International Journal of Innovative Research and Scientific Studies, 8(2) 2025, pages: 2865-2879

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Securing cross-domain authentication in vehicular ad hoc networks

Abdulaziz Zaid A. Aljarwan[1,2*], Md Asri Bin Ngadi[1]

[1]*Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia.*
[2]*Information Security Department, College of Computer Science and Engineering, University of Hail, Ha'il, Saudi Arabia.*

Corresponding author: Abdulaziz Zaid A. Aljarwan (*Email: abdulaziz.zaid84@gmail.com*)

Abstract

With the advancement of automotive telematics and communication technologies, intelligent transportation systems (ITS) have gradually come on stage, which enables the blooming of vehicular networks. The emerging fifth-generation (5G) mobile communication technology stands to deliver highly secure, low-latency wireless communication services. Furthermore, through fog computing architecture, 5G facilitates the collection of data on a global scale and controlling the entire network from a central location. However, this wireless communication model brings important difficulties for cross-domain authentication, privacy, and in turn monitoring harmful domains for the heterogeneous domains of a 5G-assisted vehicular network. To this end, this paper introduces a new cross-domain authentication solution employing blockchain and fog computing to mitigate these negative effects. The FCCA Protocol: This fog computing-enabled cross-domain authentication (FCCA) protocol establishes a secure authentication framework between vehicles and back-end fog servers, which guarantees accountability for possibly dangerous vehicles while protecting the private information of vehicle users. The FCCA protocol minimizes reliance on trusted authorities while offering a variety of important functions like cross-domain communication, single registration, authenticity of messages, privacy protection, anonymity, unlinkability, and traceability. We further proved that the FCCA protocol is resilient to hijacking, birthday collision, and man-in-the-middle attacks, which render other protocols vulnerable. Moreover, it is proven that, when including the costs of security, computation, communication, and energy, the FCCA protocol is the most cost-performance effective protocol.

Keywords: 5G, Blockchain technology, Cost-effective solutions, Cross-domain communication, Fog computing, Vehicular networks, Message authenticity.

DOI: 10.53894/ijirss.v8i2.5828
Funding: This study received no specific financial support.
History: Received: 26 February 2025 / **Revised:** 27 March 2025 / **Accepted:** 29 March **2025** / **Published:** 1 April 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: Both authors contributed equally to the conception and design of the study. Both authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

As urbanization continues to expand at a rapid pace, the concept of the ”smart city” has gained widespread interest from researchers and business leaders alike. Within the next 10–20 years, the number of vehicles on the planet is expected to double, to 2 billion [1, 2]. The development of vehicular ad-hoc networks (VANETs) allows for a more relaxed and stress-free time spent behind the wheel. To encourage cooperation among vehicles and share valuable driving information via the dedicated short-range communication (DSRC) radio, VANETs establish two types of communications: vehicle-to-infrastructure (V2I) communication and vehicle-to-vehicle (V2V) communication [3-6]. Because it uses fewer public resources and decreases road accidents and congestion, it also contributes to a more environmentally friendly way of transportation [7, 8].

Since 5G is the latest generation of wireless networking, its adoption in vehicular networks is driven by its vast capabilities, which include enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC) and massive machine-type communication (mMTC) as specified by the 3rd Generation Partnership Project (3GPP technical specifications: 3GPP TS 22.261 and 3GPP TS 23.501). The above features make sure that data delivery is timely, latency is minimal and connections are maintained efficiently thus making 5G a great candidate for supporting intelligent transportation systems (ITS) and vehicular communication applications [9, 10].

To improve driver safety and manage more unpredictable traffic patterns, transportation systems in several nations have lately undertaken significant deployments of five-generation (5G) technology [11, 12] and fog computing [13-15]. Through the use of wireless devices mounted on vehicles (termed onboard units, or OBUs), intelligent transportation systems (ITS) collect, process, and disseminate traffic data in the context of networked vehicles [16, 17].

Vehicles in fog computing-based 5G-assisted vehicular networks are highly mobile and unpredictable, making the entire system susceptible to a wide range of attacks. Security, privacy, and trustworthiness in this network are also important factors to consider. There are two main areas to focus on to create a reliable vehicular communication network in light of the growing need for privacy and authentication in the automobile industry [18, 19]. First, in fog computing-based 5G-assisted vehicular networks, all messages must be broadcast and sent anonymously because of the sensitive nature of the information they carry (users’ location, license plate numbers, etc.). However, the veracity of forwarded messages cannot be confirmed if they have been sent anonymously. Fairly preventing the spread of fraudulent messages from internal vehicles is challenging. In addition to lowering transportation efficiency, these bogus alerts can disrupt driving behavior and lead to an accident [20]. Second, although most fog computing-based 5G-assisted vehicular networks research focuses on conditional privacy and authentication, this literature lacks effective authentication, adequate scalability, and sufficient distribution. Vehicle registration, authentication, and revocation are traditionally handled by a single entity [21, 22] making the system vulnerable to attacks such as data tampering, information leakage, and the spread of fake data. Another potential downside to fog computing-based 5G-assisted vehicular networks is the potential for a single point of failure in data storage due to the use of a centralized cloud server. As a result, sensitive information is exposed, such as the location of the vehicle and the contents of communications.

To supply the answers to the aforementioned problems requires a stable communication setting. Blockchain is the technology behind the decentralized digital currency Bitcoin [23-25]. In blockchain-based networks, this solution is new since each node manages its copy of the system’s database. The blockchain can help fog computing-based 5G-assisted vehicular blockchain networks develop a reliable infrastructure for sharing data.

With its tamper-proof and decentralized qualities, the immutable and unforgeable ledger will record all participants’ actions, identity authentications, and broadcasted messages.

Therefore, this paper proposes fog computing-based cross-domain authentication called FCCA protocol for 5G-assisted vehicular blockchain networks. Using a brief group signature mechanism, FCCA may both register a temporary public key for use in cross-domain communication and realize conditional privacy protection communication within a single domain. To store transdomain vehicles’ temporary public keys that have been confirmed by miners, the blockchain is seen as a public and decentralized database. Temporary public keys verify the legitimacy of cross-domain access mechanisms. When compared to other blockchain-based efforts, the proposed approach is guaranteed to be highly efficient because the smart contract issued by the FCCA only contains two atomic operations. Hence, the main contribution of this paper is listed as follows.

Innovative FCCA Protocol for Secure and Decentralized Communication: In this study, a fog computing-enabled cross-domain authentication (FCCA) mechanism is developed for 5G-assisted vehicular blockchain networks. It presents a secure approach to both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication using blockchain, reducing the need for reliance on a trusted authority in processing transactions while also holding responsible masquerading vehicles by recording their identity after signature verification through a short memory hashtable-based data structure along with user-sensitive information.

Comprehensive Security and Performance Efficiency: Specifically, we formally show that FCCA not only meets all these security requirements for in-band and out-of-band FPC message exchange, as mentioned earlier, but also provides multi-factor intra-communication single registration, which has never been done before. It can withstand security attacks, including replay, man-in-the-middle, birthday collisions, and hijacking. We also conducted an extensive performance evaluation to show that FCCA has better scalability and computational overheads with minimum energy consumption compared to existing protocols available.

- Scalability and Practical Implementation: The FCCA protocol was designed for scalability and practical deployment in real-world use cases. Business Model and Application: The protocol is suitable for largescale vehicular networks,

as well as employs blockchain technology with unique smart contracts while depending on the use of temporary public keys to develop a normal cross-domain access mechanism.

- Experimental Validation: We verify the security and performance of FCCA through extensive experiments and simulations, together with comparisons to its related works that demonstrate significant enhancements over them.

This paper's remaining sections are structured as follows: In Section 2, we cover the related work; in Section 3, we present the background of the proposal's framework; in Section 4, we describe the proposed FCCA protocol; in
Section 5, we put those results into practice with an emphasis on theoretical analysis and simulation; and in Section 6, we wrap things up.

2. Related Work

A compromise technology, the Conditional Privacy-Preserving Authentication Protocol (CPPA) [26] allows for the tracking of hostile actions while yet protecting the privacy of users. To solve security and privacy issues in vehicular systems, the first CPPA protocol [26] was presented by Raya and Hubaux, who relied on the existing public key infrastructure (PKI). Since then, many publications [27, 28] have proposed various improvements to the safety and effectiveness of the system. Identity (ID)-based CPPA protocol was proposed due to the high cost of certificate storage and administration. ID-based CPPA protocols [29-31] not only solve the problem of certificate management by widely disseminating the identity-related secret key (email, name, etc.). The CPPA protocol for VANETs proposed by Zhang, et al. [30] combines the tamper-proof device (TPD) and the Chinese remainder theorem (CRT). The possibility of key leaking was highlighted by Xiong, et al. [31] who suggested a more secure double-insurance CPPA protocol. To solve the problem of secret key escrow, Ali, et al. [32] recently developed a certificateless signature-based pairing-free lightweight CPPA protocol for VANETs. Using the ring signature, Ali, et al. [32] proposed a new certificateless aggregate approach that provides conditional privacy protection while drastically cutting down on computational cost. Li, et al. [33] presented a lattice-based CPPA protocol with batch verification as a means of protecting against quantum attacks. The security, privacy, and efficiency concerns in VANETs are all much alleviated by current CPPA protocols, but the uncomfortable cross-domain authentication issue has been neglected.

For a fog-based vehicular system, Zhang, et al. [34] created a lightweight traffic route management technique. Using homomorphic encryption, automobiles in this approach broadcast their encrypted driving paths to a fog node. To manage traffic without having access to each vehicle's specific route information, the traffic management center (TMC) decrypts the accumulated ciphertexts sent from the fog node. In addition, the plan uses blockchain to maintain vehicle public keys. As a result, Cui, et al. [35] implemented the Internet of autonomous vehicles (IoAV) paradigm in their design to address the concerns raised by these restrictions. A trustworthy authentication mechanism is applicable in IoAV and is required to support secure autonomous vehicle (AV) remote control. A secure remote control system for AVs was proposed using their suggested chaotic map-based authenticated key agreement (CMAKA) mechanism. Users, data centers, and AVs all negotiate their unique session keys to create a safe channel of communication. Also, a physical unclonable function (PUF) was used to generate a secure private key for use in the authentication process.

This study Wang, et al. [36] explored the cloud-based road condition monitoring (RCoM) scenario, in which authorities need to keep tabs on the roads in real-time with the use of a cloud server so that they can provide appropriate reactions to emergencies in a timely fashion. When a dangerous situation occurs on the road, like a geological hazard or an accident, vehicles in the area can alert a cloud server hired by the authority. To solve these problems, Wang, et al. [36] introduced a robust RCoM scheme, provide a theoretical analysis of its performance, and show experimentally that it works as intended. Zhang, et al. [37] presented a blockchain-based conditional privacy-preserving authentication mechanism and architecture for the vehicular system. Vehicles can have their identities authenticated and their privacy protected without needing to rely on a trusted third-party authority. Vehicles suspected of being involved in illicit activity can also be tracked under the proposed scheme's terms. Smart contracts allow for the decentralized, dynamic revocation of unlawful vehicles, making the program efficient and scalable. To prove its viability, Zhang, et al. [37] implemented the scheme in an Ethereum test network and analyzed and evaluated its security and performance in great detail.

For mobile fog computing over 5G networks, Mohammed, et al. [38] proposed a new anonymous authentication technique called ANAA-Fog. Under the proposed ANAA-Fog approach, the temporary secret key used to validate digital signatures in each participating vehicle is produced by a fog server. Using the ProfVerif simulator, Mohammed, et al. [38] analyzed the ANAAFog scheme's signing procedure and showed that it is secure. This study also complied with privacy and security requirements such as the capacity to withstand security risks like forgery, replay, and man-in-the-middle attacks, as well as the ability to revoke or change information once it has been shared. Zhang and Zhao [39] offered a blockchain-based PKI identity management and authentication architecture to alleviate the burden on CAs of handling the entire digital certificate life cycle. With this in mind, to satisfy the general cross-domain needs, a trust chain based on smart contracts is being developed to replace the old certificate authority (CA) trust chain. This will allow for an effective avoidance of the communication burden produced by a large number of certificate transfers. To meet the security and privacy needs of the vehicular system, Shawky, et al. [40] presented a lightweight group signature mechanism based on symmetric key cryptography. In this topic, Shawky, et al. [40] looked at how well the strategy stands up to common forms of attack from the enemy. To create a decentralized authentication system, Wang, et al. [41] advocated for an edge computing method. To speed up the authentication process and cut down on verification time, the suggested design creates a decentralized certificate revocation list (CRL) administration system. To address the issue of unreliable authentication at the group's periphery, which originates from the distributed nature of the system, a transition zone was proposed by Wang, et al. [41]. To combat collusion in IoV, Chen, et al. [42] proposed a server-assisted attribute-based signature (ABS) with collusion resistance (SAABS-CR).

It makes use of server-assisted computation technologies to reduce the computational load on verifiers, and it is entirely resistant to collusion attacks between signers and between the signer and the aided server.

For bilinear groups, Feng, et al. [43] proposed a new privacy-preserving authentication protocol in which a registered vehicle signs a traffic-related message and transmits it to the neighboring Road-side Unit (RSU) together with its blinded certificate. Using an asynchronous zero-knowledge proof protocol, the RSU may verify the authenticity of the message without any outside help. As a result, compared to anonymous authentication methods, Feng, et al. [43]' protocol has lowered the computation time from O (n) to O (1) and the storage overhead from O (nk) to O (n).

2.1. Critical Analysis

The IEEE 802.11p standard (as surveyed by Ahmadvand, et al. [44]) supported low latency and high reliability for time/tasks specific safety applications usable in vehicular networks. Having said that, the standard itself does not provide specific methods for secure and private communications. It depends on extra layers of security, which may be prone to flaws and further complicate the system. Instead, the FCCA protocol includes network security and privacy as an integral part of communication. It provides mutual authentication and energy-efficient conditional privacy preservation by using group signatures and temporary public keys, features not natively supported in IEEE 802.11p. Additionally, the addition of blockchain technology ensures an immutable history record of authentication events making the system more attack-resistant such as against replay, man-in-the-middle, etc. To cope with the above challenges, Chen, et al. [45] proposed blockchain assisted privacy-preserving cross-domain authentication called BCGS for vehicular systems. In BCGS, the group signature system is employed to provide conditional privacy protection, and blockchain is utilized to provide trusted information sharing, which in turn supports cross-domain authentication across vehicles. The BCGS protocol is based on the roadside unit (RSU) that offers application programming interfaces for things like verifying signatures, passing along messages, retrieving transactions, and invoking smart contracts. However, since RSUs are responsible for processing and storing data, there will be an increase in transmission overhead and potential security risks. It is also expensive to deploy RSUs in widespread vehicle networks. It is challenging to apply the authentication methods developed for traditional VANETs to 5G-equipped vehicle networks. The 5G base station (5G-BS) is not engaged in the computation necessary for content sharing and does not require RSUs. As a result, this paper will propose fog computing-based cross-domain authentication called FCCA protocol for 5G-assisted vehicular blockchain networks. The FCCA protocol method is both safe and effective. 5G has the potential to better handle large-scale mobile vehicular communications with shorter time delays than existing VANETs based on the IEEE 802.11p standard. The FCCA protocol's fog computing vehicles not only boost the system's processing power but also lower the system's return pressure and improve the user's service experience by processing data locally at the vehicle terminal rather than sending it to the Trusted authority in the network's distant core.

3. Background

3.1. System Model

The FCCA protocol's system paradigm, depicted in Figure 1, entails many domains, each of which is composed of five roles: Trusted Authorities (TRAs), fog server, 5G-Base Station (5G-BS), OBUs, and the Blockchain itself. Both intra-domain authentication, in which all participants within the same domain communicate with one another, and cross-domain authentication, in which participants from different domains speak with one another, are fundamental to the authentication models. The primary roles of each organization are outlined below.

- TRAs: Each domain's TRA is an exceptionally powerful data storage and processing powerhouse. All aspects of member management, from registration to monitoring for malicious activity, are within its purview. In this setup, the TRA is where vehicles and fog servers get their secret keys to authenticate. Therefore, the TRA will produce secret keys for all members of the domain. Meanwhile, the TRA should monitor for harmful behavior in vehicles to stop them from sending out unwanted signals. For cross-domain communication, it's also necessary for the TRAs in various domains to work together to keep track of all the temporary certificates they issue.

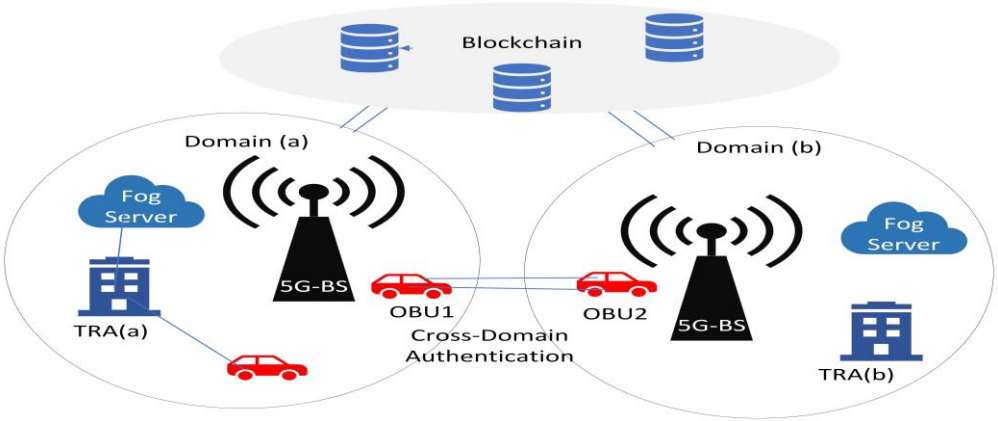

Figure 1.
System Model of the FCCA Protocol.

- 5G-Base Station (5G-BS): The 5G-BSs are stationary base stations set up at the side of the road. Its only use is as a bridge between automobiles, fog servers, and TRA, and it lacks both computing and storage capabilities. This is due to its flexibility in accommodating various forms of D2D interaction. Because 5G-BSs are physical devices, they are immune to attacks.
- Fog Server: The fog server is a piece of infrastructure located behind 5G-BS that facilitates interaction between several parties and a service provider. Mainly, it offers application programming interfaces for things like verifying signatures, passing along messages, retrieving transactions, and invoking smart contracts. In this scenario, we trust the fog serves only partially, believing that they will never intentionally break from the established protocol to steal sensitive data like user credentials.
- OBUs: The vehicle, which contains an OBU, is the network's primary communication hub. Communication between vehicles, fog servers, and TRAs is enabled through the OBU. The messages sent by the vehicle in some communication types must be verified by the recipient. Specifically, the receiver validates messages by utilizing the local public key if the sender and the recipient are members of the same domain. The temporary certificate is stored on the blockchain and is used by the receiver to verify messages. The OBU has a significant role in deploying the proposed fog computing-enabled cross-domain authentication (FCCA) protocol within the proposal system. A vehicle communication device (OBU) is necessary because it performs the management of cryptographic key generation, and secure message exchange among OBUs and fog servers. In the FCCA, OBUs carry out a generation of temporary public keys, the creation of group signatures, and verification of all incoming messages to secure communication in intra-domain and cross-domain cases. While its intended use-case within the OBU allows real-time authentication and preservation of privacy, this approach also results in less trust in central authorities compared to prior work which achieves better security for vehicular communications in 5G-enabled networks. The vehicles can manage their security and communication processes autonomously, thanks to the fact we embedded the FCCA protocol directly into the OBU.
- Blockchain: The blockchain is a distributed database managed by the TRAs and fog serves, and it stores the credentials used for cross-domain authentication registration (such as the temporary certificate). All nodes in the blockchain have access to the data because it is stored in the form of transactions. As a result, user registration and data retrieval are two of its primary features. In this case, any consortium blockchain (like Hyperledger) with smart contracts (like Ethereum) can be used to create an instance.

3.2. Design Objectives

FCCA protocol is aimed at providing a secure and efficient authentication framework for vehicular communication. The group signature mechanisms allow vehicles to authenticate in an anonymous way authenticating the authenticity. This allows for temporary public keys to be generated on a per-communication basis, which makes both replay attacks and message integrity cryptographically impractical. The adversary in the attacker model reads all exchanged messages carefully and tries to find any pattern, anomaly, or cryptographic weakness. It prevents the above-mentioned attacks by encrypting all data via lightweight cryptographic algorithms and using the decentralized nature of the blockchain network to validate the integrity of the data, through the use of FCCA protocol. The scaling, security, and interoperability aspects of the FCCA protocol led to the choosing of a blockchain to implement those functionalities. Not only does the blockchain need to support millions (if not billions) of transactions per day, it also needs to provide a secure method of validating data. And because the technology chosen is also compliant with existing vehicle communication protocols, it can be quickly adopted across a wide spread of vehicles. FCCA shows a significant improvement against conventional vehicular network attacks. More specifically, it uses group signatures to be resistant to Sybil attacks: each vehicle is allowed to obtain only valid signatures. Finally, replay and man-in-the-middle attacks are prevented through the use of blockchain and temporary public keys. The simulation results provide evidence for these claims, with existing protocols experiencing higher vulnerability rates than FCCA.

- Single registration: Each participant (e.g., vehicle, fog server) just needs to enroll his identification once, even if he or she will be communicating with recipients in multiple domains, thanks to this feature. It was obvious that this eliminated the need for the system to rely on intricate procedures for key distribution and management.
- Authenticity of Message: There are two primary components to this feature: message and identity legality. Not only does this guarantee that any tampered-with message would fail validation, but it also foils any attempts at impersonation by a hostile user.
- Privacy preservation: Vehicular systems are inherently open and dynamic, which raises the possibility that personal information regarding the vehicles' identities could be compromised during communication. Therefore, the verification procedure should not expose the vehicles' identities. In other words, an adversary who manages to intercept communications won't be able to figure out the genuine identity.
- Traceability: An efficient technique to resolve tracing issues in the event of malicious behavior is necessary to deter vehicles from abusing the privacy protection property. The trait enables reliable authorities (like police officers) to identify the true owner of the malevolent vehicle.
- Unlinkability: An attacker could try to learn private details by sifting through a large volume of communications. As a result, it is crucial to stop the enemy from associating any two communications sent by different vehicles.

- Cross-domain authentication: In real life, it is common for vehicles to need access to resources from beyond their domain, and for vehicles from other domains to exchange data with one another. Without relying on a governing body, this feature keeps all domain-to-domain communications safe and sound.
- Resistance to Other Attacks: A secure authentication in vehicular systems should also be able to withstand attacks such as replay attacks and man-in-the-middle attacks. The use of blockchain technology makes the system robust against hijacking assaults and birthday collisions.

4. The Proposed FCCA Protocol

This section describes the phases of the proposed FCCA protocol for 5G-assisted vehicular blockchain networks. Table 1 shows the math symbol and their definition. The proposed FCCA protocol mainly consists of the following phases.

Table 1.
Math Symbols and their Definition.

Math Symbol	Definition
TRA	Trusted Authority
Param	System Parameters
gsk_i	Group secret key, where *i* refers the index of the vehicle in Domain α
gpk_i	Group public key
IDij	Authentic Identity of fog server fog_j, where *j* refers the index of the vehicle in Domain β
m_v	The exchanged messages, where *v* refers a vehicle in general
T_1	The freshness timestamp
T_r	The received timestamp, where *r* indicates to a random value utilised for cryptographic operations
ΔT	The top broadcasting delay
k	Temporary secret key
SN	The message's serial number

4.1. Setup

This phase is responsible for issuing the public parameters and initializing the vehicular blockchain networks. The setup phase involves generating system parameters and initializing the vehicular blockchain networks as described in Algorithm 1.

Algorithm 1: Setup Phase

1: TRA generates system parameters $Param = \{P_1,P_2,G_1,G_2,G_T,q,e\}$
2: TRA selects group secret key $gsk_i = (r_i,x_i,a_i,b_i)$
3: TRA generates corresponding group public key $gpk_i = (Ri,Xi,Ai,Bi,g1i,g2i,g3i)$
4: TRA preloads public parameters $\{Param,(gpk_i)\}$ to all participating members
5: TRA securely saves group secret key gsk_i to each domain TRA_α
6: TRA initiates SC on the blockchain with peer TRAs

4.1.1. Issuing Parameters

The system parameter and domain parameter are generated in this phase by TRA. Each domain's unique parameters are included in the domain parameter. Given TRA_α indicates the *TRA* of i^{th} domain, where i= 1...N various domains controlled by various TRAs. It generates N unique group session keys (gsk_i) for N communicating vehicles in a group. Each gsk_i is unique by vehicle to insure reliable communication within the group and allow for authentication as well as message validation.

- TRA generates parameters-based group signature such as $Param = \{P1,P2,G1,G2,GT,q,e\}$, where
- TRA selects a group secret key $gsk_i = (r_i,x_i,a_i,b_i)$ and the corresponding group public key $gpk_i = (R_i,X_i,A_i,B_i,g_i^1,g_i^2,g_i^3)$.
- TRA preloads public parameters $\{Param,(gpk_i)\}$ to all participating
- TRA secretly saves group secret key gsk_i to each domain TRA_α.
- Assuming a reliable blockchain platform (e.g., Ethereum) offers smart contracts. Initiating the specified smart contracts on a blockchain requires N TRAs to become peer entities.

Where every member in the TRAs produces a unique signature and timestamp using an individual group session key (gsk_i). On the same timeline, even if we have two messages with a timestamp and signature based on another message it will never be identical as in every new message that is generated those signatures are in real-time and not static. The system constantly checks for malicious behavior that arises due to the nodes in TRAs. When a device is found to be untrusted, The TRA revokes its gsk_i to quarantine and stop any future communication

4.2. Enrollment Phase

This phase registers each component (i.e., fog server, vehicle) with its domain to obtain the signing key. The enrollment phase, detailed in Algorithm 2, registers each component with its domain to obtain the signing key.

- Fog server fog_j sends its authentic identity ID_l^j to TRA_α in order to enter the group as a member.

Algorithm 2 Enrollment Phase

1: Fog server fog_j sends its authentic identity ID_j^i to TRA_α
2: TRA_α generates group secret key $gsk_j^i = (s^i_j, D_j^i)$
3: TRA_α creates tag $tag_j^i = H(e(D_j^i, P_2))$
4: TRA_α uploads (gsk_j^i, tag_j^i) to blockchain
5: TRA_α returns gsk_j^i to fog_j through a secure channel

- Upon obtaining the request, TRA_α generates the group secret key $gsk_l^j = (s^j_i, D_l^j)$ and the tag $tag_l^j = H(e(D_l^j, P_2)$.
- TRA_α uploads (gsk_l^j, tag_l^j) to blockchain.
- TRA_α returns $gsk_i^j = (s_i^j, D_i^j)$ to the fog server fog_j through security channel.

The aforementioned procedure can also be used by other entities (such as vehicles) to establish their identities.

4.3. Intra-Domain Communication Phase

This stage is mostly concerned with intra-domain communication use cases, such as when a vehicle needs to communicate traffic information to other adjacent entities (such as another vehicle or a fog server). A sender takes the following action to establish their identity to send and receive messages. Intra-domain communication, highlighting the steps taken by the sender and recipient to ensure message authenticity.

- Once the signer is part of the α^{th} domain and in possession of the signing key gsk_i, then the system algorithm is used to generate a signature on the message-tuple = $(m_v||T_1)$, where T_1 and m_v are the freshness timestamp and the message, respectively.
- Sender creates a transmit message m according to $\{SN||Payload||Signature\ ||Timestamp\}$, where SN is the message's serial number, and Payload contains data on the vehicle's location, the road's condition, and so on.
- message M is transmitted from the sender to the recipient.

To verify the messages sent, the following process should be done.

- Vehicle V_i initially tests the freshness timestamp by verifying whether $|T_r - T_1| < \Delta T$ holds, where T_r is a received timestamp and ΔT is the top broadcasting delay. If not, vehicle V_i a rejects this message.
- Vehicle V_i a verifies the group signature δ_i^a by invoking Group-Verify algorithm. Once Group-Verify$(gpk_\alpha, \delta_i^\alpha, m) = 1$ holds, the message is legitimate and validated from the group member of the α^{th} domain.

For intra-domain communication, the sender and recipient follow the steps outlined in Algorithm 3.

4.4. Cross-Domain Communication Phase

Cross-domain communication scenarios, such as an α^{th} domain vehicle intending to convey traffic messages to a β^{th} domain vehicle, are the primary emphasis of this stage. Messages sent between vehicles/fog servers in separate domains cannot be encrypted using the intra-domain communication mode because these entities do not share the same public information (such as the group public key). Because of this, it implements blockchain and **Algorithm 3** Intra-Domain Communication Phase smart contracts to provide cross-domain communication.

1: Sender generates message-tuple $(m_v||T_1)$
2: Sender creates transmit message $M = \{SN||Payload||Signature||Timestamp\}$
3: Sender transmits message M to recipient
4: Recipient verifies timestamp by checking
$|T_r - T_1| < \Delta T$
5: if $|T_r - T_1| < \Delta T$ then
6: Recipient verifies group signature using
$Group\text{-}Verify(gpk_\alpha, \delta_\alpha^i, m)$
7: if Group-Verify = 1 then
8: Message is legitimate
9: else
10: Message is rejected
11: end if
12: else
13: Message is rejected
14: end if

Consider the case when a vehicle V_i an in α^{th}-domain wishes to communicate with another vehicle V_j in β^{th}-domain by sending them the message M. The following process should be done. Cross-domain communication, outlines the process of securely exchanging messages between vehicles from different domains. Per-vehicle generated ephemeral public/private key pairs are used to derive secret keys. The TRA validates those keys using cryptographic certificates. This ensures that only

authentic vehicles can participate in the communication session securely. The fog servers generate an invite which is sent to the other party so that they can authenticate and join the communication group. The TRA validates the identities of different fog servers(fog_j) by verifying his cryptographic proof and digital certificate. The fog server can only send identity (ID_j) to TRA_α and be invited to join the group after being
successfully verified.

- To enrol temporary public key, the vehicle V_i computes a group signature $\delta_i^\alpha = (D_1 = dP_1, D_2, D_3, D_4, d, u)$ and transmits the tuple *DUrequst*, $\delta_i^\alpha, T_1^* \text{ to } TRA_\alpha$ as a request of cross-domain, where D_1 will be enrolled as the temporary public key.
- After receiving a request, the TRA_α runs the Group-Verify algorithm to ensure that the timestamp and group signature is current. If yes,
  TRA_α invokes user CD Request in a smart contract to add the tuple $\{PID_v, \delta_i^\alpha, D_1\}$ to the blockchain, and then responds to V_i a with the index Tx_{id}. Keep in mind that PID_v is only a guise for the vehicle $V_i^{PID_v}$.
- Vehicle V_i^α must compute a signature using the temporary secret key k before it may connect with vehicle V_j^β. Here are the detailed procedures:
- Choose a randomly value $b \in [1, n-1]$ and calculate Q $(X_Q, Y_Q) = bP_1$, $R = X_Q$.
- Choose the freshness timestamp T_3 and issue $h = H(M)$ on message m_v, where $M = (m_v || T_3 || Tx_{id})$.
- Compute a public key signature (R,m) utilising the secret key k, where $m = b^{-1}(h + Rk)$.
- Collect the broadcasted message according to the format ($SN||Payload||\ n||P_1||P_K Signature||\ Tx_{id}||Timestamp$) and transmit it to V_j^β.
- It is a supposed that V_j^β receives the message from V_j^α at timestamp T_4, vehicle V_j^β executes the following points to verify V_j^α.
- Test the newness of the broadcasted message by verifying whether $|T_r - T_4| < \Delta T$ holds. If not, the data will be dropped.
- Query the temporary public key D_1 via the index Tx_{id} from the blockchain. If this occurs, it directly tests the signature (R,m) by utilizing D_1.
  Where, for verifying the messages, both timestamps and fresh values (nonces) are used. The combination of timestamps prevents replay, and the freshness values serve as additional security to ensure each message is unique.

Cross-domain communication is handled through the process illustrated in Algorithm 4."

Algorithm 4 Cross-Domain Communication Phase

1: Vehicle V_i^a computes group signature δ_α^i and transmits $DU_{request}, \delta_\alpha^i, T_1^* \text{ to } TRA_\alpha$
2: TRA_α runs Group-Verify algorithm to check signature and timestamp
3: if Group-Verify = 1 then
4: TRA_α invokes userCDRequest in smart contract to add ($PID_v, \delta_\alpha^i, D_1$) to blockchain
5: TRA_α responds to V_i^a with index *Txid*
6: end if
7: Vehicle V_α^i computes signature (R,m) using temporary secret key k
8: Vehicle V_α^i broadcasts message ($SN||Payload||n||P_1||PKSignature||Txid||Timestamp$)
9: Vehicle V_β^j verifies timestamp and retrieves temporary public key D_1
10: from blockchain using *Txid*
11: Vehicle V_β^j verifies signature (R,m) using D_1
12: if Signature is valid then
13: Message is legitimate
14: else
15: Message is rejected
16: end if

5. Results

To demonstrate FCCA's value, this section provides a thorough security evaluation and performance analysis in terms of the computational and communication overhead by comparing the FCCA protocol to the relevant techniques.

5.1. Security Evaluation

This section examines the robustness of the proposed FCCA protocol in light of the stated objectives in section 3.2.

- Single Registration: According to FCCA's definition, following the enrollment stage, the vehicle can be validated by fog servers or other valid group members, even if in cross-domain communication, because the TRA will have verified the vehicle's identification and result authentication information. Thus, the FCCA protocol satisfies the need for only a single registration.
- Authenticity of Message: When the verification process is complete, the vehicle (or fog server) can decide whether or not to accept the transmitted messages. To authenticate itself within its domain, a vehicle will utilise its private key to create a group signature that other vehicles will be able to verify. During the phase of cross-domain communication, the receiver checks the authenticity of the sender's signature using $R = X_Q -$ (mod n) and D_1. Guaranteed through the security of
  the signature, the message will fail verification if any alterations have been made. This enables the recipient to verify the authenticity of messages. An attacker needs to present a valid secret key in order to fake the signature of a legitimate vehicle. A legitimate secret key cannot be forged by an attacker without access to the group manager's secret key. Therefore, the attacker cannot use a fake signature to pose as a legitimate user.
- Privacy preservation: Anonymous authentication is provided by the group signature thanks to the anonymous property. Using the group's shared public key, the recipient can validate signatures generated by any member using the group's shared secret key. During authentication, the recipient learns just that the message sender is a member of the group and is not given any other information about the sender. The signature in cross-domain communication is what proves the user is who they say they are and doesn't leak any personal information. The FCCA protocol offers enhanced privacy protection because the communication process does not reveal the name of the vehicle and does not even employ a pseudonym.
- Unlinkability: The numbers $D_1 = dP_1$, $D_2 = wZ_i + dW, C3 = dP_1$, and $D_4 = r^{-1}$ V are all part of a signature and use a secret value d or w selected at random from Z_q. Two signatures from the same member of the group can be linked if it is established that values D_2 and C_2^* in the signatures share the same Z_i. But that's tough because the two values are completely random and can't be seen by anyone else in the group.
- Traceability: The identification data is registered on the blockchain as key-value pairs (e.g., PID[tag] = ID) during the enrollment stage. A user can notify TRA of this behavior when it discovers that a message
  is false. The TRA is always able to determine who the genuine signer is. If the signature $\delta = (D_1, D_2, D_3, D_4, d, u)$ is correct, the TRA can determine the signer's true identity by computing a tag, tag = H(e($D_2 - rD_1, v^{-1}D_4$)).
- Cross-Domain Communication: The vehicle has a temporary public secret key pair (*sk*, *PK*) once the cross-domain enrollment is complete; *PK* is the first component $D_1 = dP_1$ of a group signature, which is recorded in the blockchain, and *sk* is the matching random integer *d*. Since the accompanying group signature has already been authenticated by all miners, the temporary public key *PK* in the blockchain can be trusted. To rephrase, it is challenging to publish a valid temporary public key to the blockchain since an illegal member cannot establish a group signature. A digital signature formed using the secret key *sk* and a transaction *ID* including the temporary public key *PK* can guarantee the integrity, non-repudiation, and authenticity of a message when a registered vehicle communicates with other vehicles belonging to other groups. In order to validate the signature, the recipient must first acquire the *PK* from the blockchain using the transaction *ID*. The message is considered legitimate by the recipient if the signature checks out. If this condition is not met, the message will be ignored.
- Resistance to Replay Assaults: The timestamp is used to ensure that the message is current during the whole protocol phase. Any replay behavior can be identified after a message has been replayed by checking if the timestamp exceeds the maximum transmission delay. Therefore, the FCCA protocol is secure against this type of assault.
- Resistance to Man-in-the-middle Assaults: Clearly, the FCCA protocol accomplishes secure authentication during V2V and V2I communication based on the analysis of message authentication shown above.
  Therefore, the FCCA protocol is immune to such assaults.
- Resistance to Birthday Collisions Assaults: Due to the FCCA protocol's utilization of blockchain approaches, it is immune to such assaults. The adoption of secure hash algorithms (such as SHA256 and Keccak256) by blockchain technology (such as Hyperledger) to tackle the problem of birthday collision allows the FCCA protocol to realise this property.
- Resistance to Hijacking Assaults: Blockchain transactions are digitally signed using a signature technique and then broadcast to the network as a whole. No one can change the details of a transaction without breaking the signature algorithm and the blockchain.

5.2. Performance Evaluation

This section evaluates the computational overhead and communication overhead of the proposal FCCA protocol and related works such as [37, 41, 43]. The experiment of this paper is based on Chen, et al. [45] which includes fog server and 5G technology. These parameters are as follows. The participant is created on a workstation outfitted with an Intel(R) Core(TM) i5-7500 CPU and 8 GB of RAM, while the blockchain network is deployed on a server sporting an Intel(R) Xeon(R) Silver(TM) 4210R CPU running at
2.4 GHz and a whopping 32 GB of RAM. To implement the cryptographic operations, it makes use of the Pairing-Based Cryptography Library (PBC), settling on two different bilinear pairings (i.e., symmetric Type- Pairing and asymmetric Type-D Pairing). Multiple peer nodes (i.e., between 2 and 8) and 5 order nodes are part of the Hyperledger Fabric platform where

the smart contract has been implemented (docker v19.03 and Golang v1.15.10). As a consensual form of operation, Raft has been selected. The SHA-256 hashing algorithm is also used.

The FCCA protocol implementation is efficiency optimized and fits resource constrained environments such as vehicular networks, requiring cryptographic operations for key generation and signature creation/verification." Most of the processing is done by a vehicle's OBU which is responsible for managing security joints such as key management, signing, and verifying messages. Further, the architecture FCCA proposed uses edge processing where Vehicular nodes use fog servers as the edge nodes. Unburdening the OBUs Individual OBUs handle tasks, like blockchain management for temporary public key storage and for verification services, through these fog servers. This layered architecture permits local OBU processing, centralized control, and distributed support from fog servers to keep the latency low and processing efficient. The proposal exploits this distributed design to boost the performance and scalability of secure communications in 5G-enabled vehicular networks.

5.2.1. Evaluation of Computational Overhead

This section begins by evaluating the time required for basic cryptographic operations, a key metric for estimating the total cost of a protocol's computations. The following notations used in this paper are the results, with each number representing the mean from a sample of 1000.

- T_G^{ep} : indicates one exponentiation operation in *G*. The execution time of T_G^{ep} is 6.066 ms.
- T_{Gt}^{bp}: indicates one bilinear pairing operation in *Gt*. The execution time of T_{Gt}^{bp} is 12.339 ms.
- T_{Gt}^{ep}: indicates one exponentiation operation in *Gt*. The execution time of T_{Gt}^{ep} is 1.588 ms.
- T_{GT}^{bp} : indicates one bilinear pairing operation in *GT*. The execution time of T_{GT}^{bp} is 18.046 ms.
- T_{GT}^{ep} : indicates one exponentiation operation in *GT*. The execution time of T_{GT}^{ep} is 6.509 ms.
- T_{mpt}: indicates one map-to-point hash function. The execution time of T_{mpt} is 14.6 ms.
- T_h: indicates one general hash function. The execution time of T_h is 0.001 ms.
- $T_{G_1}^{pm}$: indicates one point multiplication operation in G_1. The execution time of $T_{G_1}^{pm}$ is 1.391 ms.
- $T_{G_2}^{pm}$: indicates one point multiplication operation in G_2. The execution time of $T_{G_2}^{pm}$ is 17.789 ms.

Figure 2 shows an evaluation comparison of computational overhead for the FCCA and related protocols. To explain the result of the figure, the following process is needed to sign and verify the message per each protocol in detail.

Figure 2.
Evaluation Comparison of Computational Overhead.

To generate a signature in the scheme of Wang, et al. [36] the vehicle computes four exponentiation operations in *G*, and seven bilinear pairing operations in *Gt*. Hence, the entire computational (signing) overhead in the scheme of Wang, et al. [36][36] is $7T_{Gt}^{bp} + 4T_G^{ep} = 7 * 12.339 + 4 * 6.066$

≈ 110.637 ms. While to verify the signature in the scheme of Wang, et al. [36] the vehicle computes seven exponentiation operations in *G*, and seven bilinear pairing operations in *Gt*. Hence, the entire computational (verifying) overhead in the scheme of Wang, et al. [36] is $7T_{Gt}^{bp} + 7T_G^{ep} = 7 * 12.339 + 7 * 6.066 \approx 128.835$ ms.

To generate a signature in the scheme of Wang, et al. [41] the vehicle computes three exponentiation operations in *Gt*, one general hash function, five exponentiation operations in *G*, one map-to-point hash function, and three bilinear pairing operations in *Gt*. Hence, the entire computational (signing) overhead in the scheme of Wang, et al. [41] is $3T_{Gt}^{ep} + T_h +$

$5T_G^{ep} + T_{mtp} + 3T_{Gt}^{bp} = 3 * 1.588 + 0.001 + 5 * 6.066 + 14.6 + 3 * 12.339 \approx 198.082$ ms. While to verify the signature in the scheme of Wang, et al. [41] the vehicle computes four exponentiation operations in *Gt*, one exponentiation operation in

G, one map-to-point hash function, one general hash function, and five bilinear pairing operations in *Gt*. Hence, the entire computational (verifying) overhead in the scheme of Wang, et al. [41] is

$4T_{Gt}^{ep} + T_G^{ep} + T_{mtp} + T_h + 5T_{Gt}^{bp} = 4 * 1.588 + 6.066 + 14.6 + 0.001 + 5 * 12.339 \approx 88.714$ ms.

To generate a signature in the scheme of Feng, et al. [43] the vehicle computes thirteen exponentiation operations in *Gt*, three exponentiation operations in *G*, and two bilinear pairing operations in *Gt*. Hence, the entire computational (signing) overhead in the scheme of Feng, et al. [43] is $13T_{Gt}^{ep} + 3T_G^{ep} + 2T_{Gt}^{bp} = 13 * 1.588 + 3 * 6.066 + 2* 12.339 \approx 63.52$ ms. While verifying the signature in the scheme of Feng, et al. [43] the vehicle computes five bilinear pairing operations in *Gt* and thirteen exponentiation operations in *Gt*. Hence, the entire computational (verifying) overhead in the scheme of Feng, et al. [43] is $5T_{Gt}^{bp} + 13T_{Gt}^{ep} = 5 * 12.339 + 13* 6.066 \approx 140.553$ ms.

To generate a signature in the proposed FCCA protocol, the vehicle computes one point multiplication operation in G_2, four-point multiplication operations in G_1, two general hash functions, three exponentiation operations in *GT*, and one bilinear pairing operation in *GT*. Hence, the entire computational (signing) overhead in the proposed FCCA protocol is $T_{G_2}^{pm} + 4T_{G_1}^{pm} +$

$2T_h + 3T_{GT}^{ep} + T_{GT}^{bp} = 17.789 + 4* 1.391 + 2* 0.001 + 3 * 6.509 \approx 42.882$ ms. To verify the signature in the proposed FCCA protocol, the vehicle computes four exponentiation operations in *GT*, one point multiplication operation in G_1, two general hash functions, and one bilinear pairing operation in *GT*. Hence, the entire computational (verifying) overhead in the proposed FCCA protocol is $4T_{GT}^{ep} + 2T_{G_1}^{pm} + 2T_h + 5T_{GT}^{bp} = 4 * 6.509 + 2 * 1.391 + 2 * 0.001$ $+ 18.046 \approx 46.866$ ms. To summarize the above process, Tables 2 and 3 list all operations based on signing and verifying messages. Therefore, the proposed FCCA protocol has a lower computation overheard compared with Wang, et al. [36], Wang, et al. [41], Feng, et al. [43] and the FCCA protocol.

Table 2.
Comparison of Signing Message Overhead for Authentication Schemes.

Scheme	Signing Message Overhead (ms)
Wang et al. [	$7T_{\text{bp}}^{Gt} + 4T_{\text{ep}}^{G} = 7 \times 12.339 + 4 \times 6.066 \approx 110.637$
	Wang et al. [
	Feng et al. [
	Proposed FCCA Protocol $T_{\text{pm}}^{G2} + 4T_{\text{pm}}^{G1} + 2T_{\text{h}} + 3T_{\text{ep}}^{GT} + T_{\text{bp}}^{GT} = 42.882$
41]	$3T_{\text{ep}}^{Gt} + T_{\text{h}} + 5T_{\text{ep}}^{G} + T_{\text{mtp}} + 3T_{\text{bp}}^{Gt} = 198.082$
43]	$13T_{\text{ep}}^{Gt} + 3T_{\text{ep}}^{G} + 2T_{\text{bp}}^{Gt} = 63.52$

5.2.2. Evaluation of Communication Overhead

This part evaluates the communication overhead of the proposed FCCA protocol and compares it with other exiting schemes in this section. The communication overhead is the sum of data exchanged between vehicles to fog servers for authenticating. This overhead affects the efficiency of the system, especially in crowded vehicular environments with real-time operations that need to be carried out fast.

To evaluate the efficiency of various protocols in terms of their communication overheads, the signature size must be selected. The file sizes of the transmitted messages are ignored here. This paper's experimental values for Z_q, G, G_1, G_2, GT are 20 bytes, 128 bytes, 40 bytes, 120 bytes, and 120 bytes, respectively. The size of the one-way hash's output was also predetermined to be 32 bytes.

The preceding proves that the FCCA protocol may produce a count of σ, the size of the group signature, where $D_1 \in G_1$, $D_2 \in G_1$, $D_3 \in G_1$, and $D_4 \in G_2$, d is hash function output, and group key $u \in Z_q$. Because of this, it can be calculated that there are a total of 296 bytes in the signature (403 + 120 + 32 + 20). The signature sizes of the remaining three schemes are also similar, coming in at 368 bytes, 984 bytes, and 768 bytes, as shown in Figure 3. When compared to other protocols, ours has the shortest signature size, which means less money is spent on transmissions when the quantity of messages being sent is high.

Table 3.
Comparison of Verification Message Overhead for Authentication Schemes.

Scheme	Verification Message Overhead (ms)
Wang et al. [36]	$7T_{\text{bp}}^{Gt} + 7T_{\text{ep}}^{G} = 7 \times 12.339 + 7 \times 6.066 \approx 128.835$
Wang et al. [	
Feng et al. [	
Proposed FCCA Protocol	$4T_{\text{ep}}^{GT} + 2T_{\text{pm}}^{G1} + 2T_{\text{h}} + 5T_{\text{bp}}^{GT} = 46.866$
[43]	$5T_{\text{bp}}^{Gt} + 13T_{\text{ep}}^{Gt} = 140.553$
[41]	$4T_{\text{ep}}^{Gt} + T_{\text{ep}}^{G} + T_{\text{mtp}} + T_{\text{h}} + 5T_{\text{bp}}^{Gt} = 88.714$

The highest communication overhead is observed in the scheme proposed by Wang, et al. [41] with 984 bytes.

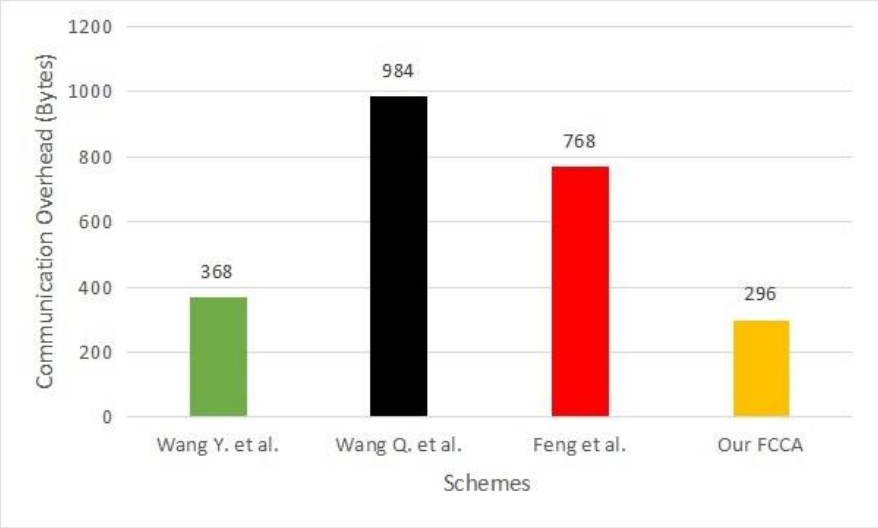

Figure 3.
Evaluation Comparison of Communication Overhead.

This is significantly larger compared to the other schemes, indicating that the protocol requires a larger amount of data to be exchanged during the authentication process, which may lead to higher latency and bandwidth consumption.

Feng, et al. [43] scheme shows a slightly reduced overhead at 768 bytes, while Wang, et al. [36] demonstrates further optimization with a communication overhead of 368 bytes. However, the proposed FCCA protocol shows the lowest communication overhead at 296 bytes, illustrating the efficiency of the protocol in reducing the amount of data exchanged during the authentication process.

The smaller communication overhead in the FCCA protocol further demonstrates that this non-incumbent channel allocation approach well suits instantaneous vehicular networks which are characterized as real-time applications where little data transmission and great communication speed are required.

The results shown in Figure 3 confirm that compared to existing schemes, the FCCA has scalability and efficiency advantages, especially for high-rate vehicular communications.

5.3. Evaluation of Energy Consumption Cost

This section evaluates the FCCA protocol and other works in terms of energy consumption cost. The energy usage can be calculated using the CPU's maximum power (10.88 watts) and the time and money required to finish the job. The amount of energy used is equal to the product of the whole processing power, P, and the time required for the calculation, t.

The energy consumption costs *E* of Wang, et al. [36] in signing message and verifying message are calculated as 10.88 * 110.637 = 1,203.73056 mJ (E = P .t) and 10.88 * 128.835 = 1,401.7248 mJ, receptively. The energy consumption costs *E* of Wang, et al. [41] in signing message and verifying message are calculated as 10.88 * 278.082 = 981.53216 mJ (E = P .t) and
10.88 * 88.714 = 965.20832 mJ, receptively. The energy consumption costs *E* of Feng, et al. [43] in signing message and verifying message are calculated as 10.88 *63.52 = 691.0976 mJ (E = P .t) and 10.88 * 140.553 = 1,529.21664 mJ, receptively. The energy consumption costs *E* of the proposed FCCA protocol in signing message and verifying message are calculated as 10.88 * 42.882= 466.55616 mJ (E = P .t) and 10.88 * 46.866 = 509.90208 mJ,
receptively. Figure 4 shows energy consumption overhead.

5.4. Discussion

The FCCA protocol is designed to address this security issue by proposing an efficient, lightweight framework that can be used to implement secure and privacy-preserving communication in vehicular networks.

Figure 4.
Energy Consumption Overhead.

All these safety and security functions have been constructed right into the method, producing an overall package that fits nicely with the vibrant, experienced 5G-enabled technology in automobiles.

5.4.1. Impact on Security

In contrast, security is greatly enhanced in 5G-enabled vehicular networks by the FCCA protocol by introducing strong authentication and integrity mechanisms. It is secured by group signatures and a temporary common public key that aids in securely authenticating vehicles from within and fog servers interacting with the network. This way prevents a wide range of attack vectors, such as man-in-the-middle, replay, and hijacking. Using blockchain technology helps to prove the security of the system as every authentication event on a registered device is recorded in an unchanging manner that can not be tampered with or modified which results also improved data integrity. The decentralized structure of blockchain eliminates a central point of control, spreading the trust throughout the network and making it more resistant to security breaches as well.

5.4.2. Impact on Privacy

FCCA protocol is a conditional privacy preservation algorithm and achieves a high level of privacy protection in security. When vehicles want to communicate, the protocol allows them to create temporary public keys that can be used for communication allowing other vehicles and fog servers to not know who is behind these messages. The availability of a confidentiality protection mechanism prevents sensitive information like vehicle location and driver identity from being exposed during communication. It also has an anonymous mode that still allows for the tracing of malicious activity. Such traceability would allow authorized entities to identify the vehicle when it misbehaves without sacrificing user privacy for all legitimate users. The aforementioned combination of anonymity and traceability is the part that this balance can make the system allow better protection of users' privacy safeguarding network security.

6 Conclusion and Future Work

Fog computing-based cross-domain authentication (FCCA) protocol has been presented in this paper to prioritize secure data delivery in 5G-assisted vehicular blockchain network environments with limited available resources. The fog servers work together to perform the required tasks, using a novel FCCA protocol with 5G-BS infrastructure. To ensure accountability for harmful vehicles and the privacy of drivers' sensitive information while decreasing dependency on the trusted authority, the FCCA protocol architecture creates a secure cross-domain authentication technique between vehicles and fog servers. The proposed FCCA protocol is secure against hijacking, birthday collisions, and man-in-the-middle attacks. FCCA is superior to other approaches in terms of security, computational, communication, and energy consumption overheads. Based on the findings and contributions presented in this study, it intends to continue the FCCA research for more security and scalability of the FCCA protocol in vehicular networks that 5G provides. Another direction is exploring how advanced cryptographic techniques, for example, post-quantum cryptography, can be integrated into the protocol to prepare it against the new security threats posed by quantum computing as well. Moreover, it intends to study the realization of the FCCA protocol in realistic vehicular scenarios, including simulations with larger network-scale scenarios to evaluate how it works in dynamic and heterogeneous situations. An interesting question would be to explore the possibility of integrating the FCCA protocol with other vehicular communication technologies such as edge AI and machine learning. When utilizing this technology, the system could improve its decision-making processes, become more efficient in anomaly

detection, and adapt to changes in network conditions as they happen. Moreover, it wants to investigate cross-layer security mechanisms that integrate network-layer trust with application-layer business-protection solutions to offer holistic secure vehicular networks. Lastly, it wishes to investigate the interoperability of the FCCA protocol with already established vehicular communication standards like IEEE 802.11p and C-V2X for enabling its adoption in current and future ITS systems. It will delve into measuring protocol performance against these standards and develop seamless onboarding strategies to help enhance network security, but not at the cost of degrading network efficiency.

References

[1] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 263-284, 2015. https://doi.org/10.1109/comst.2015.2410831

[2] M. M. Hamdi, A. S. Mustafa, H. F. Mahd, M. S. Abood, C. Kumar, and M. A. Al-shareeda, "Performance analysis of QoS in MANET based on IEEE 802.11 b," in *2020 IEEE International Conference for Innovation in Technology (INOCON)*, 2020: IEEE, pp. 1-5.

[3] Y. Li, "An overview of the DSRC/WAVE technology," presented at the In Quality, Reliability, Security and Robustness in Heterogeneous Networks: 7th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, QShine 2010, and Dedicated Short Range Communications Workshop, DSRC 2010 (pp. [pages]). Houston, TX, USA, November 17-19, 2010.

[4] A. R. Khan *et al.*, "DSRC technology in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) IoT system for Intelligent Transportation System (ITS): A review," *Recent Trends in Mechatronics towards Industry 4.0: Selected Articles from iM3F 2020, Malaysia*, pp. 97-106, 2022. https://doi.org/10.1007/978-981-33-4597-3_10

[5] M. Al Shareeda, A. Khalil, and W. Fahs, "Towards the optimization of road side unit placement using genetic algorithm," presented at the 2018 International Arab Conference on Information Technology (ACIT) (pp. 1–5). IEEE, 2018.

[6] H. Ahmadvand, C. Lal, H. Hemmati, M. Sookhak, and M. Conti, "Privacy-preserving and security in SDN-based IoT: A survey," *IEEE Access*, vol. 11, pp. 44772-44786, 2023. https://doi.org/10.1109/access.2023.3267764

[7] T. Karunathilake and A. Förster, "A survey on mobile road side units in VANETs," *Vehicles*, vol. 4, no. 2, pp. 482-500, 2022. https://doi.org/10.3390/vehicles4020029

[8] H. Ahmadvand and F. Foroutan, "DV-ARPA: Data variety aware resource provisioning for big data processing in accumulative applications," *arXiv preprint arXiv:2008.04674*, 2020.

[9] T. Norp, "5G requirements and key performance indicators," *Journal of ICT Standardization*, vol. 6, no. 1-2, pp. 15-30, 2018.

[10] W. Lei *et al.*, "5G system architecture," *5G System Design: An End to End Perspective*, pp. 297-339, 2021. https://doi.org/10.1007/978-3-030-73703-0_5

[11] S. Kannadhasan, K. Venusamy, and R. Nagarajan, "Recent trends in 5G communication: challenges and opportunities," *Advancement, Opportunities, and Practices in Telehealth Technology*, pp. 263-274, 2022. https://doi.org/10.4018/978-1-6684-5231-8.ch015

[12] G. Kakkavas *et al.*, "Design, development, and evaluation of 5G-enabled vehicular services: The 5G-HEART perspective," *Sensors*, vol. 22, no. 2, p. 426, 2022.

[13] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, "A survey of security in cloud, edge, and fog computing," *Sensors*, vol. 22, no. 3, p. 927, 2022. https://doi.org/10.3390/s22030927

[14] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing," *Plos One*, vol. 18, no. 6, p. e0287291, 2023. https://doi.org/10.1371/journal.pone.0287291

[15] K. Behravan, N. Farzaneh, M. Jahanshahi, and S. A. H. Seno, "A comprehensive survey on using fog computing in vehicular networks," *Vehicular Communications*, vol. 42, p. 100604, 2023. https://doi.org/10.1016/j.vehcom.2023.100604

[16] R. Jabbar *et al.*, "Blockchain technology for intelligent transportation systems: A systematic literature review," *IEEE Access*, vol. 10, pp. 20995-21031, 2022. https://doi.org/10.1109/access.2022.3149958

[17] A. I. Ameur, A. Lakas, M. B. Yagoubi, and O. S. Oubbati, "Peer-to-peer overlay techniques for vehicular ad hoc networks: Survey and challenges," *Vehicular Communications*, vol. 34, p. 100455, 2022.

[18] T. Zhang and Q. Zhu, "Distributed privacy-preserving collaborative intrusion detection systems for VANETs," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 148-161, 2018.

[19] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *International Workshop on Privacy Enhancing Technologies*, 2005: Springer, pp. 197-209.

[20] Y.-C. Wei and Y.-M. Chen, "Efficient self-organized trust management in location privacy enhanced VANETs," in *Information Security Applications: 13th International Workshop, WISA 2012, Jeju Island, Korea, August 16-18, 2012, Revised Selected Papers 13*, 2012: Springer, pp. 328-344.

[21] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1-13, 2014. https://doi.org/10.1016/j.comcom.2014.02.020

[22] M. A. Al-Shareeda *et al.*, "Cm-cppa: Chaotic map-based conditional privacy-preserving authentication scheme in 5g-enabled vehicular networks," *Sensors*, vol. 22, no. 13, p. 5026, 2022.

[23] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260," *Satoshi Nakamoto Institute*, 2008.

[24] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: A review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 2, pp. 778-786, 2023. https://doi.org/10.11591/ijeecs.v30.i2.pp778-786

[25] T. Dargahi, H. Ahmadvand, M. N. Alraja, and C.-M. Yu, "Integration of blockchain with connected and autonomous vehicles: vision and challenge," *ACM Journal of Data and Information Quality*, vol. 14, no. 1, pp. 1-10, 2021. https://doi.org/10.1145/3460003

[26] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39-68, 2007. https://doi.org/10.3233/jcs-2007-15103

[27] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, 2008: IEEE, pp. 1229-1237.

[28] K. Lim and D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," *Vehicular Communications*, vol. 4, pp. 30-37, 2016.

[29] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319-1328, 2015. https://doi.org/10.1109/tits.2015.2502322

[30] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722-735, 2019. https://doi.org/10.1109/tdsc.2019.2904274

[31] W. Xiong, R. Wang, Y. Wang, F. Zhou, and X. Luo, "CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 4, pp. 3456-3468, 2021. https://doi.org/10.1109/tvt.2021.3064337

[32] I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, "An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1278-1291, 2021.

[33] Q. Li, D. He, Z. Yang, Q. Xie, and K.-K. R. Choo, "Lattice-based conditional privacy-preserving authentication protocol for the vehicular ad hoc network," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 4336-4347, 2022.

[34] J. Zhang, H. Fang, H. Zhong, J. Cui, and D. He, "Blockchain-assisted privacy-preserving traffic route management scheme for fog-based vehicular ad-hoc networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 2854-2868, 2023.

[35] 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 Transactions on Intelligent Transportation Systems*, vol. 24, no. 3, pp. 3167-3181, 2022.

[36] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin, and H. Wang, "Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1779-1790, 2018. https://doi.org/10.1109/tifs.2018.2885277

[37] J. Zhang, Y. Jiang, J. Cui, D. He, I. Bolodurina, and H. Zhong, "DBCPA: Dual blockchain-assisted conditional privacy-preserving authentication framework and protocol for vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 23, no. 2, pp. 1127-1141, 2022.

[38] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. M. Alayba, and A. A. Sallam, "ANAA-Fog: A novel anonymous authentication scheme for 5G-enabled vehicular fog computing," *Mathematics*, vol. 11, no. 6, p. 1446, 2023. https://doi.org/10.3390/math11061446

[39] H. Zhang and F. Zhao, "Cross-domain identity authentication scheme based on blockchain and PKI system," *High-Confidence Computing*, vol. 3, no. 1, p. 100096, 2023.

[40] M. A. Shawky *et al.*, "Efficient blockchain-based group key distribution for secure authentication in VANETs," *IEEE Networking Letters*, vol. 5, no. 1, pp. 64-68, 2023. https://doi.org/10.1109/lnet.2023.3234491

[41] Q. Wang, D. Gao, C. H. Foh, and V. C. Leung, "An edge computing-enabled decentralized authentication scheme for vehicular networks," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, 2020: IEEE, pp. 1-7.

[42] B. Chen, T. Xiang, X. Li, M. Zhang, and D. He, "Efficient attribute-based signature with collusion resistance for Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 6, pp. 7844-7856, 2023. https://doi.org/10.1109/tvt.2023.3240824

[43] X. Feng, Q. Shi, Q. Xie, and L. Wang, "P2BA: A privacy-preserving protocol with batch authentication against semi-trusted RSUs in vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3888-3899, 2021. https://doi.org/10.1109/tifs.2021.3098971

[44] H. Ahmadvand, A. H. Jahangir, and A. F. Baarzi, "Analysis and evaluation of real-time and safety characteristics of ieee 802.11 p protocol in vanet,," *arXiv preprint arXiv:1612.01894*, 2016.

[45] B. Chen, Z. Wang, T. Xiang, J. Yang, D. He, and K.-K. R. Choo, "BCGS: Blockchain-assisted privacy-preserving cross-domain authentication for VANETs," *Vehicular Communications*, vol. 41, p. 100602, 2023. https://doi.org/10.1016/j.vehcom.2023.100602