claim that the communications it sends were not sent by it. The fog server's signature is also impossible to fabricate, so that's another plus.
- Resistance to replay attacks: To prevent replay attacks, the proposed FC-LSR scheme encrypts not only the message data but also the timestamp ts used to generate the message. In the proposed FC-LSR scheme,

it assumes that the clocks of the TA, RTAs, fog servers, and vehicles are only roughly synchronised (something that can be done with GPS). By including *ts*, all parties are able to determine if the message is recent enough to prevent a replay attack.

- Resistance to Sybil attacks: When a malevolent vehicle simultaneously assumes the identities of many cars using different anonymous, this is called a Sybil assault. That's why it's important to put restrictions on how long a vehicle may operate under a given alias and how many anonymous it can employ at once. In the proposed FC-LSR scheme, the RTA signs one initial anonymous and the anonymous expired time $E((H(AID_{Vfirst})t_{exp}), Pri_{RTA})$ into the OBU of each vehicle. This initial anonymity is used for authentication whenever a registered vehicle from an RTA enters the territory of an fog server via 5G-BS. The fog server updates the vehicle's AID_{Vfirst} with a new expired time, t_{new}. When the t_{new} is ready to time out, the car contacts the fog server to have a fresh anonymity assigned to it. The fog server then activates and signs the vehicle's new anonymity, along with the anonymity's expired time, $E((H(AID_{Vnew})t'_{new}), Pri_{Fog}$. Since only one anonymity of a vehicle can be active at any given moment in the proposed FC-LSR scheme, it is immune to Sybil attacks.
- Resistance to message injection attack: When a vehicle V registered with an RTA enters the territory of an fog server, the latter checks the authenticity of the signatures of the registering RTA ($PK_{RTAsignbyTA}$) and the originating RTA ($root_{signbyRTA}$) under the proposed FC-LSR scheme. Then, it checks if the MHT root value calculated from the MHVs contained in the beacon message matches the MHT root value signed by the RTA. If they are the same, the fog server is valid; otherwise, a message injection attack has been identified. Vehicle *V* delivers its first anonymous AID_{Vfirst} signed by its local RTA when the fog server has been verified, together with its expired time t_{exp}. The t_{exp} is checked, and then the RTA's signature is verified, by the receiver fog server. If t_{exp} is correct, then the received H(AID_{Vfirst}) is compared to the hash of the anonymous. A message injection attack is flagged if these two numbers don't match up. A malicious actor would need access to TA or RTA's private key in order to falsify their signature.

VI. PERFORMANCE EVALUATION

In the proposed FC-LSR scheme, the TA and RTA signatures are validated before the vehicle continues. Next, the vehicle uses the Missing Hash Values (MHVs) obtained from the fog server's beacon message to determine the root value of the MHT. Crypto++ 5.6.0 [36] on an Intel Core 2 1.83 GHz CPU running Windows Vista in 32-bit mode can verify an RSA 2048 signature in 0.16 milliseconds while computing a SHA-256 hash at a rate of 111 megabytes per second.

The proposed FC-LSR scheme's fog server authentication relies mostly on RSA signature verification due to the substantially reduced computation costs associated with hash function calculation. On the other hand, in the LIAP method proposed by Wang and Yuo [21], vehicles employ a linear search to verify their authenticity against the fog server certificate revocation list (RCRL). Overhead in RSU authentication is introduced by the NERA scheme's [23] use of bilinear pairing and Map-To-Point operations. Due to the fact that the ASPA protocol that proposed by Ali et al. [22] does not account for vehicle-based RSU authentication.

Consequently, Figure 5 contrasts the authentication overhead of the proposed FC-LSR scheme's fog servers with those RSUs-based of Wang and Yuo [21] and Bayat et al. [23].

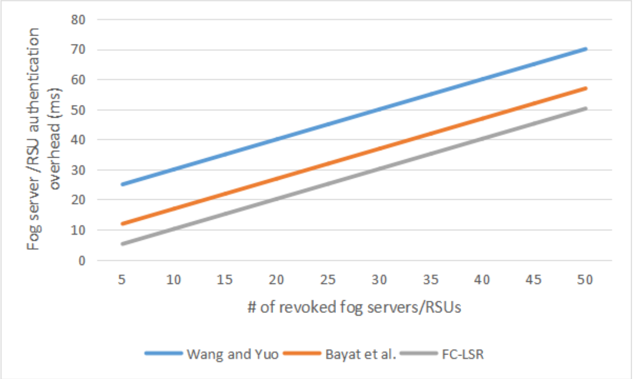


FIGURE 5. Comparison of fog Servers/RSUs authentication overhead.

The cost of authenticating RSUs in LIAP rises sharply as the proportion of revoked RSUs rises. Instead, the cost of authenticating RSUs is minimal in NERA and nearly nonexistent in fog server of the proposed FC-LSR scheme. When the number of revoked RSUs exceeds 30, Figure 5 demonstrates that the authentication overhead under LIAP is nearly three times as great as the proposed FC-LSR scheme.

In the proposed FC-LSR scheme, fog server initially uses its private key Pri_{Fog} to decrypt a message sent by a vehicle. The RTA signature is then checked for authenticity. After that, it combines the vehicle's public key with the vehicle's original anonymous and queries the MMPT. After decrypting the vehicle's message, RSU in Wang and Yuo [21] and Bayat et al. [23] both consult the Vehicle Certificate Revocation List (VCRL). The next step in the authentication process involves confirming the CA's signature on the vehicle's security document. Overhead for signature verification in Wang and Yuo [21] and Bayat et al. [23] with bilinear pairing is $T_{mtp}+T_{mul}+3T_{par}$, where T_{mul} stands for the time required to do a single-point multiplication ($T_{mul} = 17.789$ ms), T_{mtp} stands for the time required to perform a Map-To-Point hash operation (T_{mtp}=0.09 ms), and T_{par} is for the time required to execute a pairing operation (0.39 ms).

A vehicle in the ASPA protocol will utilise the first anonymous it was given by the Vehicle Manufacturing Company (VMC) to apply for a long-term certificate (LTC) from the CA. Before issuing a car an LTC, CA checks the CRL. Following this, the LTC is used to apply for a Pseudonym Certificate (PC) for the vehicle from the LTC Authority. The PC transmits a message to the Pseudonym Provider (PP), either directly or via the RSU. The Pseudonym Provider then transmits various pseudonyms to the car after confirming the vehicle's PC. Using the Digital Signature Algorithm (DSA), the signature verification time for this approach is only 0.37 ms [22].

In Figure 6, we see how the proposed FC-LSR scheme stacks up against Wang and Yuo [21], Bayat et al. [23], and Ali et al. [22] in terms of the time and effort required to verify a signature. Compared to Wang and Yuo [21], Bayat et al. [23], and Ali et al. [22], the proposed FC-LSR scheme is seen to have a much smaller signature verification overhead. In a scenario with 30 cars, for instance, the total time spent on signature verification increases to around 92 milliseconds (ms) with Wang and Yuo [21], Bayat et al. [23], and Ali et al. [22], but drops to just 4.8 ms with the proposed FC-LSR scheme.

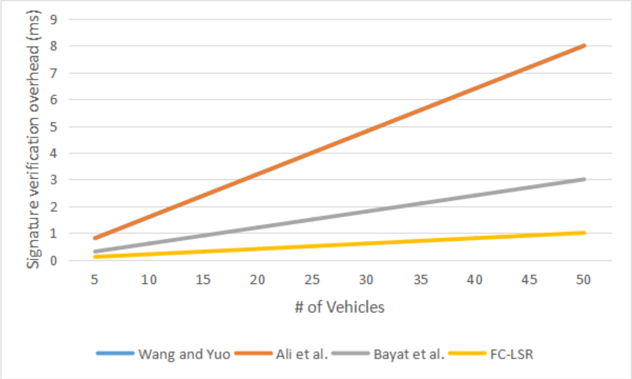


FIGURE 6. Comparison of signature verification overhead.

In the proposed FC-LSR scheme, the vehicle and fog server verify each other's identities without the need of certificates or CRLs. To recalculate the MHT root value, vehicles use the Missing Hash Values (MHVs) and Public key of the fog server PK_{Fog} received in the fog server's beacon message. After receiving this hash value, the car compares it to the root value of the MHT signed by the RTA ($root_{signbyRTA}$). The vehicle provides the RTA a signed copy of its first anonymity, the anonymity expired time $E((H(AID_{Vfirst})t_{exp}), Pri_{RTA})$, and the vehicle's public key PK_V after authenticating the fog server. Fog server first verifies the correctness of t_{exp}. Then, it checks if the received H(AID_{Vfirst}) is equal to the hash computed from the AID_{Vfirst} in the message. If the hash values are the same, then AID_{Vfirst} can be regarded correct. To the contrary, under both the Wang and Yuo [21] and Ali et al. [22] schemes, cars use long-term certificates for authentication. After that, the fog server or PPs look up the vehicles on the most up-to-date Certificate Revocation List (CRL) to make sure they are legitimate.

In the Bayat et al. [23] scheme, the TA removes the fraudulent registration and adds the legitimate registration number to the CRL. In these configurations, all entities in vehicular system have access to an up-to-date CRL of vehicles, which is maintained by the CA (Certificate Authority) or TA. The standard format for a CRL includes a header, the current date, the last time the CRL was updated, the next time the CRL will be updated, and a full list of revoked certificates that have been signed by the CA. Furthermore, as the number of entities grows, so does the size of CRL. Consequently, there is a high computational and communication cost associated with using CRLs for authentication. As an added security measure, the CA must regularly distribute CRLs. Thus, Fog servers or PPs face a substantial increase in communication overhead due to the Wang and Yuo [21], Bayat et al. [23], and Ali et al. [22] schemes.

VII. CONCLUSION

This paper proposes FC-LSR based on fog computing and 5G technology for vehicular networks. The proposed FC-LSR scheme uses Modified Merkle Patricia Trie (MMPT) combined with Merkle Hash Tree (MHT) for saving vehicles' anonymous and their efficient matching values of 'status of current' to resist Sybil attacks. The proposed FC-LCR use MHT to check if a vehicle is using a valid fog server. In addition, our solution eliminates the need for certificates during the authentication process. Fog servers aid automobiles in their territory with changing their anonymity simultaneously by providing each vehicle in their zone the same expired period. When a car's anonymity runs out, it reconnects with an fog server to pick a new one from the pool supplied by the car's home RTA during registration. The security part presents that the proposal method is achieving the requirements of privacy and security (message authentication and integrity, anonymity identity-privacy, unlinkability, and non-repudiation) and resisting security attacks (replay, Sybil, and message injection attacks). Finally, the proposed FC-LSR scheme is seen to have a much smaller signature verification overhead compared with related works.

DECLARATION OF COMPETING INTEREST

No conflict of interests exists regarding the publication of this article.

ACKNOWLEDGMENT

The authors thank the University of Jeddah for its technical and financial support.

REFERENCES

[1] J. Cui, J. Yu, H. Zhong, L. Wei, and L. Liu, "Chaotic map-based authentication scheme using physical unclonable function for internet of autonomous vehicle," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 3, pp. 3167–3181, Mar. 2023.

[2] X. Liu, Y. Wang, Y. Li, and H. Cao, "PTAP: A novel secure privacy-preserving & traceable authentication protocol in VANETs," *Comput. Netw.*, vol. 226, May 2023, Art. no. 109643.

[3] T. Yoshizawa, D. Singelée, J. T. Muehlberg, S. Delbruel, A. Taherkordi, D. Hughes, and B. Preneel, "A survey of security and privacy issues in V2X communication systems," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–36, Sep. 2023.

[4] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, Jan. 2018.

[5] J. Zhang, J. Cui, H. Zhong, I. Bolodurina, and L. Liu, "Intelligent drone-assisted anonymous authentication and key agreement for 5G/B5G vehicular ad-hoc networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 2982–2994, Oct. 2021.

[6] A. Boualouache and T. Engel, "A survey on machine learning-based misbehavior detection systems for 5G and beyond vehicular networks," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1128–1172, 2nd Quart., 2023.

[7] S. A. Asra, "Security issues of vehicular ad hoc networks (VANET): A systematic review," *TIERS Inf. Technol. J.*, vol. 3, no. 1, pp. 17–27, Jun. 2022.

[8] M. M. Hamdi, M. Dhafer, A. S. Mustafa, S. A. Rashid, A. J. Ahmed, and A. M. Shantaf, "Effect Sybil attack on security authentication service in VANET," in *Proc. Int. Congr. Hum.-Comput. Interact., Optim. Robotic Appl. (HORA)*, Jun. 2022, pp. 1–6.

[9] Q. Xie, Z. Ding, and P. Zheng, "Provably secure and anonymous V2I and V2V authentication protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 7318–7327, Jul. 2023.

[10] J. Zhang, Q. Zhang, X. Lu, and Y. Gan, "A novel privacy-preserving authentication protocol using bilinear pairings for the VANET environment," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–13, Jun. 2021.

[11] A. Imghoure, F. Omary, and A. El-Yahyaoui, "Schnorr-based conditional privacy-preserving authentication scheme with multisignature and batch verification in VANET," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100850.

[12] Y. Chen and J. Chen, "CPP-CLAS: Efficient and conditional privacy-preserving certificateless aggregate signature scheme for VANETs," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 10354–10365, Jun. 2022.

[13] I. Ali, Y. Chen, M. Faisal, M. Li, I. Ali, Y. Chen, M. Faisal, and M. Li, "Bilinear pairing-based signcryption scheme for secure heterogeneous vehicle-to-infrastructure communications in VANETs," in *Efficient and Provably Secure Schemes for Vehicular Ad-Hoc Networks*, 2022, pp. 147–173.

[14] S. Haider, G. Abbas, Z. H. Abbas, and F. Muhammad, "LWE-CPPA: A scheme for secure delivery of warning messages in VANETs," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 34, no. 3, p. 170, 2020.

[15] Y. Genc, N. Aytas, A. Akkoc, E. Afacan, and E. Yazgan, "ELCPAS: A new efficient lightweight certificateless conditional privacy preserving authentication scheme for IoV," *Veh. Commun.*, vol. 39, Feb. 2023, Art. no. 100549.

[16] A. M. Farooqi, M. A. Alam, S. I. Hassan, and S. M. Idrees, "A fog computing model for VANET to reduce latency and delay using 5G network in smart city transportation," *Appl. Sci.*, vol. 12, no. 4, p. 2083, Feb. 2022.

[17] S. Bouakkaz and F. Semchedine, "A certificateless ring signature scheme with batch verification for applications in VANET," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102669.

[18] F. Zhu, X. Yi, A. Abuadbba, I. Khalil, X. Huang, and F. Xu, "A security-enhanced certificateless conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 10, pp. 10456–10466, Oct. 2023.

[19] E. F. Cahyadi, T.-W. Su, C.-C. Yang, and M.-S. Hwang, "A certificateless aggregate signature scheme for security and privacy protection in VANET," *Int. J. Distrib. Sensor Netw.*, vol. 18, no. 5, May 2022, Art. no. 155013292210806.

[20] H. J. Nath and H. Choudhury, "A privacy-preserving mutual authentication scheme for group communication in VANET," *Comput. Commun.*, vol. 192, pp. 357–372, Aug. 2022.

[21] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, Nov. 2017.

[22] Q. E. Ali, N. Ahmad, A. H. Malik, W. U. Rehman, A. U. Din, and G. Ali, "ASPA: Advanced strong pseudonym based authentication in intelligent transport system," *PLoS ONE*, vol. 14, no. 8, Aug. 2019, Art. no. e0221213.

[23] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A new and efficient RSU based authentication scheme for VANETs," *Wireless Netw.*, vol. 26, no. 5, pp. 3083–3098, Jul. 2020.

[24] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET," *Comput. Netw.*, vol. 134, pp. 78–92, Apr. 2018.

[25] J. Li, K.-K.-R. Choo, W. Zhang, S. Kumari, J. J. P. C. Rodrigues, M. K. Khan, and D. Hogrefe, "EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *Veh. Commun.*, vol. 13, pp. 104–113, Jul. 2018.

[26] R. C. Merkle, "Protocols for public key cryptosystems," in *Proc. IEEE Symp. Secur. Privacy*, Apr. 1980, p. 122.

[27] R. Rivest, *The MD5 Message-Digest Algorithm*, document RFC1321, 1992.

[28] S. S. Moni and D. Manivannan, "An efficient RSU authentication scheme based on Merkle hash tree for VANETs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–7.

[29] N. V. Abhishek, M. N. Aman, T. J. Lim, and B. Sikdar, "DRiVe: Detecting malicious roadside units in the Internet of Vehicles with low latency data integrity," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3270–3281, Mar. 2022.

[30] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Enhancing misbehavior detection in 5G vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 9417–9430, Sep. 2020.

[31] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.

[32] S. S. Moni and D. Manivannan, "A scalable and distributed architecture for secure and privacy-preserving authentication and message dissemination in VANETs," *Internet Things*, vol. 13, Mar. 2021, Art. no. 100350.

[33] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2792–2801, Dec. 2019.

[34] *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*, Standard ETSI TS 102 941 V1.4.1, TC ITS, 2019.

[35] *Dedicated Short Range Communications (DSRC) Message Set Dictionary*, document D. SAE, J2735, Society of Automotive Engineers, DSRC Committee, 2009.

[36] W. Dai, "Crypto++ library 5.6. 0," Tech. Rep., 2009.

ABDULWAHAB ALI ALMAZROI received the M.Sc. degree in computer science from the University of Science, Malaysia, and the Ph.D. degree in computer science from Flinders University, Australia. He is currently an Associate Professor with the Department of Information Technology, College of Computing and Information Technology at Khulais, University of Jeddah, Saudi Arabia. His research interests include parallel computing, cloud computing, wireless communication, and data mining.

MONAGI H. ALKINANI received the Ph.D. degree in computer science from Western University, London, Canada, in 2017. In 2018, he joined the Deanship of Scientific Research, University of Jeddah, Saudi Arabia, where he was the Vice Dean of Research. At the Deanship, he has supervised research in the field of computer vision. Three years later, he was appointed as the Dean of the College of Computer Science and Engineering and became the Vice President of development and sustainability. He is a member of the Jeddah Computer Vision Team, where he supervises research activities and teaches image processing, artificial intelligence, and signal processing. He has been involved in many collaborative research projects financed by various instances, including the Ministry of Education and the University of Jeddah. In 2022, he was appointed as a member of the Alfaisal University's Board of Trustees by the Minister of Education.

MAHMOOD A. AL-SHAREEDA received the B.S. degree in communication Engineering from Iraq University College, the M.Sc. degree in information technology from the Islamic University of Lebanon (IUL), in 2018, and the Ph.D. degree in advanced computer network from Universiti Sains Malaysia (USM). He was a Postdoctoral Fellow with the National Advanced IPv6 Centre (NAv6), USM. He is currently an Assistant Professor of communication engineering with Iraq University College (IUC). His current research interests include network monitoring, the Internet of Things (IoT), vehicular ad hoc network (VANET) security, and IPv6 security.

MOHAMMED A. ALQARNI received the M.Sc. degree in computational sciences from the Department of Mathematics and Computer Science, Laurentian University, Sudbury, Canada, in 2012, and the Ph.D. degree in computer science from the Department of Computing and Software, McMaster University, Hamilton, Canada, 2016. He is an Associate Professor with the Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah. He researches various topics, including image processing, ad hoc networks, and the IoT.

ALAA ATALLAH ALMAZROEY is a Ph.D. student at the University of King Abdulaziz's Department of Computer Science. She was awarded her master's degree in 2020 from King Abdulaziz University in Jeddah, Saudi Arabia, from the Department of Computing and Information Technology. In 2013, she was awarded her bachelor's degree from the Department of Computer Science and Software Engineering at the University of Canterbury in Christchurch, New Zealand. Her areas of interest are artificial intelligence, Internet of Things, and computer vision.

TAREK GABER (Member, IEEE) is a Senior Lecturer of cybersecurity with the University of Salford, U.K., and an Associate Professor with Suez Canal University, Egypt. He is interested in many branches of CS, such as security, cloud computing, and deep learning.