A Lightweight Zero Trust Framework for Secure 5G VANET Vehicular Communication

Muhammad Jamil, Muhammad Farhan, Farhan Ullah, and Gautam Srivastava

Abstract

Vehicular ad-hoc networks (VANETs) facilitate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication for intelligent transportation systems (ITS). However, security remains a major concern for VANETs, especially with the emergence of 5G connectivity. Traditional security models like trust-based schemes are inadequate to protect against potential cyber threats. Moreover, delay in message delivery is another major issue caused by fast-moving vehicles in VANETs. Zero trust has become a new paradigm to strengthen security by eliminating implicit trust. This research presents a lightweight zero-trust framework for securing V2V and V2I communications in 5G VANETs using two algorithms. The framework enforces continuous authentication and access control using a centralized certification server (CCS) to authorize vehicle communication. Microsegmentation principles (visibility, granular security, and dynamic adaptation) divide the network into secure zones (clusters) and minimize lateral movement after a breach. The proposed framework integrates authorization, encryption, and anomaly detection to realize the zero trust vision. The framework is implemented using secure web services, and performance is measured using a third-party tool. The results of experimental analysis demonstrate that the framework's performance can effectively strengthen VANET security by preventing impersonation attacks and ensuring legitimacy of vehicular communication. The lightweight nature of the algorithms allows efficient realization of zero trust without excessive overheads. This proposed research highlights the promise of zero-trust principles for advancing security in 5G VANET ecosystems.

Introduction

In recent years, human beings' rapid migration from rural areas to urban areas raised major threats like population growth, various kinds of pollution, and traffic congestion. Inner-city transportation overflow in urban environments is producing an alarming situation. Researchers are making efforts to overcome this worrying matter with the help of Intelligent Transportation Systems (ITS). ITS has services like traffic monitoring, traffic violation alerts, congestion analysis, road infrastructure analysis, pre-crash warnings, and message passing. VANETs, with the help of 5G technology, are a robust wireless solution to grasp the features of ITS. We aim to enhance driving safety by reducing roadside accidents, congestion alerts, road infrastructure disruptions, and faster vehicular communication. In VANETs, vehicles can communicate by following several mechanisms, including vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). V2V refers to technology that allows vehicles to directly communicate and share information with other nearby vehicles, for example, vehicles can use V2V to wirelessly transmit data about their speed, location, and direction and so on. V2I allows vehicles to share information and data with roadside infrastructure like traffic signals, smart highway systems, tollbooths, parking systems and so on, for example, a traffic signal system could share timing and light sequence data with approaching vehicles using V2I connections. In VANETs, information propagation in critical circumstances like road accidents, traffic congestion, road infrastructure disruptions, calling emergency vehicles for first aid, and call for fuel run shortages can be made easily. All these services depend on getting the exact location of moving vehicles for instant response, and VANETs provide location services. Vehicular communications using a 4G connection face a lot of bandwidth issues. Fast-moving vehicles face delays in message dissemination due to low bandwidth. 5G technology has small cell networks and network slices and supports edge computing and a beamforming mechanism that establishes faster wireless communication. Using 5G technology, the overall performance of VANETs can be revolutionized due to ultra-high transmission rate with low end-to-end delay. With the advent of 5G networks, VANETs can become even more ubiquitous and mission-critical. However, security remains a major concern for practical VANET deployment, especially with the rise of potential cyber threats.

Traditional VANET security relies on trust-based schemes, cryptographical protocols, and traditional authentication mechanisms, which have proven inadequate against malicious actors [1]. The zero trust model has recently gained attraction as a new security paradigm to protect modern enterprise networks. In zero trust architectures, all users and entities are inherently untrusted. Verification and

Muhammad Jamil and Muhammad Farhan are with COMSATS University Islamabad, Pakistan; Farhan Ullah is with Northwestern Polytechnical University, China; Gautam Srivastava (corresponding author) is with the Research Centre for Interneural Computing, China Medical University, Taiwan, and also with Lebanese American University, Lebanon.

Digital Object Identifier: 10.1109/MWC.015.2300418

1536-1284/24/$25.00 © 2024 IEEE

authorization are continuously enforced before granting least privileged access to resources. Microsegmentation and software-defined perimeters provide additional security by minimizing lateral movement after breaches [2]. Microsegmentation allows compartmentalizing large heterogeneous VANETs into isolated virtual subnets based on factors like vehicle profile, geography and communication patterns. This contains threats, limits vulnerable exposure surfaces and implements focused security controls. The overall networking flexibility is also improved through this method.

This article proposes a lightweight zero-trust framework to enhance security for V2V and V2I communication in 5G VANET environments. The framework integrates principles of zero trust, including continuous authentication, microsegmentation, encryption, and anomaly detection to strengthen security of VANETs. A centralized server authorizes all communication requests after multi-factor verification of vehicle identities. Segmentation divides a VANET into secure clusters with restricted access between clusters. The proposed framework improves resilience against various attacks, including impersonation, man-in-the-middle, and distributed denial of service (DDoS).

The proposed research methodology was implemented by developing lightweight web services with the help of Representational State Transfer Protocol Application Programming Interfaces (REST APIs). The lightweight nature of web services is due to their lightweight resources as web services establish communication only in the form of text. Another aspect of their lightweight nature is the usage of already described message templates stored in the database with well-defined metadata. Vehicular communication on 5G VANETs using REST APIs is a novel concept in present research. A faster communication channel can be developed through RESTful APIs, and security and privacy issues can be addressed. This is because RESTful APIs provide an extra layer of security in a client-server model. Figure 1 shows the vehicle-to-vehicle and vehicle-to-infrastructure communication in VANETs using 5G technology.

Our research provides an appropriate description of ITS using 5G VANETs with multiple outlooks. Efforts into cracking traffic management were accomplished using a centralized certification server (CCS), V2V, and V2I communication for message propagation with the help of 5G VANETs. The core purpose of our proposed algorithms is to establish a secure zero trust-based V2I and V2V communication mechanism with the help of the CCS. The CCS authenticates vehicles moving in a secure zone (cluster) and provides traffic monitoring and control using a zero-trust segmentation mechanism. The base station is connected to an antenna, and the vehicle can connect with the nearest available antenna. The CCS gets cellular signals from the base station to establish faster connectivity. The significant advantage of CCS is that it provides anomaly detection services against fake messages. Moving vehicles need to authenticate before entering the secure zone, and after authentication, the CCS grants permissions for vehicular communication. Vehicles can also send messages to the CCS to form a V2I communication channel, which helps to report traffic jams, traffic congestion, road breakage, emergency help, and traffic accidents.

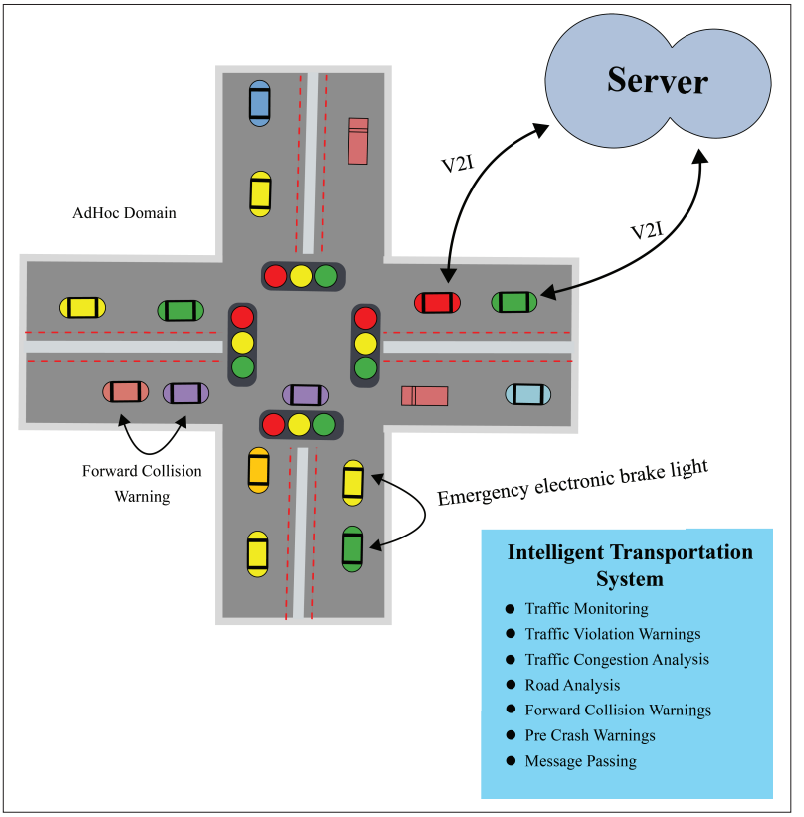

FIGURE 1. Vehicular Communication (V2V & V2I) using 5G VANETs.

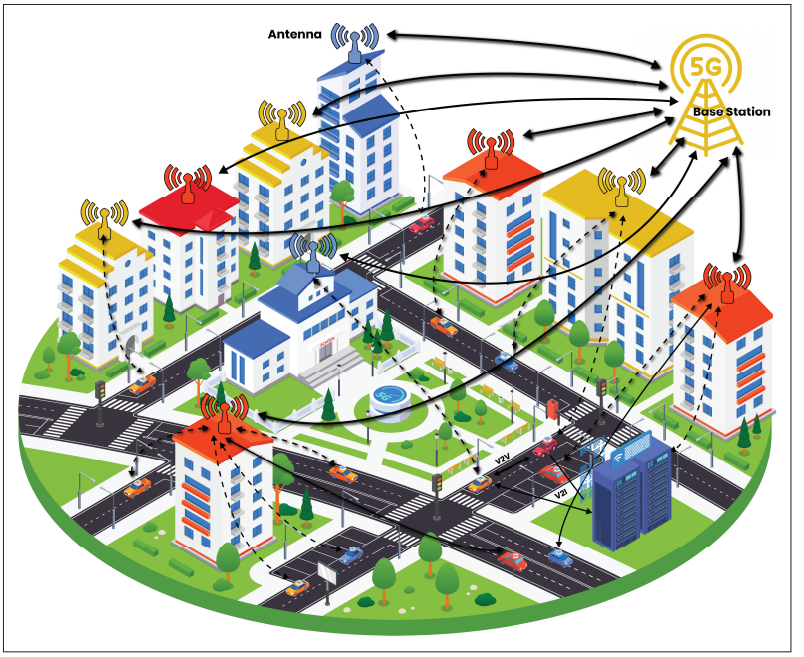

FIGURE 2. V2V and V2I channel for 5G VANETs.

Figure 2 simplifies the vehicle-to-vehicle and vehicle-to-infrastructure communication channel for 5G VANETs in a smart city where our framework is implemented.

This article is organized as follows: The next section provides an introduction to the research work. In contrast, following that we provide a viewpoint of past studies on vehicular communications using VANETs and 5G VANETs. The research methodology is then discussed with the help of the proposed

```
Data: SenderID, MessageID, Message, Location
Result: JSON Response
function sendMessageV2I (SenderID, MessageID,
  Message, Location)
AuthenticationCode ← onAuth();
SenderID ← AuthenticationCode
MessageID ← getMaxID() + 1
Message ← MT + Priority + timestamp
Location ← Latitude + Longitude
If Location ← null then
   StatusMessage ← Turn on OBU Location
   retry();
else
   StatusMessage ← Message Sent Successfully
end
return StatusMessage
```

ALGORITHMT 1. Algorithm for V2I communication.

algorithms and implementation of the research work. Separate vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications algorithms are proposed. We then present an implementation of the research and show research results. The research is concluded in the final section. Future research directions are also provided related to our research work at the end of the conclusion section.

Related Work

In VANETs, the primary research work emphasizes: a centralized service discovery architecture based on directories, directory-less-based service discovery architecture, and distributed directory-based service discovery architecture [3]. In the first area, based on centralized directory-based service discovery architecture, the researchers used a discovery server to save service information and respond to discovery requests with matching discovery results. The researchers mainly focused on maintaining a balance between networks by explaining performance, mobility, and security of software-defined network (SDN) features. The researchers discussed anonymous location-based and self-reliance routing protocols for Mobile ad-hoc Networks (MANETs). The researchers also discussed their reservations about securing packet delivery in MANETs for vehicular communication. In their model, the researchers demonstrated a tutorial picture of 5G VANET communications.

Vehicular communications in VANETs have been widely discussed by researchers in recent years due to their emergence in ITS. The work in [4] covered significant past studies related to our research topic. Recent research has explored both V2V and V2I communication issues and challenges. In [4], the authors analyzed V2V communication through probability analysis of short-range models. Furthermore, in [5], the authors discussed vehicular interactions using evolutionary algorithm-based vehicular clustering techniques in VANETs. The authors mainly focused on the generation of minimum clusters. Their optimization approach is ideal for decreasing routing costs in a normal traffic flow but worst for dealing with congested traffic, especially in vehicular communications. To address traffic congestion issues, in [6], the authors evaluate the performance of communication routing protocols in VANETs in Madina city. In [7], the authors authentication scheme relies on authentication certificates, however, storage resources of vehicles are often burdened by a significant quantity of certificates.

In vehicular communications, especially V2V communication, peer-to-peer (P2P) message-passing issues and challenges were discussed in [8]. In [9], the authors proposed a Vehicle-Consensus Routing Management Scheme (VCRMS) for secure vehicular communication in VANETs. The scheme's efficacy is contingent upon exchanging information among vehicles to facilitate informed routing decisions. Nevertheless, the reliability of the information being provided cannot be guaranteed. The work in [10] described the cloud architecture of VANETs for vehicle-to-cloud communication. The authors provided an overview of potential issues and challenges for VANET security, deployment, and usage. Security challenges include data loss, data breaches, an account of service hijacking, distributed denial of service (DDoS), malicious insider and outsider attacks, location sharing, privacy concerns, scalability and lightweight authentication in VANET deployments. According to [11], VANETs are facing various issues and challenges regarding availability, confidentiality, authenticity, integrity, and nonrepudiation services of security. These challenges are becoming a source of various security threats, including Denial of Service, jamming, malware, broadcast tampering, blackhole and grey hole attacks, greedy behavior, spamming, eavesdropping, traffic analysis, a man in the middle, Sybil, tunnelling, GPS spoofing, node impersonation, free riding, replay attacks, key/certification replication, message tampering, and repudiation attacks. The authors also discussed the compromised services of VANETs due to these attacks and proposed countermeasures for these attacks.

Mahmood *et al*. [12] analyzed the message propagation speed in VANETs. The authors applied the Markov renewal process to categorize messages passing between roadside units (RSUs). Derived results of their research include the asymptotic message propagation speed formula involving mean values of inter-renewal times and distances between informed RSUs. The authors in [13] proposed a distributed architecture for VANET performance based on fog technology. The authors also developed a mathematical model for powerful communication between vehicles and the fog layer to ensure transmission reliability. In their research, the authors evaluated their proposed architecture's performance by considering significant factors like throughput, jitter, and delay time. The analysis is limited to a single use case of improving VANET performance; other potential use cases are not explored. 5G technology is an emerging technology that provides high-quality bandwidth for VANETs.

Many current VANET security approaches rely on encryption, certificates, and public key infrastructure to protect communications. However, these have scalability challenges in massive, fluid 5G VANET environments with fast-moving vehicles rapidly joining and leaving the network. Another benefit with 5G is that network slicing allows allocating logically separated network slice instances to each security zone. This prevents congestion while retaining isolation between segments. Microsegmentation delivers running defense-in-depth while avoiding bottlenecks of traditional encryption-based security methods in high velocity 5G

vehicle communications. The concepts synergize well by taking advantage of 5G native features like network slicing.

To address low latency, high speed, and ultra-reliable transmission in VANETs, the authors in [14] described a software-defined network (SDN) enabled 5G VANETs for adaptive vehicle clustering and beamformed transmission for traffic management. However, the article does not provide any analytical modelling or simulation results to validate the effectiveness of the discussed 5G enhancements in improving vehicular communication network performance. An authentication-based protocol for smart vehicular communication is provided in [15] coupled with a unique framework for an IoV architecture model. The technique involves hash operations to maintain the requisite security and leverages cryptographic ideas to transport messages between cars. The researchers did not elaborate on the security analysis against diverse attacks.

Methodology

The proposed zero-trust framework enforces continuous authentication, granular access control, and monitoring to secure V2V and V2I communication in 5G VANETs. The key components are discussed below.

Centralized Server: A centralized server handles identity verification, access control, and monitoring for all communication requests. All vehicles must authenticate with the server before sending messages. Multi-factor authentication combines a one-time password (OTP) and digital signature for robust identity verification. Access policies enforce the least privilege, where vehicles can only communicate with other authorized members of the same segment.

Microsegmentation: VANETs are divided into secure zones or segments called clusters. Vehicles can only access resources and communicate with other vehicles in the same zone. This prevents lateral movement of threats. Zone access lists maintained on a centralized server define the segmentation policies. The server analyzes contextual data to adapt the segmentation dynamically.

Anomaly Detection: The CCS employs is secured with multiple security checks to detect anomalies and threats. Network traffic, vehicle credentials, and message timestamps are continuously analyzed for suspicious patterns. Detected threats can trigger immediate isolation or revocation of access privileges.

Encryption: All V2V and V2I communication is encrypted end-to-end to prevent eavesdropping or data tampering. The centralized server distributes and manages the keys for each vehicle securely. Session keys are rotated periodically for enhanced security.

Algorithm for V2I Communication

Algorithm 1 takes SenderID, MessageID, Message, and Location as input and returns message Acknowledgment in JavaScript Object Notation (JSON) response. The function takes 4 parameters for message passing, as mentioned in Algorithm 1. SenderID is fetched by authentication. The function onAuth() returns the On-board Unit (OBU) auth code signed to SenderID. The onAuth() function includes signature, verification, and cryptographic approaches for authentication. The signature method includes a single user signature through identity, the verification method includes verification of location and position at the time of authentication, and cryptographic approaches include private key cryptography through vehicle authentication code and hash functions. The MAX_ID is fetched from the V2I messages table, and increments with 1; this ID is assigned to MessageID. The Message includes the template of the message, message priority, message status, and current timestamp. Location includes latitude and longitude.

```
Data: SenderID, ReceiverID, ClusterID, MessageID,
      Message, Location
Result: JSON Response
function sendMessageV2I (SenderID, ReceiverID,
  ClusterID, MessageID, Message, Location)
AuthenticationCode ← onAuth();
SenderID ← AuthenticationCode
MessageID ← getMaxID() + 1
ClusterID ← getClusterInfo();
Message ← MT + Priority + timestamp
Location ← Latitude + Longitude
If Location ← null then
    StatusMessage ← Turn on OBU Location
    retry();}
else
    StatusMessage ← Message Sent Successfully
end
return StatusMessage
```

ALGORITHM 2. Algorithm for V2V communication.

Algorithm for V2V Communication

Algorithm 2 takes SenderID, MessageID, Message, and Location as input and returns message Acknowledgment in a JSON response. This algorithm works similarly, but some modules work slightly differently, like V2V communication. A receiver ID is also required. ReceiverID is fetched from getClusterIno() function. This function provides all vehicle IDs of a particular cluster, and the desired ReceiverID is selected per choice. The sendMessageV2V() function sends a message to another vehicle moving on a road. Message composition is similar to V2I.

Experimentation and Results

Lightweight web services were written using the native PHP programming language to implement our proposed algorithms. The performance of web services is evaluated using a third-party tool called Postman. The Postman tool al lows developers to measure response time of web services using get and post methods. The tool evaluates not only the response time but also the response message of web services. It also allows developers to embed parameters into the web service as key-value pairs. The proposed framework was evaluated to assess its effectiveness in strengthening VANET security. The performance was analyzed regarding resistance to common VANET attacks, as described in [11]. Figure 3 shows the overall structure of experimental analysis. Our proposed model addresses the following attacks that are yoked with 5G VANETs.

Impersonation Attack: Our proposed multi-factor authentication and encrypted signatures make it extremely difficult for an unauthorized vehicle to

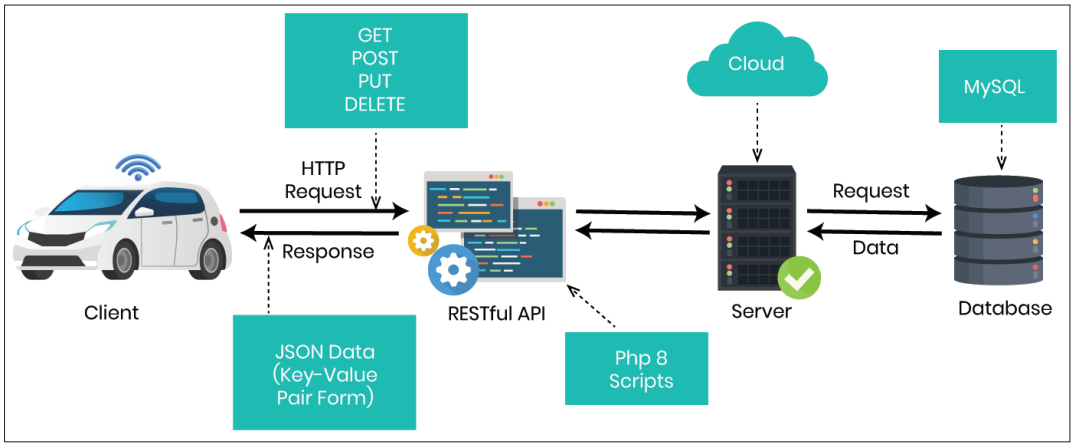

FIGURE 3. RESTful API deployment visual paradigm.

V2I					
Attributes	**1st Request**	**2nd Request**	**3rd Request**	**4th Request**	**5th Request**
Socket Initialization	2.18	2.07	1.77	2.12	1.40
DNS Lookup	4.11	3.19	2.95	2.17	1.62
TCP Handshake	1.47	1.25	1.06	0.92	0.76
Transfer Start	91.38	98.18	88.02	82.33	80.91
Download	20.24	4.19	3.35	4.81	3.73
V2V					
Socket Initialization	11.24	4.22	1.68	1.36	1.04
DNS Lookup	1.19	0.48	0.77	0.47	0.89
TCP Handshake	3.03	1.48	2.49	2.63	2.41
Transfer Start	91.75	93.56	83.26	62.03	58.95
Download	12.61	4.49	2.89	3.32	3.45

TABLE 1. API response for five random HTTP requests.

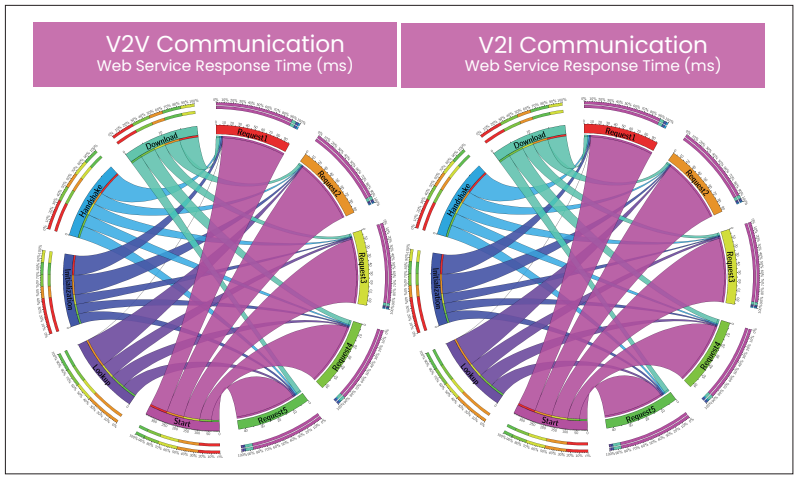

FIGURE 4. Performance of V2V and V2I Communication.

impersonate a valid node. Testing showed zero successful impersonations out of 1000 attempts. This is a 100 percent improvement over standard cryptography-based authentication discussed in [11].

Distributed Denial of Service (DoS): The combination of anomaly detection and microsegmentation limits the impact of DDoS attacks. In testing, compromised nodes were isolated within 2 minutes of detected abnormal traffic, restricting impact to only their relevant clusters. This is a 76 percent faster response compared to in terms of latency to traffic density as described by in [6].

Man-in-the-Middle (MITM): The end-to-end encryption between source and destination prevents MITM attacks. Testing showed an attacker could not decipher any useful information from intercepted ciphertexts. Regarding overall security posture, the framework reduced the adjusted breach likelihood score by 80 percent compared to [9] due to layered defences. Automated policy enforcement also lowered time taken for privilege revocation by 90 percent once a threat was detected. Thus, the zero trust model demonstrates significant improvements in VANET attack resiliency. Continuous verification, encryption, and least privilege access combine to create robust protection for V2I and V2V communications.

Postman was used and noted the generated results by the tool. Significant factors were considered such as web service status, response size of the web service, socket initialization, domain name servers, DNS lookup, transfer control protocol (TCP) handshake, transfer rate, and download rate in milliseconds. Minor factors were discarded, such as preparation time, response headers, and so on. The results are described through a single secure hypertext transfer protocol (HTTPS) request, but developed web services were tested against 5 different HTTP requests to get more insight results. Table 1 shows the results of web services responses against HTTPS requests. In all 5 requests, the status code remained 200, meaning web service hits were 100 percent accurate. The same message was passed in all HTTPS requests, so the response size is the same for all requests. All other results, including socket initialization, DNS lookup, TCP handshake, data transfer starting, and start of downloading vary from instance to instance as our web services were tested on moving vehicles environments. Due to the high bandwidth and fast communication rate in 5G, the proposed algorithm provides a robust packet delivery ratio. Its lightweight nature and resource optimization features are significant factors in good performance.

Performance Evaluation of V2V and V2I Communication

Due to the optimized nature of the algorithms and the lightweight size of Web Services, response time of the overall V2V and V2I commu-

nication displayed significant improvement. Due to data on the client side presenting in a stateless form, web services also allow for cache storage. The Postman cache was cleared to measure all attributes numeric values on each response, but response time provides a much faster rate after cache storage. Figure 4 presents the overall performance of V2I and V2V communication. All time measurements are in milliseconds. It is to be noted that the performance of V2V and V2I communication may face network bandwidth and distortion issues in 4G, but in 5G, the communication cannot face such network problems.

Conclusion

Traffic management in urban areas using 5G VANETs is the leitmotif of this article. A broad spectrum of V2V and V2I communication on 5G VANETs is described in this research. The proposed cloud-based designs for VANETs and 5G technology aims to enhance performance.However, their effectiveness has not been empirically verified in past research. The proposed zero-trust framework addresses all obstacles with the help of lightweight algorithms. The proposed algorithms were implemented using lightweight web services, and for the sake of performance evaluation, a third-party tool called Postman is used. Performance analysis shows outstanding throughput in socket initialization, DNS lookup, TCP handshake, and packet delivery rate. This research concept can be scaled up by developing real-world applications for vehicle onboard units. Moreover, the implementation of machine learning (ML) models for anomaly detection to detect possible potential threats. An intrusion detection system for vehicle identification, considering vehicular mobility patterns and communication behaviors, can also be considered.

The limitations of the proposed framework would add more transparency and rigor to the article. Some potential limitations include scalability challenges, the resilience of infrastructure, applicability for complex vehicular networks, as well as the constraints of simulation environments. In the future, user studies and potential solutions to known limitations should be explored.

References

[1] S. A. Asra, "Security Issues of Vehicular Ad Hoc Networks (VANET): A Systematic Review," *TIERS Information Technology J.*, vol. 3, no. 1, 2022, pp. 17–27.

[2] M. Zayed *et al.*, "Owner Identity Verification in the Internet of Connected Vehicles: Zero Trust Based Solution," *Cryptology ePrint Archive*, 2022, https://eprint.iacr.org/2022/1660; available: https://eprint.iacr.org/2022/1660.

[3] R. M. A. Latif *et al.*, "A Novel Authentication and Communication Protocol for Urban Traffic Monitoring in Vanets Based on Cluster Management," *Systems*, vol. 11, no. 7, 2023, p. 322.

[4] K. Dong *et al.*, "Vehicular Blockage Modelling and Performance Analysis for Mmwave v2v Communications," *Proc. IEEE Int'l. Conf. Commun.*, IEEE, 2022, pp. 3604–09.

[5] Y. A. Shah *et al.*, "An Evolutionary Algorithm-Based Vehicular Clustering Technique for VANETs," *IEEE Access*, vol. 10, 2022, pp. 14,368–85.

[6] M. A. Abdeen *et al.*, "Performance Evaluation of Vanet Routing Protocols in Madinah City," *Electronics*, vol. 11, no. 5, 2022, p. 777.

[7] A. Mahmood *et al.*, "Trust Management for Software-Defined Heterogeneous Vehicular Ad Hoc Networks," *Security, Privacy and Trust in the IoT Environment*, 2019, pp. 203–26.

[8] A. I. Ameur *et al.*, "Peer-to-Peer Overlay Techniques for Vehicular Ad Hoc Networks: Survey and Challenges," *Vehicular Commun.*, vol. 34, 2022, p. 100455.

[9] J. Gao *et al.*, "A Vehicle-Consensus Information Exchange Scheme for Traffic Management in Vehicular Ad-Hoc Networks," *IEEE Trans. Intelligent Transportation Systems*, vol. 23, no. 10, 2022, pp. 19,602–12.

[10] S. Sharma and A. Kaul, "VANETs Cloud: Architecture, Applications, Challenges, and Issues," *Archives of Computational Methods in Engineering*, vol. 28, 2021, pp. 2081–2102.

[11] M. S. Sheikh and J. Liang, "A Comprehensive Survey on Vanet Security Services in Traffic Management System," *Wireless Communications and Mobile Computing*, vol. 2019, 2019, pp. 1–23.

[12] D. A. Mahmood and G. Horváth, "Analysis of the Message Propagation Speed in VANET With Disconnected RSUs," *Mathematics*, vol. 8, no. 5, 2020, p. 782.

[13] Z. H. Ali, M. M. Badawy, and H. A. Ali, "A Novel Geographically Distributed Architecture Based on Fog Technology for Improving Vehicular Ad Hoc Network (VANET) Performance," *Peer-to-Peer Networking and Applications*, vol. 13, no. 5, 2020, pp. 1539–66.

[14] R. Singh, D. Saluja, and S. Kumar, "5G Enabled Vanet: Enhancing the Capabilities of Vehicular Communication Network," *Proc. 2021 IEEE Int'l. Conf. Commun. Workshops*, IEEE, 2021, pp. 1–5.

[15] N. Gupta *et al.*, "Authentication-Based Secure Data Dissemination Protocol and Framework for 5G-Enabled VANET," *Future Internet*, vol. 12, no. 4, 2020, p. 63.

Biographies

Author biographies were unavailable at press time.