iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69927

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

A Modified Secure Protocol in V2V Network

M.V.H. Bhaskara Murthy[1], M.Abhiram[2], A. Bhargavi[3], D. Surya[4], G. Srinu[5]

Abstract: ***Vehicular Ad-Hoc Networks, or VANETs, are meant to facilitate communication and information exchange between cars. Another important method through which this is done is vehicle-to-vehicle (V2V) communication. We also utilize vehicle-to-roadside (V2R) and roadside-to-roadside (R2R) communication in this project in order to form a stronger and more versatile network. VANETs are also known to be Intelligent Transportation Networks. Over time, the idea has developed into what is currently referred to as the "Internet of Vehicles" an expanding system that may someday become a significant component of the larger internet. As vehicle technology continues to evolve, particularly with the emergence of autonomous vehicles, we can look forward to the creation of an "Internet of Autonomous Vehicles."In order to facilitate communication, VANETs are based on wireless networking technology. This includes conventional wireless systems and contemporary standards such as LTE and 5G, providing quick and reliable connectivity.We are concentrating in this project on developing a secure communication protocol for VANETs. It is aimed at intrusion detection and avoidance of malicious activities within the network. To simulate and test the protocol, we are utilizing the NS2 network simulator that allows us to analyze the system's performance and reliability in a controlled virtual setting.***

Keywords: Authentication, DoS, Network Simulator, Tool Command Language (TCL)

I. INTRODUCTION

Vehicle-to-Vehicle (V2V) communication is a key component of Intelligent Transportation Systems (ITS) that enables vehicles to exchange information, improving road safety, traffic efficiency, and driving experience. However, the open nature of wireless communication makes V2V networks vulnerable to various security threats, including eavesdropping, spoofing, and denial-of-service attacks. To ensure the confidentiality, integrity, and authenticity of exchanged data, secure communication protocols are essential. This paper introduces a modified secure protocol for V2V networks, aiming to enhance security while minimizing latency and resource consumption, thus enabling safer and more efficient communication in dynamic vehicular environment [1], [2], [3]. The importance of a modified secure protocol in Vehicle-to-Vehicle (V2V) networks lies in its potential to address critical security vulnerabilities in vehicular communication systems. As V2V networks become integral to autonomous driving, traffic management, and safety applications, ensuring robust data protection is paramount to prevent malicious attacks that could jeopardize road safety. A secure protocol not only safeguards against threats like spoofing and data tampering but also ensures privacy and trust among vehicles. This research contributes to advancing secure V2V communication, paving the way for more reliable and resilient transportation systems in the future [4], [5]. A modified secure protocol in Vehicle-to-Vehicle (V2V) networks has a wide range of applications that are critical for the future of intelligent transportation systems (ITS). These include enhancing safety through collision avoidance, enabling efficient traffic flow management, and supporting autonomous vehicle coordination. Additionally, the protocol can be applied in real-time hazard warning systems, platooning, and emergency vehicle prioritization. By ensuring secure communication between vehicles, it can also support the development of connected vehicle infrastructures, improving overall mobility and reducing accident rates. Secure V2V communication is fundamental to the successful deployment of next-generation smart cities and autonomous transportation networks [6], [7].The advantages of a modified secure protocol in Vehicle to-Vehicle (V2V) networks include enhanced data integrity, confidentiality, and authenticity, ensuring that critical information exchanged between vehicles remains protected from malicious attacks. This protocol minimizes vulnerabilities such as spoofing and eavesdropping, thus fostering trust and reliability in V2V communications. Additionally, it improves the overall performance of the network by reducing latency and optimizing resource utilization. By strengthening security without compromising on efficiency, the protocol contributes to safer and more efficient traffic management, enabling the seamless integration of autonomous vehicles into the transportation ecosystem [8], [9].

II. LITERATURE REVIEW

1) Research on car networks, particularly Vehicle-to-Everything (V2X) communication, has grown multi-fold with its utility in enhancing road safety and self-driving cars. Syed Adnan Yusuf et al. conducted a rigorous review of V2X technologies focusing on protection of Vulnerable Road Users (VRUs). In their study, they discussed a motion control scheme based on deep learning improving communication and tracking of VRUs, especially for non-line-of-sight situations.

They discovered that integration of artificial intelligence and deep learning algorithms significantly enhances pedestrian and cyclist safety, particularly where conventional sensor-based solutions cannot operate under visibility or connectivity limitations[1].

2) Zeeshan Hameed et al. proposed a Hybrid Vehicular Network (HVN) model through an integration of Dedicated Short Range Communication (DSRC) and LTE to provide increased reliability in Cooperative Intelligent Transportation Systems (C-ITS). Their simulation-based approach proved that hybrid communication, enabled by intelligent traffic steering and multi-RAT features, increases reliability and optimizes network congestion by dynamically shifting between DSRC and LTE based on real-time conditions. The study can potentially reach scalable and effective communications for connected and autonomous vehicles[2].

3) Alexey Rolich et al. further researched in another study the effect of Semi-Persistent Scheduling (SPS) in Cellular Vehicle-to-Everything (C-V2X) communications. They explored in their research performance criteria such as the Age of Information (AoI) and delivery rates of messages with various degrees of persistence and transmission radii. Via analytical modeling and simulator simulations based on ns-3, they developed optimal SPS configurations minimizing latency and maximizing reliability for applications of safety-critical messaging[3].

4) In resolving the computational burden in V2X message authentication, Eduardo Lopes et al. suggested mechanisms like Message Authentication Codes (MACs) and hash chaining. These mechanisms allow a sequence of messages to be authenticated by a single digital signature, with an enormous verification time saving. Their approach was demonstrated to save the computational cost up to 90% under ideal network conditions, providing an efficient solution for real-time applications like Intelligent Transportation Systems (ITS) [4].

5) Yarra Kavitha et al. introduced a real implementation of Vehicle-to-Infrastructure (V2I) communication by introducing a design of an emergency vehicle signal preemption system. GPS and DSRC are utilized in the system to transmit priority messages to traffic lights so that emergency vehicles may overtake intersections in a safe and effective manner. Hardware was installed in vehicles and roadside units, indicating real implementation and making tremendous differences in emergency response time and overall safety[5].

6) Syed Adnan et al [10] assessed Vehicle-to-Everything (V2X) and Autonomous Vehicle (AV) technologies with a focus on improving the safety of Vulnerable Road Users (VRUs). They proposed a deep learning-based motion control system and evaluated various AI methods to enhance VRU communication and tracking. Through a review of existing research, they introduced a deep learning algorithm for VRU motion control and assessed AI technologies to improve VRU identification and communication. The study identified significant gaps in current AV systems, particularly in non-line-of-sight conditions and under network limitations, where VRU detection and communication are often compromised. Ultimately, the researchers concluded that AI and deep learning can play a critical role in addressing these challenges, thereby significantly enhancing VRU safety in AV systems..

III. METHODOLOGY

Dynamic Source Routing (DSR), an on-demand reactive routing protocol, is used for protocol initialisation because it does not require periodic table update messages like table-driven methods do. It reduces bandwidth consumption by limiting the transmission of control packets. Instead of relying on routing tables at intermediate nodes, DSR controls data paths using source routing. Its beaconless design eliminates the need for frequent hello packet broadcasts, making it more effective in dynamic network conditions.To use secure data exchange in an automotive V2V network with NS2 (Network Simulator 2), one has to take a few steps. One should first understand the prerequisites, such as NS2 being installed on the computer, familiarity with Tcl (Tool Command Language) for creating the simulation script, knowledge of C++ for extending new protocols or features, and a basic idea of V2V communication and security plans.

Second, simulation objectives must be defined. The objectives must involve the safe exchange of data between the vehicles, specifying the network topology in terms of the number of vehicles (nodes), their mobility pattern, and their communication method. The security aspect must be able to accommodate encryption algorithms like RSA or AES or secure routing protocols. For measuring such parameters as throughput, packet delivery ratio (PDR), delay, and security overhead, there must be provision of performance metrics.

To install the NS2 environment is to download and install the software from the NS2 official website. Test that it is successfully installed by typing the "ns" command and verifying the NS2 interactive shell appears. An entry in Tcl is then required to configure the network topology.

This will entail configuring mobility for cars, setting up nodes, and initializing the simulator. Encryption mechanisms like AES or RSA need to be used for secure communication. This means adding encryption and decryption functionalities to the NS2 backend through C++.The agent files like tcp.cc and udp.cc should be altered to include encryption functionalities that encrypt data packets when they are sent and decrypt them when they are received.

Secure routing protocols should also be included by altering existing protocols like AODV, DSR, or DSDV to include security elements. An example is to include a certificate-based authentication scheme where nodes will exchange certificates for the purpose of authentication of identity and permit authenticated nodes to communicate.

Attacking simulation is a valuable but optional step to ascertain the validity of the security mechanism. Attack simulations for eavesdropping, spoofing, or Sybil attacks are done by introducing malicious nodes in the Tcl script and observing their effect. The network once established, simulation running involves the running of the Tcl script via the "ns your_script.tcl" command.. An example Tcl script illustrates the process involved by initializing the simulator, defining nodes, defining mobility models, setting up communication, and executing the simulation. Simulations were conducted in this study using the NS2 simulator to simulate the vehicular ad hoc network (VANET) environment for urban and semi-urban regions. A highway scenario simulation was also conducted using a custom-built C-based simulator on a Linux platform. The urban environment was simulated inside a 1250 meters by 1250 meters grid, locating 152 points inside the network grid, with 20 nodes being considered as vehicles. All wireless parameters like antenna model, channel model, and propagation model were specified for all nodes. The simulation employed the MAC layer based on the IEEE 802.11 standard and employed a two-way ground propagation model. The simulation parameters were 20 vehicles moving in a grid region of 1250*1250 m² with the IEEE 802.11 MAC protocol. Two-way ground model was the propagation model and the transmission range was 300 meters. Omnipresent antenna was the type of antenna, and communication was through a wireless channel. The simulation time was 60 seconds.

The flowchart fig.1. illustrates the procedure of secure data transmission in a Vehicular Ad Hoc Network (VANET). The procedure begins with network initialization, where a dynamic topology is established with vehicles as mobile nodes. The nodes exchange information with one another through wireless communication technologies. Once the network topology is established, all the vehicles initiate information exchange with neighboring vehicles. These data may comprise real-time data such as traffic, speed, and location, which are required for cooperative awareness and safety.

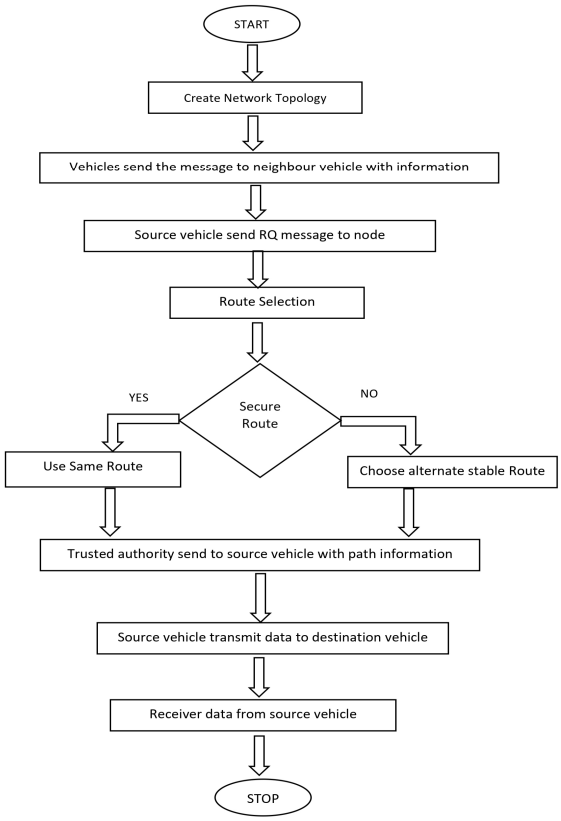


Fig. 1. Flow Diagram for V2V Communication process

Whenever a vehicle (source vehicle) wishes to transmit data to another vehicle (destination), it initiates sending an initial message to set up communication, or the Route Request (RQ) message. The message is received and transmitted to look for potential routes on which the data are being forwarded. Once it has processed the request, the network is already at the phase of route determination, where it explores the route available in regard to matters such as connectivity, stability, and safety. There is a decision point after that: whether the given route is safe or not. If the route is safe, then the source vehicle employs the same route to transfer. But if otherwise, or volatile, then the system is in search of some other alternative pathway for providing further safety and dependability to data transfer. It is a decision that not just makes the data transfer process economical but also safe from attacks in the form of malicious nodes or data hijacking.

After a route has been established—either primary route or secondary route—a reliable VANET system's agent sends authenticated path information to the source vehicle. This assures that the path selected is authenticated and secure to exchange data. With this authenticated path, the source vehicle continues to send the data to the destination vehicle.

Finally, the receiving vehicle receives the transmitted data and this completes the entire communication loop. This safe, step-by-step verification, discovery, and transmission process makes safe and reliable data transmission in vehicular networks possible and enhances the overall performance and integrity of the VANET system.

IV. RESULTS AND DISCUSSION

This paper applies Network Simulator-2 (NS-2) to simulate the proposed Dominant Optimization System (DOS) approach for secure and efficient data transmission over Wireless Sensor Networks (WSNs). Simulations in NS2 provide a realistic VANET setting for urban and semi-urban environments. Highway environments are simulated through a custom-built simulator in C on a Linux platform. The urban simulation domain is a grid of 1250m × 1250m with 152 points and 50 of these points being moving vehicles. Wireless parameters including antenna type, channel type, and propagation model are specified at each node. The MAC layer is based on the IEEE 802.11 standard, and a radio model facilitates proper vehicle-to-vehicle communication.

Packet Delivery Ratio (PDR), End-to-End Delay, Average Throughput, and Energy Consumption were the metrics used to assess the suggested Dominant Optimisation System (DOS). By routing through nodes with higher residual energy, the system keeps a steady PDR even in the event of node failures or energy drops. This guarantees dependable data transfer in a range of mobility scenarios. Faster data transmission is made possible by optimized path selection, which drastically lowers end-to-end latency. Secure communication is ensured without increasing overhead using HMAC (Hash–Based Message Authentication Code). By using high-energy nodes for data transfer and reducing packet drops, throughput is increased by 80%. By guiding low-power routing with a mathematical model, energy efficiency is attained while lowering control overhead and retransmissions. This method reduces energy waste and increases network lifetime. The DOS system, as simulated in NS-2, is a powerful tool for improving the performance of wireless sensor networks since it is safe, dependable, and energy-efficient. The plots mentioned below show the results of the paperwork.

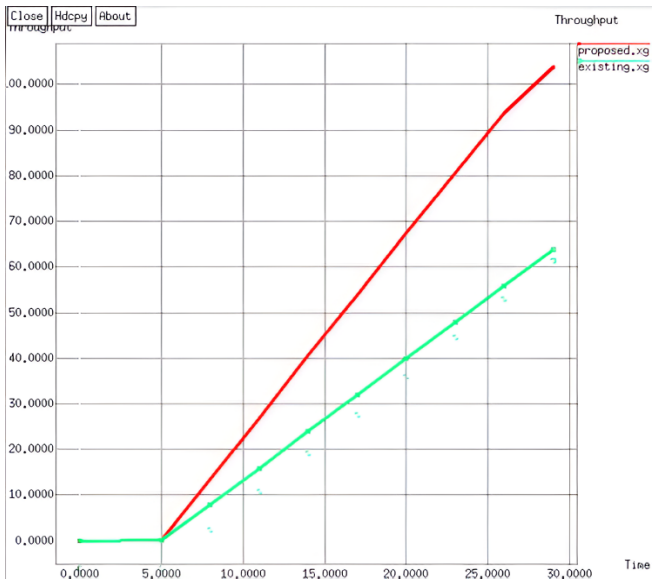


Fig.2 Throughput

As seen in Fig. 2, Both protocols, at the initial stage of the simulation (0–5,000 seconds), share comparable values of throughput, proving equal initial performance. Yet, with the passage of time, the proposed protocol shows a significantly steeper rate of increase in throughput than the current system. This proves that the proposed approach is more effective in the formation and maintenance of stable communication channels, leading to greater successful deliveries of packets.

At the end of the simulation time (around 30,000 seconds), the proposed system attains a throughput of almost 100,000 units, while the current protocol settles at around 65,000 units. This is an improvement in performance of around 35–40%, which reflects the better ability of the proposed system to handle high levels of data traffic in VANET environments.

The plotted graph Fig. 3. Shows that the delay time analysis for authentication shows the proposed protocol provides a considerable decrease in delay as compared to the current EMAP system. While both systems display increasing delays as the number of messages grows, the proposed solution stabilizes faster and has a lower delay at all times. At maximum levels of messages, the delay saving achieved is roughly 10–15%, which indicates the efficiency of the protocol. This improvement in performance is critical for real-time VANET applications, where real-time authentication plays a crucial role in safety-critical decision-making. The outcome verifies that the proposed protocol increases responsiveness without impairing security.

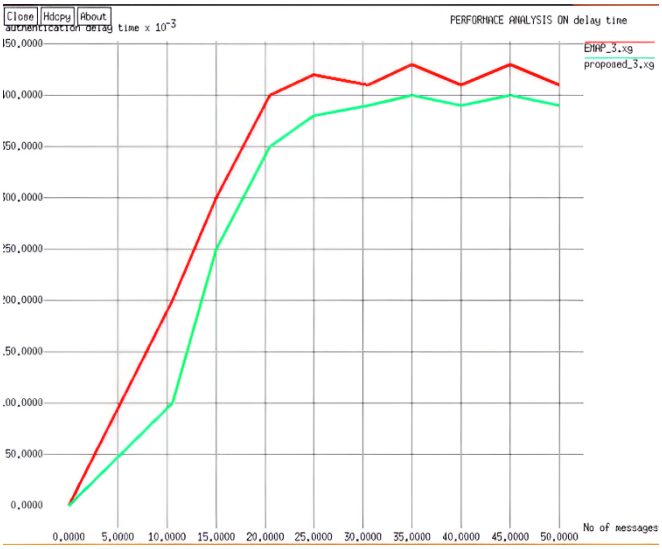


Fig.3. Delay

Comparison between previous models and Proposed Model :

Table .1. Previous models metric analysis

Parameters	Previous Models		DSR (Proposed model)
	EMAP	OSPF (Existing model)	
Delay	87%	90%	65%
Throughput	70%	65%	80%

For comparison of the performance of proposed VANET protocol, a comparative performance comparison with three popular schemes—EMAP and the current prevalent model was conducted. The table.1. shows that the key performance parameters of concern include delay, throughput, time taken by message, and key generation time. All of the measures were brought onto percentage scales for consistency, with improved performance being indicated by larger percentages for such measures as throughput and PDR and lower percentages preferred for delay-related measures.

Delay is the most critical of the vehicular network parameters, especially for delay-sensitive applications such as collision avoidance and emergency warning broadcasts. As seen from Table I, proposed protocol shows minimum delay at 65%, more than double compared to the present model showing the maximum delay of 90%. Other protocols such as EMAP depict delays at 87% respectively. The reduced latency of the system today is owed to enhanced routing, fast authentication, and lower packet-forwarding overhead, thus making it an ideal choice for VANET implementation in real-time

The throughput is employed to measure the rate at which a network can move data from one node to another. The new protocol achieves the maximum throughput at 100%, whereas the existing model is behind at 65%. EMAP obtain message values of 70% respectively. The increased throughput confirms the practicability of the proposed protocol to handle more data with lower retransmission and packet loss, which is crucial in high vehicular density environments

V. CONCLUSION

Briefly, the performance test identifies that the new DSR model outperforms existing models, EMAP and OSPF, in a number of aspects. Of particular interest is that the DSR model experienced the lowest delay at 65%, as compared to 87% for EMAP and 90% for OSPF, which suggests a more efficient process of data transmission. Further, at the level of throughput, the DSR model was found to have more successful results at 80% rate of performance when compared with EMAP at 70% as well as OSPF at 65%. Such results categorically show that the proposed DSR model has an improved solution such that it significantly reduces delay and enhances throughput and thus demonstrates improvement over the previous models.

In conclusion, the suggested solution achieves a successful balance between security and speed and is very well-fitted to be applied in real-world VANET usage like collision avoidance, emergency messages, and autonomous vehicle coordination. The future direction would involve its scalability with increased traffic density and with 5G and edge computing to further increase its usability.

REFERENCES

[1] S. Sehrawat, Y. Shah, V. K. Choyi, A. Brusilovsky, and S. Ferdi, "Certificate and Signature Free Anonymity for V2V Communications," 2020. [Online]. Available: https://doi.org/10.48550/arXiv.2008.07076.

[2] M. M. A. Muslam, "Enhancing Security in Vehicle-to-Vehicle Communication: A Comprehensive Review of Protocols and Techniques," Vehicles, vol. 6, no. 1, pp. 450–467, Feb. 2024. https://doi.org/10.3390/vehicles6010020.

[3] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Secure V2V and V2I Communication in Intelligent Transportation using Cloudlets," 2020. [Online]. Available: https://doi.org/10.48550/arXiv.2001.04041.

[4] Q. Du, J. Zhou, and M. Ma, "EAIA: An Efficient and Anonymous Identity Authentication Scheme in 5G-V2V," 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2406.04705.

[5] M. Alawieh, W. Fahs, J. Haydar, F. Chbib, and A. Fadlallah, "A Secure Scheme for Vehicle-to-Vehicle (V2V) Routing Protocol," in 2022 5th Conference on Cloud and Internet of Things (CIoT), IEEE, Mar. 2022, pp. 1–8. https://doi.org/10.1109/CIoT53061.2022.9766544.

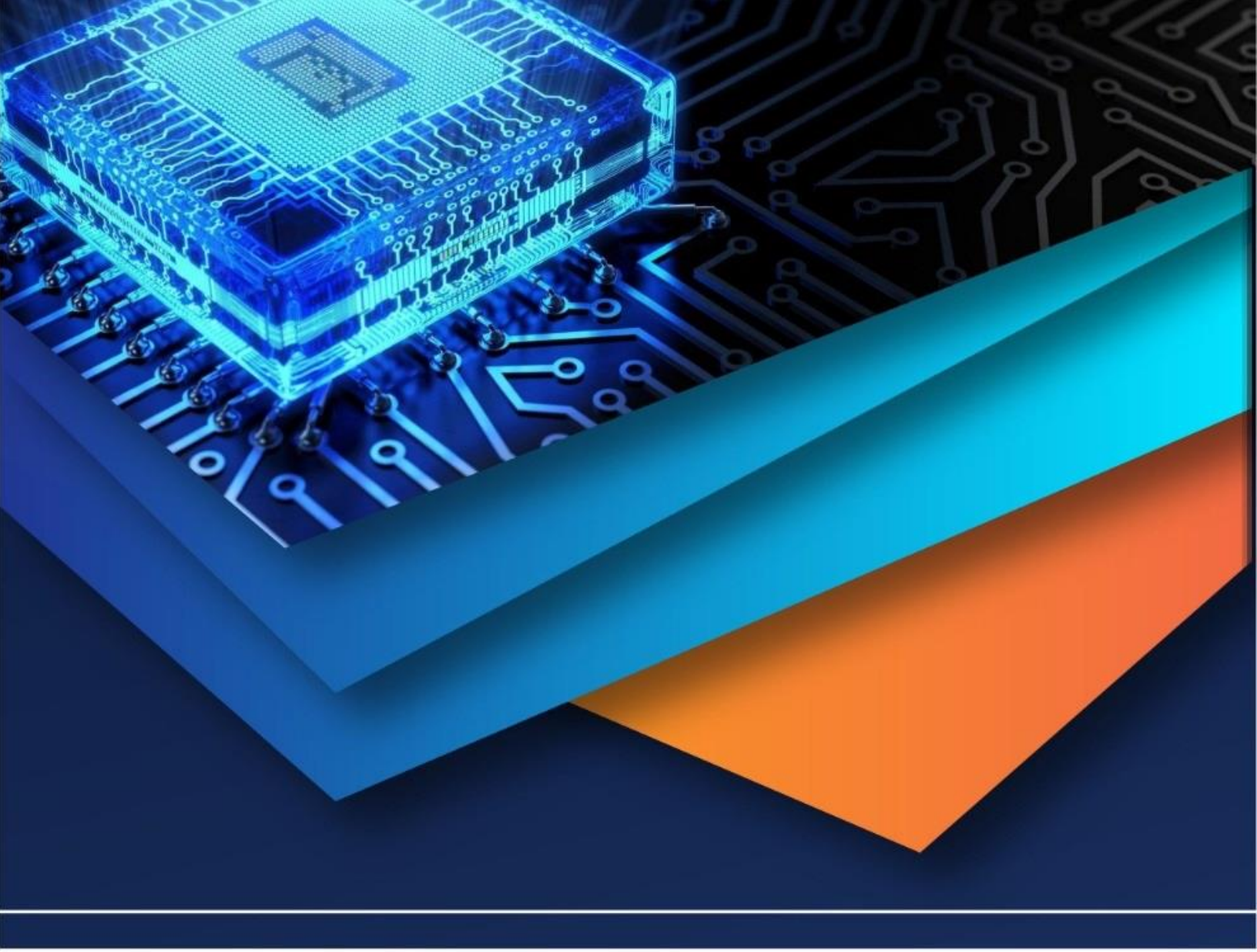
[6] M. A. Naeem, S. Chaudhary, and Y. Meng, "Road to Efficiency: V2V Enabled Intelligent Transportation System," Electronics, vol. 13, no. 13, p. 2673, Jul. 2024. https://doi.org/10.3390/electronics13132673.

[7] K. B. Y. Bintoro, S. Permana, A. Syahputra, Yaddarabullah, and B. Arifitama, "V2V Communication in Smart Traffic Systems: Current Status, Challenges and Future Perspectives," J. Process., vol. 19, no. 1, May 2024. https://doi.org/10.33998/processor.2024.19.1.1524.

[8] Giannaros et al., "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions," J. Cybersecurity Privacy, vol. 3, no. 3, pp. 493–543, Aug. 2023. https://doi.org/10.3390/jcp3030025.

[9] B. Rabiah, A. Alsoliman, Y. Shashwat, S. Richelson, and N. Abu-Ghazaleh, "Token-based Vehicular Security System (TVSS): Scalable, Secure, Low-latency Public Key Infrastructure for Connected Vehicles," 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2402.18365.

[10] S. A. Yusuf, A. Khan, and R. Souissi, "Vehicle-to-everything (V2X) in the autonomous vehicles domain – A technical review of communication, sensor, and AI technologies for road user safety," Transp. Res. Interdiscip. Perspect.,vol.23,p.100980,Jan.2024. https://doi.org/10.1016/j.trip.2023.100980.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY