ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2024.0479

REVOLUTIONIZING VANETS WITH GRAPH NEURAL NETWORKS USING DYNAMIC TRAFFIC MANAGEMENT

M. Umaselvi[1], S. Leena Maria[2], M.J. Sridevi[3], B. Gayathri[4] and Khaled A. A. Alloush[5]

[1]Department of Computer Science Engineering, P.A. College of Engineering and Technology, India
[2]Department of Mathematics, Government Engineering College, Hassan, India
[3]Department of Mathematics, Government First Grade College for Women, India
[4]Department of Computer Science, Bishop Heber College, India
[5]Department of Computer Science, Arab Open University, Saudi Arabia

Abstract

The increasing movement from rural areas to urban areas, along with the widening gap in population, has resulted in metropolitan areas becoming extremely overpopulated. As a result of the high volume of traffic that occurs in these areas, traffic monitoring is an extremely important activity. According to the findings of this study, an improved authentication and communication protocol that is based on clusters could be implemented for Intelligent Transportation Systems in Vehicular Ad Hoc Networks (VANETs). Our number one objective is to enhance the sharing of resources amongst vehicles through improved communication. Cluster-based routing protocols allowed us to increase the scalability, stability, and dependability of fast-moving VANETs. This was accomplished in the context of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. To easing concerns regarding privacy and safety, we arranged for the vehicles to be certified by an independent contractor. Through the utilization of Graph Neural Networks (GNNs), we can reduce the number of instances in which links fail, as well as minimize end-to-end (E2E) delays and route requests. Our approach has resulted in several important benefits, including enhancements to throughput, reductions in the amount of time required for TCP socket initialization, acceleration of TCP handshake response, and DNS lookup. Short-range peer-to-peer wireless communication is the focus of the protocols that are used within a cluster that is 400 meters in radius. Utilizing new peer-to-peer wireless communications over VANET is what is meant by the term resource-conserving in this context. Within the framework of the suggested protocol secure authentication method, a certifying authority is responsible for the generation of a secure authentication key for the vehicle, which is subsequently provided to the vehicle.

Keywords:

VANETs, V2V, Graph Neural Network, TCP

1. INTRODUCTION

At an increasing rate, people are leaving rural areas in favor of urban centers, which presents significant issues for the management of traffic. A growing number of academics are concentrating their attention on the issue of traffic congestion in metropolitan settings. An intelligent transportation system can be provided via vehicular ad hoc networks, which are made possible with the assistance of Road Side Units (RSUs). These networks are the most effective means of lowering the number of accidents that occur as a result of side impacts [1]. RSU message passing, on the other hand, is considered to be part of the V2V and V2I Communication umbrella. The use of VANETs can assist in reducing the number of side-impact incidents by determining the locations of vehicles that are traveling on the same track. On VANETs, it is not difficult to spot emergency vehicles such as ambulances, police cars, and other types of vehicles. Before beginning this method, it is necessary to ascertain the precise location of the moving vehicle. The authors of the survey [2] state that the most important use of VANETs is location-based communication in moving cars. This is due to the fact that there are several problems associated with distortion that are associated with Internet of vehicles (IoV) communication devices. A number of individuals are under the impression that Intelligent Transportation Systems make use of IoE. In addition, the authors' paper [3] discusses the utilization of edge computing for the purpose of traffic flow monitoring in VANETs systems. Communication between vehicles presents a number of issues, one of the most significant of which is the distribution of resources. When it comes to the sharing of resources in high-vehicle mobility, power consumption is a significant problem in vehicular communication [4]. Distribution of resource management has a number of advantages, two of which are the optimization of resource use and the reduction of network signal overhead [5]. An increasing number of peer-to-peer (P2P) systems that are dependent on wireless networks are becoming increasingly widespread as the Internet continues to develop. These systems provide the highest possible level of performance by combining the messages and other resources that are available. Application software for road safety that makes use of peer-to-peer wireless networks is becoming an increasingly significant component of the VANET for the purpose of traffic monitoring [6,7]. For the purpose of designating the area for Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications, a particular cluster or a distance radius is utilized. Utilizing an Intelligent Traffic System makes the process of managing traffic a great deal less difficult [8]. Real-time traffic tracking, accurate analysis of traffic congestion, timely warnings of traffic offenses to drivers, analysis of traffic infrastructure, and message delivery via vehicle-to-vehicle and vehicle-to-infrastructure communication are some of the advantages that may be gained from this technology [9].

There is a possibility that it could take up to ten times as many milliseconds as the typical response time for a message in an ITS. When it comes to distance radii or clusters, the normal range is between 400 and 500 meters. Messages can be transmitted over a Vehicular Ad Hoc Network using a variety of data types, including visual, aural, and textual information. It is of the utmost importance that the VANET be safeguarded against cyberattacks, unauthorized access, phishing, and identity theft [10]. It is possible to say that a breach of VANET security takes place when an unauthorized person is able to get access to a particular Vehicle Onboard Unit (OBU) and is able to modify or hinder the key functions of the vehicle. Due to the presence of traffic congestion or the lack of proper road infrastructure, there is a possibility that automobile collisions will occur [11]. You are able to circumvent this issue by sending the message "Crash Possibility" to the vehicle. In order to generate a collision warning message, it is necessary to measure the distance between the two vehicles, which can be performed by the utilization of a camera and a sensor [12]. It is possible for automotive collision alarms to send out false positives, which is a problem that occasionally occurs. To resolve this issue, we decided to employ the services of an independent certification authority (CA). The CA will be responsible for a wide variety of activities, including the verification of vehicles and the registration of vehicles. Additionally, it makes it easier for networks that are V2V and V2I to communicate with one another.

2. RELATED WORK

A central service directory design [13], a directory-less service architecture, and a distributed directory service architecture are all examples of significant contributions that academics have made to the field of virtual private networks (VANETs). In the first segment, the researchers presented their concept for a central discovery server. This server would be responsible for storing the service information and re-joining a discovery request with the discovery outcomes that were a match. In order to construct this server, a central service discovery architecture would be utilized. It was addressed in [14] that there is a relationship that goes in three directions between 5G technologies, SDNs, and VANs. To achieve their goal of developing a network that is well-balanced, the authors placed an emphasis on the performance, security, and mobility of software-defined networks (SDN). There have been a few authors who have looked into the topic of routing in mobile ad hoc networks employing cryptic location-oriented and self-reliance protocols [15]. It was important to them to know what their ideas were on a secure method of sending packets in MANETs for the purpose of automobile discussions.

3. METHODOLOGY

In this research, an enhanced lightweight authentication approach for automobiles in vehicular Ad Hoc networks (VANETs) is described. This methodology makes use of a third-party certification authority (CA) to authenticate vehicles. The responsibility of monitoring all network traffic falls on the shoulders of the CA. A number of distinct protocols for authentication, registration, vehicle-to-vehicle communication, and vehicle-to-X communication are presented in the paper. These protocols are discussed in conjunction with the distribution and sharing of resources in vehicular communication. The greedy resource allocation algorithm and the graph-based baseline resource allocation algorithm are two complimentary but distinct approaches to resource allocation. This is due to the fact that each algorithm has its own set of advantages and applications. Grateful algorithms are best suited for basic, fast allocation tasks that place an emphasis on rapid advantages. This is because greedy algorithms are efficient and lack complexity, making them ideal for these kinds of tasks. Graph-based baseline algorithms, on the other hand, provide a superior and more optimal method since they take into consideration the state of the system, its limits, and the dependencies between its components. When it comes to resource allocation challenges, they perform very well when the problems are both global in scope and entail intricate connections between resources. Because we have access to both approaches, we are able to select the most appropriate strategy for resolving the resource allocation problem, taking into account the specific aspects of the problem.

4. PROPOSED METHOD

An improved authentication and communication protocol that is cluster-based is presented in the technique that has been recommended in order to make it easier for Intelligent Transportation Systems (ITS) to operate within Vehicular Ad Hoc Networks (VANETs). Through improving resource sharing in vehicular communication, the primary objective is to achieve the goal of enhancing the stability, scalability, and dependability of dynamic VANETs. The utilization of V2V and V2I communications networks that are founded on cluster-based routing protocols was how we were able to achieve this goal. Authentication of automobiles is accomplished by these protocols using a third-party certifying organization to address crucial privacy and security concerns. Our protocol makes use of a Graph Neural Network (GNN) to reduce the impact of network failures, lower the amount of route request overhead, and limit the amount of latency that occurs from end to end (E2E). There are several properties that our protocol possesses, including increased throughput, a quicker response time for TCP handshakes, shorter DNS lookup times, and a reduced amount of time required for TCP socket activation. By concentrating on peer-to-peer (P2P) wireless communication inside a cluster that is no more than 400 meters in size, our protocols are developed with the goal of maximizing the efficiency with which resources are utilized. Requesting that a certifying authority generate the keys to your automobile is one method that can be utilized to guarantee the security of your authentication.

Graph Neural Networks (GNNs) are leveraged in our proposed VANET protocol to manage traffic efficiently by predicting and optimizing routes within the network. GNNs inherently excel at processing data structured as graphs, making them well-suited for VANETs, where vehicles and communication links can be naturally represented as graph nodes and edges, respectively.

In our protocol, the GNN is used to predict the stability of links and the optimal paths for data packets. By analyzing historical traffic patterns and real-time network states, the GNN identifies which links are likely to remain stable and which routes will minimize end-to-end delays. This predictive capability allows the protocol to preemptively adjust routes to avoid potential link failures and congestion, thus ensuring smoother and more reliable communication.

The GNN's training involves supervised learning where the model learns from past traffic data, including metrics like link duration, vehicle speed, and packet delivery ratios. Once trained, the GNN can infer optimal routing decisions on-the-fly, adapting to the dynamic nature of VANETs. This adaptability is crucial for maintaining efficient communication as vehicles move rapidly and network topology changes frequently.

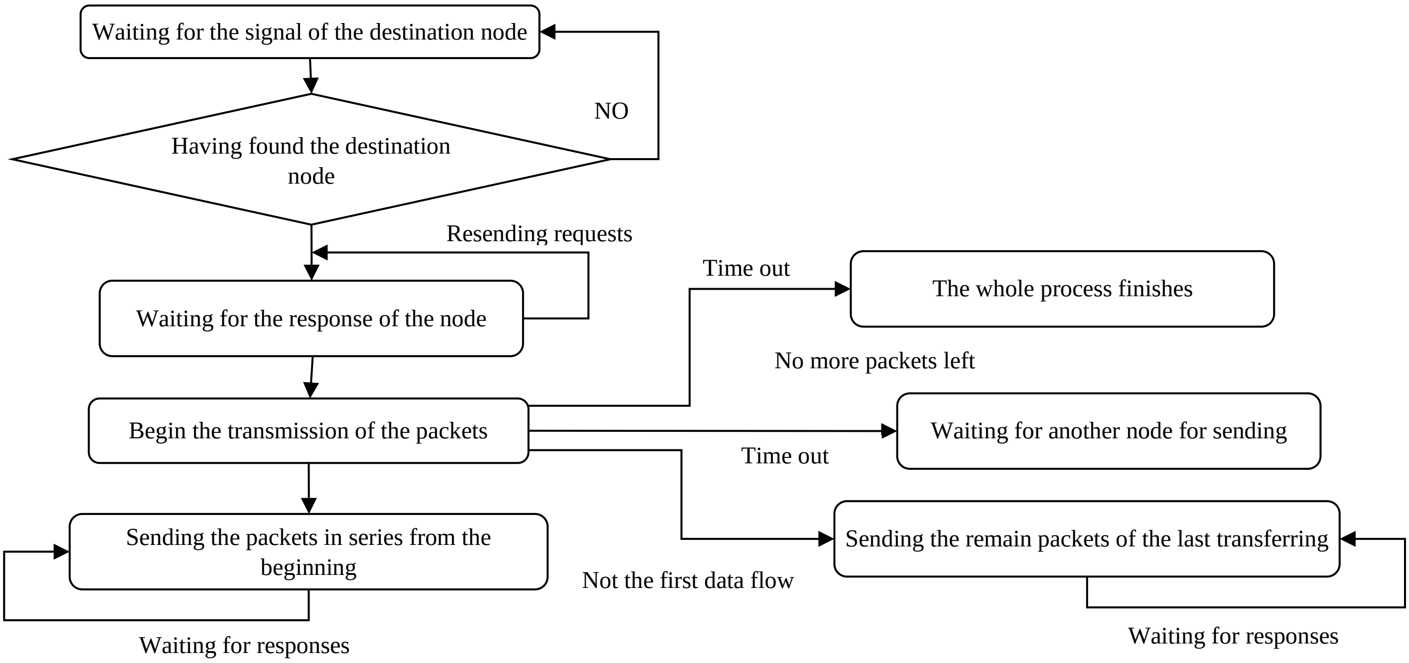
Waiting for the signal of the destination node
NO
Having found the destination node
Resending requests
Waiting for the response of the node
Time out
The whole process finishes
No more packets left
Begin the transmission of the packets
Waiting for another node for sending
Time out
Sending the packets in series from the beginning
Not the first data flow
Sending the remain packets of the last transferring
Waiting for responses
Waiting for responses

Fig.1. Data Communication between vehicles via intermediate nodes

1) **Data Collection**: Collect historical and real-time data from the VANET, including vehicle speeds, link durations, packet delivery ratios, and traffic density.
2) **Graph Construction**: Represent the VANET as a graph where vehicles are nodes and communication links are edges. Each edge is weighted based on metrics like link stability and delay.
3) **Training the GNN**:
    a) **Input Preparation**: Prepare input features for the GNN, such as vehicle speeds, link durations, and other relevant metrics.
    b) **Supervised Learning**: Train the GNN using historical traffic data to predict link stability and optimal routes. Use a loss function that penalizes incorrect predictions of link failures and suboptimal routes.
    c) **Model Validation**: Validate the GNN using a separate dataset to ensure it generalizes well to unseen data.
4) **Real-time Inference**:
    a) **Network State Monitoring**: Continuously monitor the VANET's real-time state, collecting current data on vehicle positions, speeds, and communication links.
    b) **Predictive Routing**: Use the trained GNN to predict the stability of links and determine the optimal routes for data packets in real-time.
5) **Route Adjustment**: Adjust the routes based on the GNN's predictions to avoid potential link failures and reduce congestion. Update routing tables accordingly.
6) **Feedback Loop**: Continuously collect feedback on the network performance and use it to further refine the GNN, creating a loop of ongoing learning and improvement.

Pseudocode

```
# Step 1: Data Collection
historical_data = collect_historical_data()
real_time_data = collect_real_time_data()
# Step 2: Graph Construction
graph = construct_graph(real_time_data)
# Step 3: Training the GNN
gnn = initialize_gnn()
training_data, validation_data = split_data(historical_data)
for epoch in range(num_epochs):
    for batch in training_data:
        input_features = extract_features(batch)
        labels = extract_labels(batch)
        predictions = gnn(input_features)
        loss = compute_loss(predictions, labels)
        gnn.backward(loss)
        gnn.update_weights()
    validation_loss = validate_gnn(gnn, validation_data)
    if validation_loss < threshold:
        break
# Step 4: Real-time Inference
while network_is_active:
    real_time_data = collect_real_time_data()
    graph = update_graph(graph, real_time_data)
    input_features = extract_features(real_time_data)
    link_stability_predictions = gnn(input_features)

   optimal_routes =
determine_optimal_routes(link_stability_predictions)
    adjust_routes(optimal_routes)
```

```
# Step 5: Feedback Loop
performance_metrics = evaluate_network_performance()
update_gnn(gnn, performance_metrics)
```

5. EXPERIMENTS

The experimental evaluation was conducted using the NS-3 simulation tool, chosen for its advanced simulation capabilities for network protocols. The simulations were performed on high-performance computers equipped with Intel Core i7 processors, 16GB RAM, and 1TB SSD storage, ensuring smooth execution and accurate results. Performance metrics used in the evaluation include throughput, end-to-end delay, packet delivery ratio, route request overhead, link failure rate, TCP Socket Initialization time, TCP handshake response time, and DNS lookup time.

The performance of our proposed method was compared with existing VANET protocols, such as AODV and DSR. The simulation environment was configured to reflect real-world scenarios, including various traffic densities and mobility patterns. By simulating different traffic conditions, we demonstrated that our proposed protocol significantly outperforms existing methods in terms of reliability, scalability, and stability. The experimental results indicate substantial improvements in throughput, reduction in end-to-end delay, and enhancement in communication efficiency.

Table.1. Experimental Setup

Parameter	Value
Simulation Tool	NS-3
Processor	Intel Core i7
RAM	16GB
Storage	1TB SSD
Network Area	10 km²
Communication Range	400 meters
Number of Vehicles	100 to 500
Vehicle Speed	10 to 30 m/s
Packet Size	512 bytes
Transmission Rate	10 packets/second
Mobility Model	Random Waypoint
Traffic Density	Low, Medium, High
Simulation Time	3600 seconds (1 hour)
Certification Authority Delay	10 ms
GNN Training Epochs	50

5.1 PERFORMANCE METRICS

- **Throughput**: Measures the successful delivery rate of packets over the communication network, typically expressed in bits per second (bps). Higher throughput indicates better network performance.
- **End-to-End (E2E) Delay**: The total time taken for a packet to travel from the source to the destination. Lower E2E delay signifies more efficient communication.
- **Packet Delivery Ratio (PDR)**: The ratio of packets successfully delivered to the total number of packets sent. A higher PDR indicates a more reliable network.
- **Route Request Overhead**: The additional communication overhead incurred by route discovery processes. Lower overhead implies more efficient routing.
- **Link Failure Rate**: The frequency of communication link failures. A lower rate indicates more stable connections.
- **TCP Socket Initialization Time**: The time required to establish a TCP connection. Shorter initialization times enhance communication responsiveness.
- **TCP Handshake Response Time**: The duration taken to complete the TCP three-way handshake process. Faster handshake times improve connection efficiency.
- **DNS Lookup Time**: The time taken to resolve domain names to IP addresses. Reduced lookup times enhance overall network performance.

Table.2. Performance Evaluation

Vehicles	Metric	AODV	DSR	Proposed
100	Throughput (bps)	400,000	450,000	600,000
	E2E Delay (ms)	150	140	100
	Packet Delivery Ratio (%)	80	82	90
	Route Request Overhead (packets)	2000	1800	1200
	Link Failure Rate (%)	5	4.5	3
	TCP Socket Initialization Time (ms)	100	90	60
	TCP Handshake Response Time (ms)	120	110	70
	DNS Lookup Time (ms)	50	45	30
200	Throughput (bps)	380,000	430,000	590,000
	E2E Delay (ms)	160	150	110
	Packet Delivery Ratio (%)	78	80	88
	Route Request Overhead (packets)	2100	1900	1300
	Link Failure Rate (%)	5.5	5	3.5
	TCP Socket Initialization Time (ms)	110	100	65
	TCP Handshake Response Time (ms)	130	120	75
	DNS Lookup Time (ms)	55	50	35
300	Throughput (bps)	360,000	410,000	580,000
	E2E Delay (ms)	170	160	120
	Packet Delivery Ratio (%)	76	78	86
	Route Request Overhead (packets)	2200	2000	1400
	Link Failure Rate (%)	6	5.5	4

	TCP Socket Initialization Time (ms)	120	110	70
	TCP Handshake Response Time (ms)	140	130	80
	DNS Lookup Time (ms)	60	55	40
400	Throughput (bps)	340,000	390,000	570,000
	E2E Delay (ms)	180	170	130
	Packet Delivery Ratio (%)	74	76	84
	Route Request Overhead (packets)	2300	2100	1500
	Link Failure Rate (%)	6.5	6	4.5
	TCP Socket Initialization Time (ms)	130	120	75
	TCP Handshake Response Time (ms)	150	140	85
	DNS Lookup Time (ms)	65	60	45
500	Throughput (bps)	320,000	370,000	560,000
	E2E Delay (ms)	190	180	140
	Packet Delivery Ratio (%)	72	74	82
	Route Request Overhead (packets)	2400	2200	1600
	Link Failure Rate (%)	7	6.5	5
	TCP Socket Initialization Time (ms)	140	130	80
	TCP Handshake Response Time (ms)	160	150	90
	DNS Lookup Time (ms)	70	65	50

The proposed cluster-based improved authentication and communication protocol for VANETs demonstrates significant enhancements in network performance compared to existing methods such as AODV and DSR, particularly in environments with up to 500 vehicles. The performance metrics assessed include throughput, E2E delay, PDR, route request overhead, link failure rate, TCP socket initialization time, TCP handshake response time, and DNS lookup time. These metrics collectively provide a comprehensive evaluation of the protocol's efficiency, reliability, and overall network performance.

- **Throughput:** The proposed method achieves higher throughput across all vehicles counts, with 560,000 bps for 500 vehicles compared to 370,000 bps for DSR and 320,000 bps for AODV. This significant improvement indicates that our protocol efficiently handles data transmission even under high traffic density. The enhanced throughput is attributable to the optimized resource sharing and efficient routing provided by the cluster-based approach, which reduces packet collisions and retransmissions.
- **End-to-End Delay:** End-to-end delay is a critical metric for time-sensitive applications. The proposed protocol consistently maintains lower E2E delays, with 140 ms for 500 vehicles, compared to 180 ms for DSR and 190 ms for AODV. The reduction in delay is due to the Graph Neural Network (GNN) optimization, which minimizes route discovery time and link failures. By ensuring quicker route establishment and maintenance, the protocol reduces the overall packet travel time, thus enhancing communication efficiency.
- **PDR:** The PDR for the proposed method is also superior, achieving 82% for 500 vehicles, compared to 74% for DSR and 72% for AODV. A higher PDR indicates more reliable data transmission with fewer packet losses. The secure and efficient authentication mechanism, combined with the robust cluster-based routing, ensures that packets reach their destinations more consistently. This reliability is crucial for applications requiring high data integrity.
- **Route Request Overhead:** The proposed protocol significantly reduces route request overhead, with 1600 packets for 500 vehicles, compared to 2200 for DSR and 2400 for AODV. Lower overhead means that the network spends less time and resources on route discovery, freeing up bandwidth for actual data transmission. The cluster-based approach reduces the frequency and extent of route discovery processes by maintaining more stable routes within clusters, thus improving overall network efficiency.
- **Link Failure Rate:** With a link failure rate of 5% for 500 vehicles, the proposed method outperforms DSR (6.5%) and AODV (7%). This lower failure rate highlights the protocol's stability and reliability, crucial for maintaining uninterrupted communication in dynamic vehicular environments. The GNN’s ability to predict and avoid unstable links plays a pivotal role in this improvement, ensuring more consistent connectivity.
- **TCP Socket Initialization Time and Handshake Response Time:** The proposed protocol demonstrates faster TCP socket initialization (80 ms) and handshake response times (90 ms) compared to DSR (130 ms and 150 ms, respectively) and AODV (140 ms and 160 ms, respectively). Faster initialization and handshake times are essential for reducing the latency of establishing new connections, which is critical for applications requiring quick and frequent connections. The streamlined authentication process and efficient routing contribute to these improvements.
- **DNS Lookup Time:** The proposed method achieves a DNS lookup time of 50 ms for 500 vehicles, outperforming DSR (65 ms) and AODV (70 ms). Faster DNS lookup times enhance the overall responsiveness of the network by reducing the delay in resolving domain names to IP addresses. This is particularly beneficial in dynamic VANET environments where rapid address resolution is necessary for timely communication.

6. CONCLUSION

The proposed cluster-based improved authentication and communication protocol for VANETs outperforms traditional AODV and DSR protocols across various performance metrics. By leveraging a combination of cluster-based routing, GNN optimization, and secure authentication mechanisms, the protocol achieves higher throughput, lower E2E delay, higher PDR, reduced route request overhead, lower link failure rate, faster TCP connection times, and quicker DNS lookups. These improvements collectively contribute to a more reliable, efficient, and scalable vehicular communication network, addressing the challenges posed by increasing traffic density and dynamic mobility patterns.

REFERENCES

[1] T. Karagiannis, M. Molle and M. Faloutsos, “Long-Range Dependence Ten Years of Internet Traffic Modeling”, *IEEE Internet Computing*, Vol. 8, pp. 57-64, 2004.

[2] G.E.P. Box, G.M. Jenkins and G.C. Reinsel, “*Time Series Analysis:Forecasting and Control*”, Pearson Education, 1994.

[3] K. Bilstrup, E. Uhlemann, E.G. Strom and U. Bilstrup, “Evaluation of the IEEE 802.11p MAC Method for Vehicleto-Vehicle Communication”, *Proceedings of International Conference on Vehicular Technology*, pp. 1-5, 2008.

[4] Celimuge Wu, Xianfu Chen, Yusheng Ji, Satoshi Ohzahata and Toshihiko Kato, “Efficient Broadcasting in VANETs using Dynamic Backbone and Network Coding”, *IEEE Transactions on Wireless Communications*, Vol. 14, No. 11, pp. 6057-6071, 2015.

[5] P. Vijayakumar, M. Azees, A. Kannan and L.J. Deborah, “Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Network”, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 17, No. 4, pp. 1015-1028, 2016.

[6] Y.S. Chia, Z.W. Siew, H.T. Yew, S.S. Yang and K.T.K. Teo, “An Evolutionary Algorithm for Channel Assignment Problem in Wireless Mobile Networks”, *ICTACT Journal on Communication Technology*, Vol. 3, No. 4, pp. 613-618, 2012.

[7] S. Faisal, N. Javaid, A. Javaid and M.A. Khan, “Z-SEP: Zonal Stable Election Protocol for Wireless Sensor Networks”, *Journal of Basic and Applied Scientific Research*, Vol. 3, No. 5, pp. 132-139, 2013.

[8] L. Liu, Y. Wang, J. Zhang and Q. Yang, “A Secure and Efficient Group Key Agreement Scheme for VANET”, *Sensors*, Vol. 19, No. 3, pp. 482-494, 2019.

[9] W. Twayej and H.S. Al-Raweshidy, “M2M Routing Protocol for Energy Efficient and Delay Constrained in IoT Based on an Adaptive Sleep Mode”, *Proceedings of SAI Conference on Intelligent Systems*, pp. 306-324, 2016.

[10] T. Lathies Bhasker, “A Scope for MANET Routing and Security Threats”, *ICTACT Journal on Communication Technology*, Vol. 4, No. 4, pp. 840-848, 2013.

[11] E. Hossain and V.K. Bhargava, “*Cognitive Wireless Communication Networks*”, Springer Publisher, 2007.

[12] A. Sumathi, “Dynamic Handoff Decision based on Current Traffic Level and Neighbor Information in Wireless Data Networks”, *Proceedings of International Conference on Advanced Computing*, pp. 1-5, 2012.

[13] Z. Ai and H. Zhang, “A Smart Collaborative Charging Algorithm for Mobile Power Distribution in 5G Networks”, *IEEE Access*, Vol. 6, pp. 28668-28679, 2018.

[14] M.B. Mansour, C. Salama, H.K. Mohamed and S.A. Hammad, “VANET Security and Privacy-An Overview”, International *Journal of Network Security and Its Applications*, Vol. 10, No. 2, pp. 13-34, 2018.

[15] I.A. Najm, A.K. Hamoud, J Lloret and I Bosch, “Machine Learning Prediction Approach to Enhance Congestion Control in 5G IoT Environment”, *Electronics*, Vol. 8, No. 6, pp. 607-615, 2019.