International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 11, No. 3, 2024, pp. 5-9.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Authentication and Privacy-Preserving Protocol Utilizing Fog Computing in 5G-Enabled Vehicular Networks

Amitesh Bhagat [a], Vibha Kaul [b]

[a] *Augmented Memory Systems Lab, Bareilly Institute of Digital Neurotech, India.*
[b] *Augmented Memory Systems Lab, Bareilly Institute of Digital Neurotech, India.*

Abstract

Fifth-generation (5G) vehicular networks (VN) are an innovative mobile communication paradigm that has the potential to significantly reduce avoidable automobile accidents and provide many entertainment options for commuters. Security risks may jeopardize the communications sent by a car in a VN due to the inherent openness of these networks. This indicates possible safety and confidentiality issues associated with VN in Fog Computing (FC). This study introduced an Authentication and Privacy-Preserving Protocol (A&PP) using FC in 5G-enabled VN. A revolutionary feature masking entails the initial stage of vehicle message requests. It utilizes sophisticated cryptographic techniques, significantly complicating prospective assaults, and prevents even a Trustworthy Entity (TE) from deducing its fundamental intent. The proposed A&PP using FC in the 5G-VN framework has the least cost of 2240 bits, which is exceptionally low compared to other frameworks.

Keywords: Vehicular Networks, 5G, Fog Computing, Feature Masking, Authentication, Privacy-Preserving.

DOI: 10.71086/IAJSE/V11I3/IAJSE1152
Received: 11 June 2024/Revised: 17 July 2024/Accepted: 19 August 2024/Published: 30 September 2024

Overview of FC and VN

Development and advancement in automobile technology are often considered highly exciting. As people's health increases, the domain of automobile engineering advances correspondingly (Rasheed et al., 2020). The jamming of city roadways and traffic jams are only two challenges that have highlighted contemporary VN. Timely alerts, navigation assistance, transportation state information, surface conditions, junction warnings, and crosswalk notifications are critical traffic concerns that may be sent to users via automotive networks.

To enhance driver security and effectively handle increasingly erratic traffic conditions, several nations have recently implemented extensive installations of 5G technology, VN, and FC into their public transit networks. Wireless devices installed in cars, known as onboard units (OBUs), collect, operate, and disseminate highway data within the framework of VN (Zhang et al., 2020).

Broad adoption encounters substantial challenges despite the promised uses of 5G-enabled vehicle networks. 5G-enabled VN communication is vulnerable to several risks due to its wireless nature. Authentication is essential for transmitting communications across an authorized channel. Attorneys may easily corrupt other individuals on 5G-enabled VN without a robust authentication mechanism. Traffic congestion may occur if malicious cars disseminate false information about an event and obstruct traffic flow. It may mimic a roadside unit (RSU) or automated toll gate to access other drivers' confidential information. Moreover, drivers may be reluctant to participate in 5G-enabled VN due to apprehensions about security and protection (Mohammed et al., 2023).

Due to the mobile and public nature of 5G-enabled VN connections, hostile actors may potentially manipulate or intercept the exchanges between cars. The verification tool may thereafter ascertain the correctness of the data. Conditional A&PP solutions were created by many academics to address both security and privacy issues (Almazroi et al., 2023). Nonetheless, the authentication of vehicles inside these A&PP frameworks required the implementation of the RSU, which constitutes a costly component of VN. Moreover, these A&PP systems entail significantly elevated transmission and computational overhead. This article focuses on FC since it decreases the volume of information sent to the cloud rather than on FC or cloud computing (Al-Mekhlafi et al., 2023).

Authors in (Cui et al., 2020) assert that FC may fulfill the requirements of VN by using an FC server in place of RSUs. The FC server is deemed unreliable and can use resources like computing and memory. Several scholars have developed advanced A&PP techniques to provide safe communication among cars based on relevant investigations. These methods incur substantial processing and communication expenses. The primary inquiry of this study is how our novel architectural design would mitigate the system's expense. Simultaneously, 5G-enabled VN using FC addresses several safety and privacy concerns. Addressing these challenges necessitates a sophisticated A&PP architecture for instantaneous services in FC-based 5G-enabled VN. Consequently, this work has proposed a novel FC-A&PP architectural design for 5G-enabled VN that leverages FC.

A&PP using FC in 5G-Enabled VN

This study presents a framework for A&PP tailored for VN inside 5G-FC environments. Robust cryptographic mechanisms, including the inattentive transfer protocol, have enhanced confidentiality and safety. Through such gadget inquiries, the Onboard Unit (OBU) implements a novel concealing technique in TEs using vehicle demand messages, significantly complicating possible assaults and preventing the TE from acquiring any data regarding the rationale behind the vehicles' inquiries.

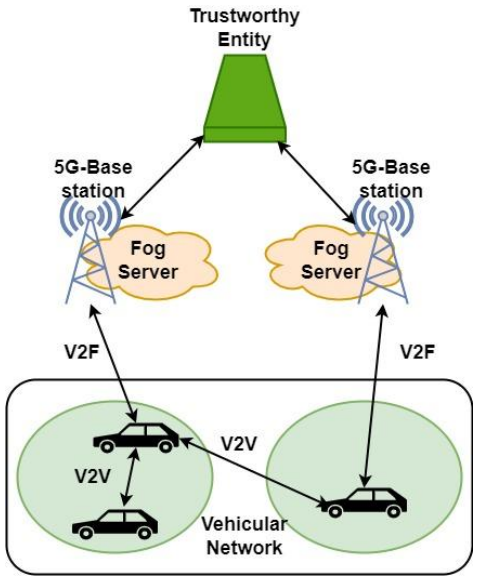


Fig. 1: Architecture of the Proposed System

Fig. 1 illustrates the elements of the proposed framework for 5G-enabled vehicle FC.

• TE: Generally, the consortium of automotive manufacturers is tasked with registering automobiles and issuing them matching identities derived from the vehicle's identification number. The TE develops, disseminates, and routinely maintains the system's public variables. Therefore, TE encompasses substantial storage capacity, significant computing power, and several RSUs. A further distinction between TEs and OBUs is that the former monitors and eliminates unauthorized vehicles. Other organizations rely on TE because of its esteemed reputation for integrity and dependability, which may result in unforeseen repercussions.

• 5G-Base Station (5G-BS): The predominant meaning refers to the foundational architecture enabling 5G mobile networks to provide radio connectivity. The BS was enough for previous wireless networks, but the acronym "NR" (New Radio) has become prevalent with the emergence of 5G.

• OBU: Each connected car has an OBU that can interact with other OBUs and FC servers using 5G-BS despite its limited computing and storage capacity. It comprises memory systems, computational units, detectors, and other components. The computational unit aggregates security alerts using information like the vehicle's velocity, acceleration, highway conditions, and trajectory. A mobile channel is thereafter used to transmit these communications to nearby participants.

• FC Server: The FC server is often positioned at intersections near 5G BS, certain structures, and other specified locations. Compared to TE, its handling and storing capacity is worse, although it surpasses OBU. The middle node coordinates OBU and TE communication, authenticates and regulates the vehicles inside its domain, and disseminates keys. The use of security systems further guarantees communication safety.

Considering the fragile communication environment and elevated trust in TE, the suggested technique guarantees secrecy during message delivery and processing. Even if the communication is compromised, an assailant would have significant difficulty in efficiently evaluating the legitimate data if they include disguised information in the vehicle's inquiry message, therefore substantially increasing the cost of the assault. The design subsequently optimizes encryption and decryption to save processing expenses and improves the OT approach to increase its applicability in vehicle inquiry circumstances. A&PP is essential since the TE must neither infer the vehicle's planned usage from the inquiry information sent by the vehicle nor should the TA's supplied service record include any extraneous details not included in the vehicle's request. The proposed A&PP protocol includes initialization, registration, request, and authentication stages.

Initialization Phase

The system necessitated this step to set up the parameters, which needed to be executed once. Since it occurs only once, the initialization phase is deemed independent of using a reliable TE to mitigate or eradicate reliance on any one authority. The TE determines the system variables to be utilized in the ensuing operations.

Registration Phase

At this point, the TE is tasked with registering for registration. It encompasses both FC server registration and vehicle registration.

Request Phase

At this juncture, FC servers must facilitate interaction between TEs and OBUs while concurrently performing safety services to ensure network security. Consequently, the FC server facilitates the transmission of the vehicle's inquiry information. We consider the situation in which the FC server is misled or compromised. The assailant can swiftly ascertain the vehicle's function and the operator's identification by analyzing its movement and the ensuing request messages. Thus, obscured information is a straightforward and crucial method to impede attackers and TEs from discerning the vehicle's genuine request. The vehicle conceals the request message with extensive metadata, making it impossible for an intruder or FC server that detects it to ascertain the true intent of the query from the ciphertext matrix. Thus, the privacy and authenticity of the solicited information are guaranteed.

Authentication Phase

The Authentication Phase delineates a secure vehicle-to-fog (V2F) authentication within an intelligent transportation or vehicular fog computing system. The process starts with the vehicle creating a secure message and sending an authentication message to the Fog Server. The Fog Server checks the authentication information and replies to the vehicle. After completing the verification, the vehicle returns the secure message to the FC Server. The Fog Server will then send the authentication verdict to the network so other vehicles can authenticate the security message. This algorithm provides verified, collaborative, and distributed authentication for IoT vehicles using fog computing technology, reducing latency and improving trust across vehicular networks.

Results and Discussion

The system necessities for the evaluation included Windows 12, 4 GB of RAM, and an Intel Core i5 CPU operating at 3.4 GHz.

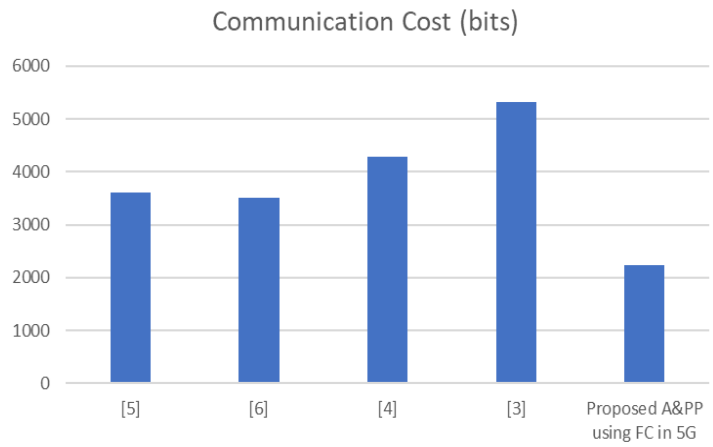


Fig. 2: Communication Cost (bits) of Various Frameworks

Figure 2, "Communication cost (bits) of various frameworks," illustrates the communication cost burden of different frameworks relative to each other. The proposed A&PP using FC in the 5G framework has the least cost of 2240 bits, which is exceptionally low compared to other frameworks. Thus, it can be concluded that data overhead is significantly reduced with this framework. Conversely, the other frameworks exhibit the highest expenditure noted in the framework [3] at 5312 bits, followed by [4] 4288 bits, [5] 3616 bits, and [6] 3520 bits. This comparison shows the method's merits, which optionally communicates the information to be transmitted, thereby validating its acceptability for 5G environments while securing the information and optimizing data transmission.

Conclusion

This work presented an Authentication and Privacy-Preserving Protocol (A&PP) using FC in 5G-enabled VN. A groundbreaking feature masking involves the preliminary phase of vehicle communication requests. It employs advanced cryptographic methods, greatly complicating potential attacks and preventing even a TE from discerning its

underlying purpose. The suggested A&PP using FC inside the 5G-VN framework incurs a minimal cost of 2240 bits, which is remarkably lower than that of other frameworks. Experimental findings validate the suggested protocol's efficacy compared to current methods for ensuring security and confidentiality in VN communications.

References

Rasheed, I., Zhang, L., & Hu, F. (2020). A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing. *Computer Networks*, *176*, 107283. https://doi.org/10.1016/j.comnet.2020.107283.

Zhang, J., Zhong, H., Cui, J., Tian, M., Xu, Y., & Liu, L. (2020). Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks. *IEEE Transactions on Vehicular Technology*, *69*(7), 7940-7954. https://doi.org/10.1109/TVT.2020.2994144.

Mohammed, B. A., Al-Shareeda, M. A., Manickam, S., Al-Mekhlafi, Z. G., Alayba, A. M., & Sallam, A. A. (2023). ANAA-Fog: A novel anonymous authentication scheme for 5G-enabled vehicular fog computing. *Mathematics*, *11*(6), 1446. https://doi.org/10.3390/math11061446.

Almazroi, A. A., Alqarni, M. A., Al-Shareeda, M. A., & Manickam, S. (2023). L-CPPA: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5G-enabled vehicular system. *Plos one*, *18*(10), e0292690. https://doi.org/10.1371/journal.pone.0292690.

Al-Mekhlafi, Z. G., Al-Shareeda, M. A., Manickam, S., Mohammed, B. A., Alreshidi, A., Alazmi, M., ... & Rassem, T. H. (2023). Efficient authentication scheme for 5G-enabled vehicular networks using fog computing. *Sensors*, *23*(7), 3543. https://doi.org/10.3390/s23073543.

Cui, J., Wang, Y., Zhang, J., Xu, Y., & Zhong, H. (2020). Full session key agreement scheme based on chaotic map in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, *69*(8), 8914-8924. https://doi.org/10.1109/TVT.2020.2997694.