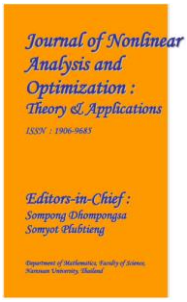
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.20 : 2024
ISSN : **1906-9685**



MITIGATING BROADCAST STORM IN VANETS THROUGH KEY-BASED MESSAGE TRANSMISSION

R. Shiddharthy Assistant Professor, Nallamuthu Gounder Mahalingam College, Pollachi. E-mail: gurushiddharthy@gmail.com

Abstract
Vehicular Ad Hoc Networks (VANETs) use low-cost wireless communication technologies to relay traffic information to nearby vehicles. One of the main objectives of Intelligent Transportation Systems (ITS) is to disseminate road information to vehicles promptly to reduce the risk of accidents. When a vehicle receives information from its neighbor, it becomes part of the VANET, helping to control and forward the received information to other nearby vehicles. This paper proposes a design to mitigate broadcast storms, named Key-Based Message Broadcast for VANET (KMB-V). This method forms small clusters of vehicles, each with a Cluster Head (CH), and utilizes a unique key for message transmission to avoid broadcast storms. The proposed approach demonstrates superior performance in terms of Packet Delivery Ratio (PDR), network lifespan, and throughput compared to previous methods.

Keywords
VANET, ITS, Broadcast Storm, key-bases message broadcast, PDR

Introduction

Vehicular Ad Hoc Networks (VANETs), a subset of Mobile Ad hoc Networks (MANETs), heavily rely on broadcasting transmissions for communication. These networks facilitate the exchange of traffic information among neighboring vehicles through affordable wireless communication technologies. VANETs employ a peer-to-peer network infrastructure, known as Intelligent Transport Systems (ITS), to enable data transmission between vehicles. The primary objective of ITS is to enhance safety for drivers, passengers, and vehicles by promptly sharing road information to mitigate the risk of accidents [1].

In VANETs, when a vehicle receives communication from its neighboring vehicle, it becomes an integral part of the network, responsible for controlling and forwarding the received information to other nearby vehicles. VANETs consist of mobile nodes equipped with sensors, as well as Road-Side Units (RSUs) designed to access data from vehicles and relay it to passing vehicles through wireless intercommunication [2].The architecture of VANETs encompasses On-Board Units (OBUs) facilitating Vehicle-to-Vehicle (V2V) communication, as well as communication with fixed street units known as RSUs, termed Vehicular-to-Infrastructure (V2I). In certain scenarios, both V2V and V2I transactions are combined to form a hybrid architecture [3].

Three distinct types of communication are prevalent in VANETs, namely V2V transactions, V2I transactions, and hybrid transactions combining both V2V and V2I communication modes.

Vehicle-to-Vehicle Communication (V2V)

Vehicle-to-Vehicle Communication (V2V) facilitates direct communication between vehicles, enabling them to exchange crucial data such as speed, position, and traffic information without the need for any intermediary medium. The primary objective of this communication is to enhance safety on roads by enabling vehicles to share real-time information and thereby avoid potential accidents.

This system operates through On-Board Units (OBUs), which serve as the communication interface for transmitting and receiving data between vehicles [3].

Vehicle-to-Infrastructure Communication (V2I)

In this communication framework, vehicles are enabled to exchange information with Roadside Units (RSUs). This interaction is bidirectional, allowing both the vehicle and the RSU to share relevant data between them. Acting as a reliable information hub, the RSU disseminates collected data to vehicles as they enter its radio range. Furthermore, the RSU plays a pivotal role in suggesting both security and non-security functionalities for the on-board units (OBUs) installed in vehicles [2],[3].

Hybrid Architecture

This architectural model combines Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. It enables vehicles to communicate with both Roadside Units (RSUs) and nearby vehicles for the exchange of information. This setup supports both single-hop and multiple-hop communication, accommodating high node mobility and facilitating rapid network topology adjustments within a limited mobility design. Additionally, it operates under the assumption of an infinite power supply. The effectiveness of Vehicular Ad-Hoc Networks (VANETs) is contingent upon the transmission of messages among vehicles, a process influenced by the high mobility of nodes, which necessitates frequent routing and topology modifications [3]. For a visual representation of this simplified VANET architecture, refer to Figure 1.

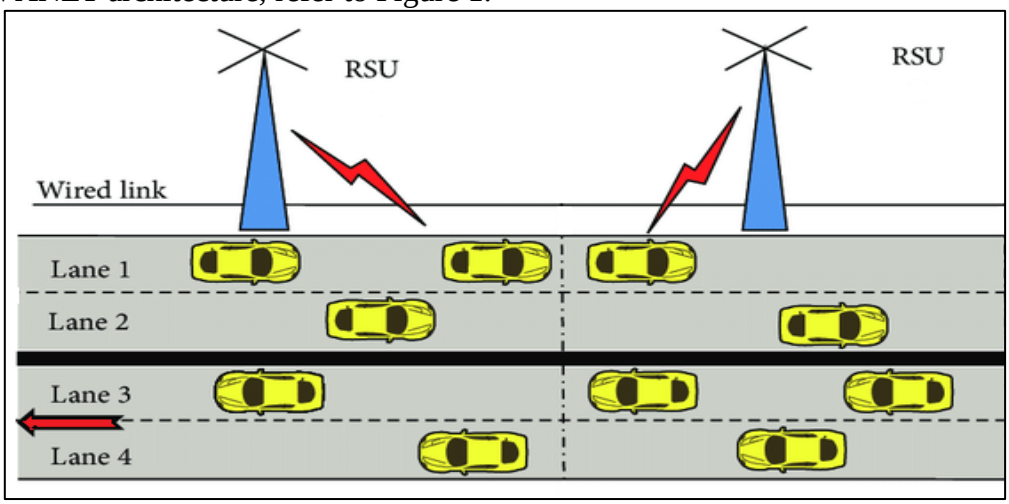


Figure 1: Simple Architecture for VANET

Some research efforts have concentrated on examining the robust connectivity inherent in Vehicular Ad-Hoc Networks (VANETs), particularly in regions characterized by high vehicular traffic density. However, the reception of redundant messages from both vehicles and Roadside Units (RSUs) often results in resource wastage, encompassing costs and time (Source: [4]). The proliferation of redundant messages can instigate a broadcasting storm, a hazardous scenario for VANETs, which imperils the network's design and reliability. To address this challenge, a novel design is proposed in this paper, termed Key-Based Message Broadcast for VANET (KMB-V), aiming to mitigate the broadcasting storm phenomenon.

This KMB-V approach involves the formation of clusters comprising a minimal number of nodes (vehicles) with designated Cluster Heads (CHs). By constraining the number of transmissions, this KMB-V method establishes a highly efficient broadcasting mechanism and resulting in enhanced propagation speed and overall network performance (Source: [5]). The subsequent section of this research is structured as follows: Section 2, Related Work, provides an overview of various protocols and prior investigations. Section 3 delineates an evaluation scenario for the proposed protocol and outlines the algorithms under assessment, along with their explanations. Section 4 conducts a comparative evaluation of the proposed methodology's performance. Finally, Section 5 presents the conclusions drawn from the study.

Related Work

The author [6] details the intra-cluster routing protocol, which is a hybrid protocol that partition a massive network into a tiny cluster. The CHs are elected through usual technique and it is responsible for communication between the cluster members and nearby CHs. The high responsibility of the CH is to find out the optimal route to reach each cluster members. Generally, cluster decreases the control overhead and it expands the size of the network.

In paper [7] suggested a cluster-based directional routing algorithm for public transportation. Constrained variables such as direction, location, and acceleration have been calculated and considered in deciding on CH. The proposed protocol in [8] relies on movement as a parameter and attempts to maintain the CHs as a constant object. This reduces communication overhead and the MAC layer argument while maintaining an excellent Packet Delivery Ratio (PDR). To select CH, the greedy traffic-aware routing protocol (GYTAR) and a crossroad-based routing protocol are proposed.

Similarly the [9] proposed Greedy Perimeter Coordinator Routing (GPCR) convey a tiny packet of information using a direct route to a destination in an intersection. The researchers also discuss the volume and load conscious VANET protocols that outperform the other protocols. When compared to GYTAR and AODV, the idea for IRTIV is a position-based routing protocol that tries to minimize end-to-end delay. It determines the immediate rate of vehicular traffic and the related path to the target.

In [10], the author presented a Beacon Less Routing algorithm for Vehicular Environment (BRAVE) to reduce overhead communication when broadcasting. In [11], CHEF guarantees that the nodes are optimized and that sufficient energy levels are selected for CH. CH proposed a collecting approach that proposes and enhances fuzzy logic rules over time. This CHEF follows four fuzzy rules that are primarily focused on the Base Station (BS), the module's remaining energy, and node awareness with local distance.

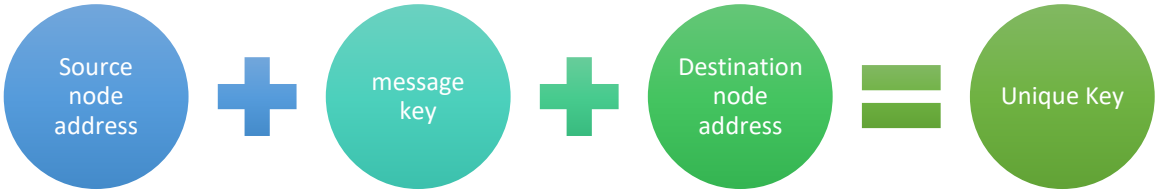
Proposed Work

The proposed work key-based message broadcast for VANET (KMB-V) generates a unique key for each message transmission to avoid message-broadcasting storm whereas the message must be deliver to the all possible vehicles with high reliability and minimum delay.

Key-Based Message Broadcast for VANET (KMB-V)

The key-based message broadcast for VANET (KMB-V) proposes an algorithm to overcome the network from broadcast storm through sharing a unique key for each message transmission. The key consists of three identification alphanumeric unique numbers for each transmission. Figure 2 presents a unique key structure.

Figure 2: Proposed Unique Key Structure



Source node address is the address of a source vehicle (8 bit), which is going to transmit the data to the destination vehicle or to RSU. Message key consists of 8 bit key combination from the original message and destination node address is the address of the destination vehicle (8 bit).

Generally, each node (vehicle) forwards a hello packet to its CH to join into the cluster. While sending the hello packet itself, the unique node address is generated and forwarded to the concern node. Likewise, for each RSU, the node generates a special address to identify the RSU.

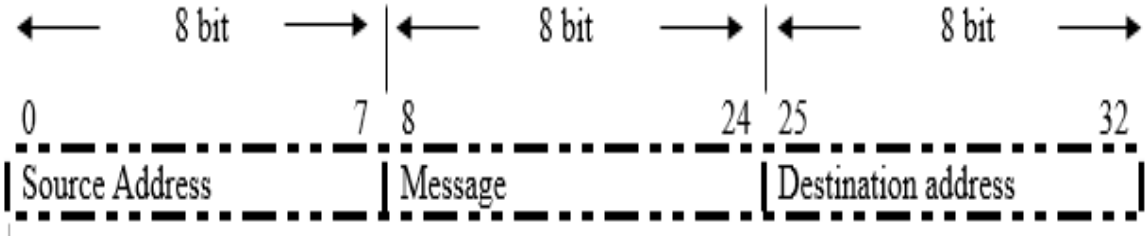


Figure 3: Unique Key Message Format

Figure 3 presents the unique key message format for each data transmission. Instead of sending the same messages repeatedly, this unique format easily identifies that the message is received already and alerts the sender that message was received early. When a sender receives alert from most of the node then, the receiver stops forwarding the message to other nodes. Figure 4 shows the working structure of the proposed work.

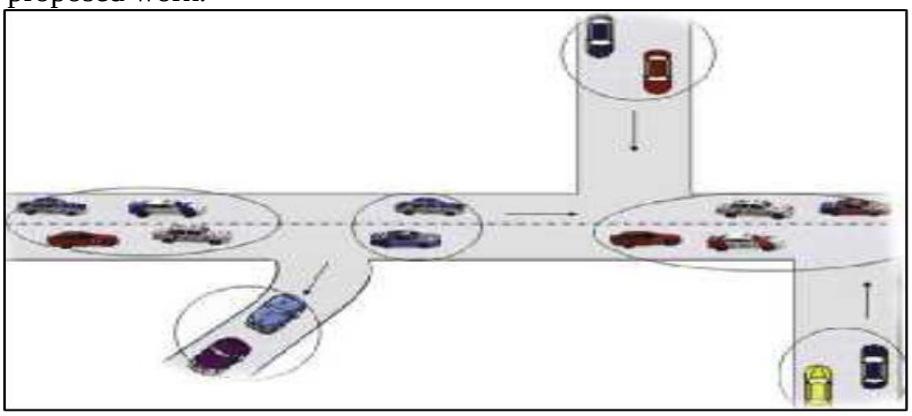


Figure 4: Working structure of the proposed work

This proposed work follows traditional LEACH (Low Energy Adaptive Clustering Hierarchy) to elect CH. The CH election is processed in two phases namely Set-up Phase and Steady Phase. Setup phase elects CH based on the chosen value between 0 (Zero) to 1 (one). In next phase, which is steady phase the CH election is based on the performance metrics such as distance between nodes, distance to RSU, number of transmitted vehicles of a node and so on. Therefore, the broadcasting storm detains the performance of the network and as well, it reduces the lifetime of the network to some extent. The algorithm is proposed in steady phase to elect better CH based on the unique key data transmission,

Algorithm

Key-based Message Broadcast Algorithm

Step – 1: Unique value between 0 to 1 is assigned to all node through LEACH's dynamic value allocation as in setup phase.

Step – 2: Threshold value is identified using

$$T(n) = \frac{P}{1-P\times(r \bmod \frac{1}{P})} \quad \forall n \in G$$

Step – 3: Node that holds nearer or equal value to the threshold value is elected CH for the initial round

Step – 4: Initialize the CH and send message to nearer vehicles to form cluster

Step – 5: Cluster members forwards the unique node address to each other to forward/receive Messages between the vehicles.

Step – 6: Once the node addresses are transmitted, the key generation will be processed.

$$key = Source_{addr} + \frac{original_{msg}}{Key_{gen}} + destination_{addr}$$

Where, $Source_{addr}$ is source address of the node and $destination_{addr}$ is destination address of the node. $original_{msg}$ is original safety event message content of (254 bytes) and Key_{gen} is the key generation process consist of 254 bytes alphanumeric keys that generate a unique key of size 8 bit (1 byte by 254 bytes message content/254 alphanumeric keys)

Step – 7: Start message transmission by transmitting unique key to all nearby nodes

Step – 8: Destination node checks the unique key with received key to identify the uniqueness of the key.

Step – 9: IF key is unique, the destination node sends the ACK (acknowledgement) and the original message will be forwarded

ELSE key is not unique then the destination node sends an alert message stating that the message is already received to the sender. Whenever, the alert message is received, the transmission of the particular message is stopped.

Step – 10: Stop the process

Figure 5: Key-based message broadcast algorithm

The algorithm outlined in Figure 5 illustrates the process of message transmission among vehicles. Upon forwarding or receiving node addresses from nearby vehicles, the message exchange ensues. Subsequently, once nearby addresses are gathered, nodes harboring messages for the clusters dispatch them. In response, cluster heads (CH) and other cluster nodes issue acknowledgments (ACKs) upon receipt of new messages, whereas already received messages trigger alert messages back to the sender. Upon receiving a sufficient number of alert messages (60% or more), the sender ceases forwarding the original message to the recipient, redirecting it instead to nodes that haven't sent alerts. This measure helps avert broadcasting storms by eliminating redundant message transmissions.

Results and Discussion

The proposed work focuses in minimizing the broadcast storm in VANET that improves the network lifetime, packet delivery ratio, and Throughput. Table I displays different simulation parameters used in the proposed work.

Table I: Simulation Parameters of the proposed work

PARAMETERS	VALUE
Channel	Wireless channel
Antenna	Omni/Directional Antenna
MAC Protocol	IEEE 802.11
Routing Protocol	LEACH
No. of Nodes	100
Simulator	NS 2.35
Simulation Time	3600 Sec
Protocol	KMB-V LEACH
Traffic Status	Continuous arrival

The proposed work is compared with the existing schemes to identify the performance of the proposed KMB-V LEACH in network lifetime, Packet Delivery Ratio (PDR), and Throughput. Network lifetime is an essential factor for a network to continue the purpose of developing such network without any pitfalls.

However, the improvement in lifetime definitely improves the performance of the PDR. The better selection of correct nodes as CH in terms improves the purpose of this network, in such a way the proposed work concentrates in improving the correct selection of CH and member nodes for betterment of the network.

The Figure 5 shows the network lifetime of the proposed and existing schemes.

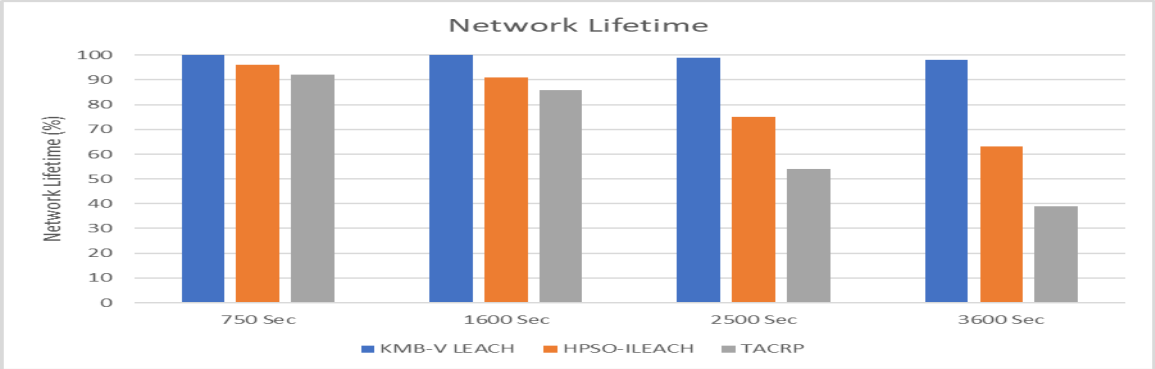


Figure 5: Network Lifetime

The proposed KMB-V LEACH attains a maximum of 96 % lifetime after 3600 Sec of simulation, whereas the existing schemes HPSO-ILEACH [10] and TACRP [11] maintains 54% and 32 % respectively.

The Figure 6 presents throughput between the proposed and existing schemes as well.

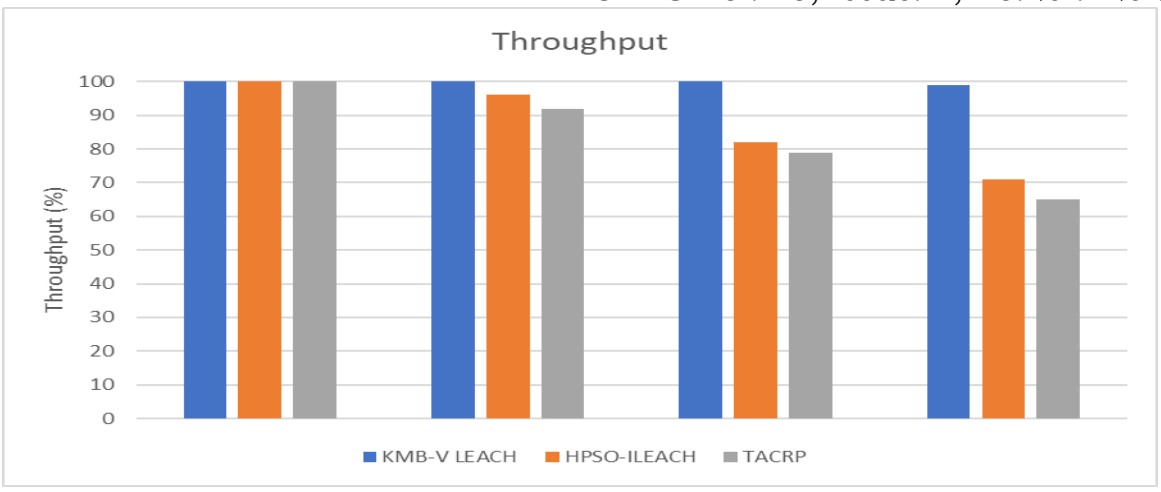


Figure 6 Throughput

Throughput is to measures the correct selection of CH, member nodes, transmission of correct message after key transmission and so on. This parameter identifies that the proposed KMB-V LEACH maintains 98% of throughput stating that for every 100 connectivity 98 connections were connected successfully and transmitted new information or correctly identified as older one. However, the existing schemes throughput is reduced to 52% (HPSO-ILEACH) and 35 % (TACRP). The lesser throughput percentage states that lesser connectivity, lesser message transmission and higher old message key transmission and so on.

Figure 7 shows the Packet Delivery Ratio between the schemes.

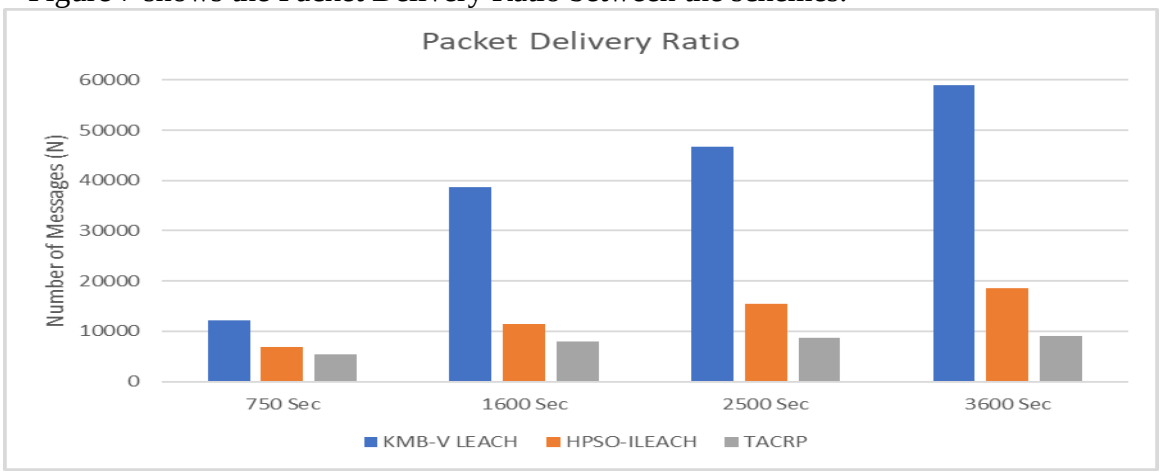


Figure 7: Packet Delivery Ratio

The PDR of proposed work is 31% higher than the HPSO-ILEACH protocol and slight higher to TACRP protocol. The proposed work outperforms due to unique key formation that avoids broadcast storm as well as improves the lifetime, throughput and PDR ratio to the betterment of the VANET.

Conclusion

Vehicular Ad Hoc Networks (VANETs) play a crucial role in disseminating real-time road and passenger safety information efficiently. However, the swift transmission of data can lead to inefficiencies due to broadcast storms, where messages are forwarded repeatedly. To mitigate this issue, the proposed solution emphasizes the generation of unique keys for each message transmission. These keys are forwarded along with the message to destination nodes, allowing them to identify whether the message has already been transmitted.

If the message is detected as already received, the destination node sends an alert message to prevent redundant broadcasting. When a sender node accumulates 60% or more alert messages, the original message is discarded from the transmission list. This approach demonstrates superior performance across parameters such as Packet Delivery Ratio (PDR), network longevity, and throughput compared to existing methodologies. Looking ahead, integrating key transmission with security features holds promise for detecting and mitigating malicious nodes within VANETs.

References

1. Lakshmi, K., & Soranamageswari, M. (2023, October). Enriched Model of Pigeon Inspired Pseudonym Generation for Privacy Preservation of Vehicles Location in VANET. In *2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 173-177). IEEE.
2. Peyman, M., Fluechter, T., Panadero, J., Serrat, C., Xhafa, F., & Juan, A. A. (2023). Optimization of vehicular networks in smart cities: from agile optimization to learnheuristics and simheuristics. *Sensors*, *23*(1), 499.
3. Varma, I. M., & Kumar, N. (2023). A comprehensive survey on SDN and blockchain-based secure vehicular networks. *Vehicular Communications*, 100663.
4. Kumar, S. (2023, December). Improved Tree-Based Data Dissemination Protocol to Prolong Lifetime of Sensor Nodes for Internet of Things. In *2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC)* (pp. 997-1002). IEEE.
5. Ghodichor, N., Sahu, D., Borkar, G., & Sawarkar, A. (2023). Secure Routing Protocol To Mitigate Attacks By Using Blockchain Technology In Manet. *arXiv preprint arXiv:2304.04254*.
6. Usha, M., Sathiamoorthy, J., Ahilan, A., & Mahalingam, T. (2023). SWEEPER: Secure Waterfall Energy-Efficient Protocol-Enabled Routing in FANET. *IETE Journal of Research*, 1-15.
7. Tao, Y., Du, H., Xu, J., Su, L., & Cui, B. (2023). On-Demand Anonymous Access and Roaming Authentication Protocols for 6G Satellite–Ground Integrated Networks. *Sensors*, *23*(11), 5075.
8. Ji, S., & Mishra, A. K. (2024). 5G Network Implementation: A Survey on Security Issues, Challenges, and Future Directions. In *Developments Towards Next Generation Intelligent Systems for Sustainable Development* (pp. 62-88). IGI Global.
9. Abdulkader, O. (2024). An Efficient Congestion Control Model Based on VSR for BSM Broadcasting in VANET. *Indian Journal of Science and Technology*, *17*(1), 90-96.
10. Ahmed, H. A., & Cheelu, D. (2024, March). A Comparison of Message Broadcast Protocols for Reliable Broadcasting in Vehicular Ad hoc Networks. In *2024 International Conference on Automation and Computation (AUTOCOM)* (pp. 347-351). IEEE.
11. Debalki, Y. A., Hou, J., Adane, B. Y., Mawutor, V. G., & Dang, H. (2024). A distributed relay selection using a fuzzy-BCM based decision making strategy for multi-hop data dissemination in VANETs. *Wireless Networks*, 1-22.