Real time network monitoring and Traffic Analysis in VANET

Fabiha Tasnim
20-43426-1

Bsc CSE
American University of Bangladesh
Dhaka, Bangladesh
fabihatasnim00@gmail.com

Md Sadik Chowdhury
20-43427-1

Bsc CSE
American University of Bangladesh
Dhaka, Bangladesh
sadikchowdhury770@gmail.com

***Abstract*— Vehicular Ad-Hoc Networks (VANETs) have emerged as a transformative technology for enhancing road safety, traffic management, and communication between vehicles and infrastructure. The study of machine learning approaches, routing protocol, emergency in routing protocol, security , privacy and the system models and simulator tools have covered in this paper. Real-time network monitoring and traffic analysis in VANETs play a pivotal role in ensuring efficient traffic flow and timely response to road incidents. However, these benefits must be balanced with concerns regarding data privacy and security. This paper proposes a novel approach by integrating homomorphic encryption into real-time network monitoring and traffic analysis in VANETs. In this paper the integration of homomorphic encryption into real-time network monitoring and traffic analysis in VANETs presents a promising avenue for achieving the dual goals of efficient traffic management and robust data privacy. This research contributes to the advancement of secure VANETs and lays the foundation for a future where data-driven insights and privacy in vehicular communication systems.**

Keywords*— VANET, Privacy, Security, Homomorphic Encryption, Traffic Management.

I. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) are a specific category of Mobile Ad hoc Networks (MANETs). MANET systems seek to connect mobile devices, typically those moved under human power, to each other to create a network. Another area of mobile networking systems that aimed to connect together objects being moved about by vehicles was developed as a result of MANETs. Initially, this field was considered a sub-category of MANETs, but after further research, it was found that they might discover numerous distinct opportunities while facing many different obstacles. As a result Vehicular Ad-hoc Networks (VANETs) as a result was created to draw attention to some of the peculiar features of this environment. In conclusion, VANETs are wireless networks of automobile devices are produced involuntarily. VANET enables communication between vehicles (V2V - Vehicle-to-Vehicle) and between vehicles and infrastructure (V2I - Vehicle-to-Infrastructure). VANETs are a crucial component of Intelligent Transportation Systems (ITS) and play a vital role in enhancing road safety, traffic efficiency, and overall driving experience. Real-time network monitoring and traffic analysis in VANETs are essential aspects of managing and optimizing these dynamic vehicular networks. As vehicles communicate with each other and the surrounding infrastructure, a vast amount of data is generated, including location information, speed, acceleration, braking, road conditions, and more. In this paper analyzing these data in real-time allows stakeholders such as traffic managers, city planners, and emergency services to make informed decisions and take appropriate actions promptly. In emergency situation by monitoring vehicles helps and immediate action will be taken. This paper will aid to enhance the traffic safety, to congestion of management to improve the efficiency of traffic to response emergency as medical, safety and more to make decision for data-driven. In real-time network monitoring and traffic analysis in VANETs will face challenges that will be worked on this paper that are high mobility, scalability, data accuracy and trustworthiness and privacy and security. Extra approaches will be added to vehicles to contact with every vehicle that will be needed to connect as ambulance, police cars, fire brigades vehicle and more. By leveraging the potential of VANETs and advanced data analytics, smart cities and transportation systems can move towards a safer and more connected future.

II. LITERATURE REVIEW

Shendekar et al. [5] discusses the Vehicular Ad-Hoc Network (VANET) and its applications in communication (V2V & V2I) and safety applications. It analyzes previous work on accident prediction using Machine Learning methods, including SVM, KNN, CNN, Deep learning, and Fuzzy Logic. The paper also examines the benefits and need for in-depth studies on fuzzy logic. The paper outlines various methods for traffic accident prediction models, highlighting contributions, methods, simulations, accuracy, and limitations of previous studies. The application of fuzzy logic methods can help identify the best approach and develop better techniques in VANET. The study serves as a basic and informative lesson for future papers.

Gang Qu et al. [1] reviews the basics of VANETs and their security services, discussing anonymous authentication schemes, trust models, and their properties for efficient trust management. It provides an evaluation of VANET performance and security, integrates simulation platforms, and discusses trust models, simulator tools, security services, and location-based privacy. The paper generalizes the outline of security, privacy, and trust processes in VANETs, avoiding existing surveys on well-researched security topics. The paper provides a comprehensive analysis of various trust management models, focusing on security attacks, fills gaps, and reports recent developments, privacy-preserving authentication and new technique for protecting privacy, trust models, and simulator tools. The study serves as an informative study for privacy preservation and trust management techniques in VANETs.

According to Naeem et al. [3] Vehicle-to-vehicle, vehicle-to-structure, vehicle-to-cloud, vehicle-to-house, vehicle-to-network, and vehicle-to-pedestrian correspondence are crucial aspects of improving road safety, traffic efficiency, and comfortably of vehicles. VEINS Technology can be used for street arrangement plans, distinguishing between connected and non-connected vehicles using Basic Safety Message (BSM) packages. Multiple sensors, including BSM packages, inductive loop, video, and magnetometers, are fused to accurately identify CVs and non-CVs vehicles. Methods include using simulators like SUMO, Network Simulator, and VANET Simulator to reduce road accidents and improve communication range, performance, and reliability. Cellular-based C-V2X technology is superior to WLAN in terms of communication range, performance, and reliability. Hardware-on-top of simulation (HILS) technique captures roadway sensor information from four sources: DSRC broadcast messages, inductive circles, video detectors, and wireless magnetometers. This study aims to detect real-time traffic problems and address them promptly, reducing sudden accidents on road-side areas. By implementing these measures, every part of the road can be properly controlled, ensuring a safer and more efficient transportation system.

Ghori et. al [4] discusses the classification of routing protocols, including geo-based, cluster-based, and topology-based, and their impact on video streaming quality. It also discusses the challenges of good quality video streaming and identifies AODV as a suitable protocol compared to DSR. The paper analyzes existing literature and implements AODV using OPENET, revealing better results than DSR. The paper provides a comprehensive overview of routing protocols and their methodology in VANET, making it effective for beginners. The paper also offers simulations of ADOV and DSR in simple and complex scenarios.

Sheikh and Jun Liang [2] aims to protect the vehicular network from malicious nodes and fake messages by ensuring proper communication between vehicles through On Board Units (OBU) and dedicated short-range communication (DSRC) through Road Side Units (RSU). The system can communicate with neighboring vehicles using sensors, cameras, and GPS, ensuring that transferred messages are not injected or altered by attackers. The paper applies wave layout and five main domains for VANET security requirements, including availability, confidentiality, authenticity, data integrity, and nonrepudiation. Privacy-Preserving Authentication categories authentic schemes to provide a complete structure for VANET application attributes. The paper also provides various types of VANET simulators, such as mobility and network simulators. The survey paper uses various methods to ensure VANET security, address challenges, and gather knowledge about multivariate attacks to defend against future attacks. Organizations working with VANET should follow these security-related approaches to ensure proper security.

Sharma et. al. [6] described to evaluate and compares topological and geographical routing protocols for data-based VANET health monitoring applications. Vehicles can sense health information and transmit it to nearby ambulances, allowing for remote monitoring in hazardous conditions. Wireless Biomedical Networks (WBAN) enables monitoring of physiological parameters like ECG, body temperature, and blood pressure through physical activities. It analyzes AODV, DSDV, OLSR, GPSR,

GPSR-M, and MM-GPSR protocols with different node numbers, CBR connections, communication range, and packet size on Network Simulator (NS-3.23) and Simulation of Urban Mobility (SUMO) platforms. The results provide useful knowledge for analyzing routing protocols for VANET's data-based smart health monitoring applications. The paper explains the WBAN and VANET-based health monitoring framework and research challenges in health monitoring applications. The authors compare the performances of topology-based protocols like AODV, DSDV, OLSR, and position-based protocols like GPSR, MM-GPSR, and GPSR-M for health monitoring application perspectives. The experimental results show that position-based routing protocols perform better than topological protocols in terms of throughput. Topology-based protocols show low AEED but suffer from jitter in high node density networks.

Lee et al. [7] explores the key features of a VANET environment and its applications, focusing on historical and modern perspectives. It examines the current state of VANET technologies and their progress towards successful deployment in real-world applications. The paper highlights the field's unique characteristics and applications, evaluating concepts that have faded into obscurity and those that have recently been conceived. It also discusses research being conducted in developing VANET technology and compares it to previously developed ideas. The paper also discusses the applications that can be implemented with VANET technology and potential new applications not previously considered. The paper provides a longitudinal discussion of VANET applications, providing insight into the origins and future of VANET applications.

III. PRESENT SYSTEM

Vehicular Ad Hoc Network (VANET) using vehicles can connect with one another and with roadside infrastructure using a Vehicular Ad Hoc Network (VANET). The major objectives of VANETs are to improve traffic flow and safety and offer a variety of other services. The current VANET system includes several important elements and technologies, including:

A. Roadside Units (RSUs):

RSUs are fixed communication nodes positioned alongside the roads. They serve as a link between moving objects and the main infrastructure. To keep an eye on traffic and the state of the roads, RSUs can be fitted with a variety of sensors and cameras [2].

B. Vehicles (On-Board Units - OBUs):

Each vehicle has an On-Board Unit (OBU), which is able to communicate wirelessly with other vehicles and infrastructure using technologies including Wi-Fi, DSRC, LTE, and 5G. OBUs also include sensor components like GPS, accelerometers, and cameras to collect data on the condition of the vehicle and its surroundings [2].

C. Trusted Authority:

The entire VANETs' trust and security are managed by TA, who also has the responsibility for determining the accuracy of cars and revoking nodes in the event that a vehicle broadcasts a false message or engages in harmful activity. Consequently, the TA needs to have powerful computing capabilities and enough storage [2].

D. Communication Protocols:

To enable information sharing between cars and infrastructure, VANETs use specialized communication protocols. Common communication standards for VANETs include Dedicated Short-Range Communication (DSRC) and Cellular Vehicle-to-Everything (C-V2X) [3].

E. Safety Applications:

- Collision Avoidance: To prevent collisions, vehicles can communicate information about their position, speed, and direction. The technology can alert both drivers if it anticipates a crash.
- Emergency Vehicle Warning: OBUs can receive alerts from emergency vehicles and provide drivers with plenty of time to vacate the road.
- Traffic management: By exchanging information about traffic conditions, vehicles can assist drivers in choosing routes and avoiding congestion [1].

F. Non-Safety Applications:

- Infotainment: Vehicles have access to local data on attractions, dining establishments, and entertainment alternatives in the area.
- Dynamic route planning: Using real-time traffic information, cars can select the quickest routes in the moment.
- Parking assistance: By sharing information about available parking places, cars can cut down on the time spent looking for a spot [1].

G. Routing Protocol:

Routing protocols in Vehicular Ad Hoc Networks (VANETs) are crucial for efficient and reliable communication between vehicles and infrastructure. These protocols determine how data packets are forwarded from source to destination, considering the unique characteristics of vehicular environments. Commonly used routing protocols include Geographic Routing (GREEDY), Anchor-Based Routing, Position-Based Routing, Adaptive Beacon-Less Position-Based Routing, Geographic Source Routing (GSR), Topological Routing Protocols (VIR), Dynamic Source Routing (DSR), Broadcast-Based Protocols, Probabilistic Broadcasting, Cluster-Based Forwarding (CBF), Vehicle Cluster Routing Protocol (VCRP), Hybrid Protocols (PAR), Geo-0cast Routing, Content-Centric Protocols , and Cross-Layer Geographical Routing (CLGR). The choice of routing protocol depends on the specific VANET application, communication technology, vehicle mobility patterns, and network size. Hybrid solutions that combine the strengths of multiple protocols are often used to address the challenges posed by dynamic vehicular environments [4].

H. Data Fusion and Processing:

In order to extract useful information, the data gathered from multiple sources (vehicle sensors, RSUs, central servers) needs to be processed and fused. Predicting traffic patterns, road conditions, and other pertinent information can be done using machine learning algorithms [5].

I. Security and privacy:

VANETs need to solve security issues such secure communication, message authentication, and user data privacy. To defend against malicious assaults, encryption, digital signatures, and secure key management are crucial [1].

J. Emergency Warning:

VANETs can send alerts to nearby vehicles when an emergency vehicle approaches, providing information about its type, location, and direction. This helps drivers prepare for the vehicle. VANETs Can also manage traffic flow in emergency zones, using dynamic rerouting to divert traffic and reduce congestion. Additionally, VANETs facilitate the dissemination of emergency alerts and notifications, including weather and natural disaster notifications, ensuring road safety [6].

K. Centralized Management System:

A centralized system oversees the whole VANET network, gathers and processes data, and distributes pertinent information to infrastructure and cars. Additionally, this system is capable of issuing orders for emergency response and traffic control [7].

L. Challenges:

VANETs confront difficulties such network congestion, high-speed communication dependability, data privacy issues, and interoperability across various vehicle brands and communication technology [7]**.**

The present system in a VANET is an intricate integration of vehicles, infrastructure, communication protocols, data processing, and applications makes up the current VANET system. Vehicular Ad Hoc Networks (VANETs) face challenges such as communication reliability, scalability, privacy, security vulnerabilities, interoperability, QoS(Quality of service), data fusion, energy efficiency, and regulatory frameworks. Communication reliability is crucial for real-time applications like emergency notifications and traffic updates, while scalability and security are issues. Interoperability requires standardized approaches, while QoS and energy efficiency are essential for efficient data management. Real-world validation is crucial for bridging the gap between simulations, protect personal and sensitive data and practical implementation. Additionally, regulatory and policy frameworks present challenges in spectrum allocation, privacy regulations, and liability considerations. Further improvement in VANETs is necessary to create more reliable, secure, and efficient networks, revolutionizing road safety, traffic management, protection of sensitive and personal data and driving experiences. Through real-time communication and wise decision-making, it seeks to increase traffic efficiency, road safety, and overall driving pleasure.

IV. ANALYSIS

Analysis is needed to conduct analysis to evaluate the effectiveness, dependability, and efficiency communication protocols and routing algorithms created especially for vehicle contexts. Analysis measures the efficiency of security measures, guaranteeing that private data is kept secure and the network is resilient to future online threats. Analysis aids in the design of systems that reliably convey emergency warnings and permit effective coordination between vehicles and emergency services, which is essential in emergency situations where quick and precise information dissemination is essential. Analysis opens the path for safer, more effective, and technologically advanced vehicular communication networks by revealing insights about VANET behavior, difficulties, and potential solutions.

Paper's Title	Features	Method	Usability	Limitations
1. A survey on recent advances in vehicular network security, trust, and privacy. [1]	• Security services with their threats and attacks. • Idea of OBU,RSU and TA of VANETs. • Three types of trust models and efficient trust management in VANETs. • Elaborates the idea of trust model, simulator tools, trust management, security service and location-based privacy in	• Generalizes several processes of security, privacy and trust. • Provides new techniques for protecting privacy and trust models, fills in the gaps, and reports recent developments. • Simulation tools, authentication schemes and trust management models have been approached.	• Overview of VANETs privacy, security and trust survey. • Classifications of security attacks, privacy-preserving authentication, trust models, simulator tools can help identify threats and develop better approach. • An informative study for privacy preservation and trust management technique in VANETs.	• No real life implementation or experiment of trust model and simulator. • Specific details process of Simulator tools but no description of working details in real. • Less focus on privacy preservation technique and sensitive data protection.
2. A comprehensive survey on VANET security services in traffic management system [2]	• Protect from malicious nodes and fake messages. • communicate with other vehicles Through OBU (On Board Unit). • contain the network devices for dedicated short-range communication (DSRC) through RSU (Road Side Unit). • Communicate by sensors, GPS, cameras. • Provides	• different wireless communication frequency channel for Control full VANET system properly. • apply wave layout & use five main domains such as (availability, confidentiality, authenticity, data integrity, and nonrepudiation). • Authentic schemes to provide a complete structure how VANET	• security challenge address properly. • knowledge about multivariate attack, for defend future attacks.	• Only provides the idea and no experiments in real. • Lack of VANET Emergency support roadway. • No specific details of simulators working process.

	VANETs security.	application attribute will be design. • simulators like:(mobility simulator and network simulators).		
3. Vehicle to everything (V2X) communication protocol by using vehicular AD-HOC network [3].	• V2V, V2I, V2X (Vehicle to everything) • VEINS technology used for maps to utilize street arrangement plans. • Connected vehicles (CVs) and non-connected vehicles (non-CVs), and filtering algorithm using Basic Safety Message (BSM) packages. • Multiple sensors like (BSM packages, inductive loop, video, and magnetometer) are fused to accurately identify CVs and non-CVs vehicles	• Used simulator like SUMO, Network Simulator, VANET Simulator. • Cellular-based C-V2X technology is superior to WLAN based in terms of communication range, performance, and reliability. • (HILS) technique that capture roadway sensor information from four different sources DSRC broadcast messages, inductive circles, video detectors, and wireless magnetometers.	• Emergency traffic like medical vehicle or others emergency transport don’t have to wait a long time in road. • Decrease sudden accident on road-side area through this traffic. • Under control of the roads.	• Identification of CVs and Non-CVs term to find particular vehicle is registered or not under VANET Server.. • No implementation as explanation. • No central control.
4. VANET routing protocols: review, implementation and analysis [4]	• Definition and method of routing protocol. • classifications of routing protocol like Geo-based routing, Cluster Based Routing Protocols, Topology Based Routing Protocols and so on. • AODV by OPENET is	• Best approachable protocols. • Implements by OPENET. • AODV which is perform well than DSR by simulation.	• overview of routing protocol and its methodology in VANET effective. • Provides better result of routing protocol. • Simulation of routing protocol like ADOV and DSR in simple and complex	• No discussion about privacy, security of VANETs. • Lack of real-world examples and implementation

	suitable protocol than DSR.		scenario	
5. Traffic Accident Prediction Techniques in Vehicular Ad-hoc Network: A Survey [5]	• V2V & V2I • Machine Learning technique • SVM, KNN, CNN and fuzzy logic approach. • Benefits of fuzzy logic approach.	• Using SVM, NN, CNN, KNN, Deep Learning method • Accuracy of methods, and find Fuzzy Logic approach to be better.	• Develop better technique using these approaches. • Predict accident and take necessary steps to prevent it. • Informative paper for further study.	• Qualitative and not quantitative. • No explanation of Fuzzy Logic technique used and its method. • Lack of concepts, works-activity, and specific technical tools, simulator tools are not providing
6. Evaluation of VANETs routing protocols for data-based smart health monitoring in intelligent transportation system [6]	• Routing protocols used and resolve communication-related issues in emergencies using VANET. • Analysis of topology-based and position-based routing protocols. • Execute AODV, DSDV, OLSR, GPSR, GPSR-M, and MM-GPSR protocols in NS-3.23 by creating road network simulation.	• Health monitoring applications and the WBAN and VANET based health monitoring system. • topology-based routing protocols like AODV, DSDV, OLSR, and position-based routing protocols like GPSR, MM-GPSR, and GPSRM for health monitoring application perspectives. • Traffic simulator used Ubuntu 18.04 LTS operating system, NS3.23 Network Simulator, SUMO-0.32.0. • position-based routing protocols perform better than topological protocols	• In VANETs routing protocols are used for emergencies. • Position –based routing protocol is better and emergencies this method will work. • The simulators and protocols are used.	• Health emergencies working process did not described properly. • No implementation of routing protocols in real life. • Authentication of emergency notifications did not clarify.

V. PROPOSED IDEA

After analyzing the papers the major target of VANETs is to enhance the traffic safety and management of vehicles and traffic and protect the data and have privacy, security and trust and in VANETs. The system models including OBU, RSU and TA of VANETs introduced more precisely to preserve the system. The most used techniques for routing is AODV and DSR. And for predicting accidents SVM, KNN and CNN is the best machine learning approaches but fuzzy logic technique gives better result. For maintaining the privacy and security simulators like SUMO, network simulator, mobility simulator have demonstrated. For emergency situations position-based routing protocol gives better response. But papers are only illustrated the privacy ideas and simulators but do not clarify the methods properly. In this paper, Homomorphic Encryption will define the method of privacy and security more precisely in VANETs. Homomorphic encryption is an innovative cryptographic method created to allow secure computations on sensitive data while keeping it encrypted. In order to secure data while keeping its usability, homomorphic encryption, a ground-breaking cryptographic technology, has important applications in vehicular ad-hoc networks (VANETs). With homomorphic encryption, sensitive data can be encrypted in VANETs so that calculations can be made directly on the encrypted data without the need for decryption. When protecting privacy while enabling data-driven insights and analysis, this is especially important. The working process of homomorphic encryption in VANETs involves several key steps. First, when a vehicle collects sensitive data, such as location information or personal identifiers, it encrypts the data using a homomorphic encryption scheme. This encrypted data retains its mathematical structure enabling certain mathematical operations to be performed on it even in its encrypted form. This is in contrast to traditional encryption, where data must be decrypted before any computation can take place. When encrypted data needs to be processed, such as in traffic analysis or statistical computations, authorized parties, such as traffic management authorities it can perform operations on the encrypted data without having to decrypt it first. In the VANET context, this means that aggregated traffic information, route optimization, or other computations can be performed on encrypted data without revealing the individual vehicle identities or precise locations. The results of these operations remain encrypted until the authorized party decrypts them to obtain the final outcome. This process enhances the privacy of VANET participants while still enabling data-driven decision-making. The encrypted nature of the data ensures that even if the encrypted information is intercepted or accessed without authorization, it remains unintelligible without the decryption keys. Homomorphic encryption in VANETs thus strikes a balance between data security and utility, fostering a safer and more privacy-conscious vehicular communication ecosystem.

VI. DISCUSSION

Homomorphic encryption in real-time network monitoring and traffic analysis in Vehicular Ad-Hoc Networks (VANETs) offers a promising solution for enhancing data privacy and informed traffic management decisions. However, it faces limitations such as computational overhead, limited allowable operations, key management, scalability, and balancing accuracy and privacy preservation. Additionally, integrating homomorphic encryption requires overhauling existing VANET architectures and considering the trade-off between security and usability. In this paper, the idea homomorphic encryption cannot implement in real and no mathematical calculation of VANETs. Despite these challenges, homomorphic encryption holds promise for securing VANET traffic analysis, but ongoing research and innovation are needed to effectively address these challenges.

The future of real-time network monitoring and traffic analysis in Vehicular Ad Hoc Networks (VANETs) holds significant potential through the integration of homomorphic encryption. As technology evolves, the exploration of homomorphic encryption techniques can address the crucial concerns of rivacy and security. Advanced research in this domain could lead to the development of novel methods that enable enpcrypted data to be analyzed in real-time without compromising the sensitive information it contains. This would facilitate privacy-preserving data sharing, secure authentication, and robust traffic analysis, all while safeguarding individual data. The challenge lies in optimizing the computational overhead associated with homomorphic encryption to ensure efficient processing in the dynamic and time-sensitive VANET environment. By combining the power of real-time monitoring and traffic analysis with the benefits of homomorphic encryption, the future of VANETs could encompass a new era of secure, privacy-aware, and efficient vehicular communication systems. In additional, block chain and zero-knowledge proof method can be more relatable for data security where without decrypting the data the necessity will be done.

VII. CONCLUSION

In conclusion, the field of real-time network monitoring and traffic analysis in vehicular ad hoc networks (VANETs) has enormous promise for modernizing transportation systems. Real-time data from vehicles and infrastructure may be collected and analyzed owing to the integration of cutting-edge technologies; this information is useful for understanding traffic patterns, traffic congestion, and safety concerns. Future vehicular communication systems have both potential and challenges as a result of the integration of real-time network monitoring, traffic analysis, and homomorphic encryption in Vehicular Ad Hoc Networks (VANETs)., such as computational complexity, interoperability challenges, and the trade-off between security and data value. The advantages of protecting individual privacy while allowing secure data analysis have enormous promise for improving the overall effectiveness and security of VANETs. The actual application of homomorphic encryption in VANETs, necessitates overcoming a number of constraints, such as computational complexity, interoperability challenges, and the trade-off between security and data value. As researchers, industry professionals, and policymakers collaboratively address these challenges, the envisioned future of VANETs emerges as a landscape where real-time analysis thrives under the protective umbrella of homomorphic encryption, ultimately contributing to safer, more efficient, and privacy-aware transportation ecosystems.

VIII. REFERENCES

[1] Lu, Zhaojun, Gang Qu, and Zhenglin Liu. "A survey on recent advances in vehicular network security, trust, and privacy." *IEEE Transactions on Intelligent Transportation Systems* Vol 20.2, pp. 760-776, 2018.

[2] Sheikh, Muhammad Sameer, and Jun Liang. "A comprehensive survey on VANET security services in traffic management system." *Wireless Communications and Mobile Computing* 2019 (2019), pp. 1-23.

[3] Naeem, Muhammad Ahtsam, et al. "Vehicle to everything (V2X) communication protocol by using vehicular AD-HOC network." *2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*. IEEE, (2020).

[4] Rizwan Ghori, Muhammad, Ali Safa Sadiq, and Abdul Ghani. "VANET routing protocols: review, implementation and analysis." *Journal of Physics: Conference Series*. Vol. 1049, 2018.

[5] Shendekar, Shweta, Samrat Thorat, and Dinesh Rojatkar. "Traffic Accident Prediction Techniques in Vehicular Ad-hoc Network: A Survey." *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2021.

[6] Sharma, Suresh Kumar, et al. "Evaluation of VANETs routing protocols for data-based smart health monitoring in intelligent transportation systems." *International Journal of Mathematical, Engineering and Management Sciences* , Vol 7.2, pp. 211, 2022.

[7] Lee, Michael, and Travis Atkison. "Vanet applications: Past, present, and future." *Vehicular Communications* vol 28 pp. 103-130, 2021.