International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 08 Issue 03 March 2025
DOI: 10.47191/ijcsrr/V8-i3-34, Impact Factor: 8.048
IJCSRR @ 2025
www.ijcsrr.org

Secure and Efficient Routing in Fog-Enabled VANETs: A Clustering-Based Approach

Anshu Devi[1], Ramesh Kait[2], Virender Ranga[3]
[1,2]Department of Computer Science & Applications, Kurukshetra University, Haryana
[3]Information Technology Department, Delhi Technological University, Delhi, Haryana

ABSTRACT: Vehicular Ad Hoc Networks (VANETs) play a crucial role in intelligent transportation systems (ITS) by enabling seamless vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. However, VANETs face significant challenges related to security, routing efficiency, and dynamic load balancing. This paper proposes a novel approach integrating clustering-based routing, fog computing, and authentication mechanisms to enhance network performance. The article proposes a new method for node authentication and redistribution of loads in vehicular ad-hoc networks (VANETs). The proposed method is designed to do better for VANETs in all aspects related to secure node authentication and the efficient load assignment among fog nodes. The approach uses a polynomial-based node authentication protocol and balances the network load dynamically by evaluating two parameters: Network Availability Bandwidth (NAB) and request count. Simulation-based performance evaluation was carried out for comparisons with existing algorithms. Metrics of comparison included throughput, packet delivery ratio (PDR), and latency. The proposed method clearly shows all improvements over existing algorithms. Throughput increased by 8591.86 packets per second; PDR improved to 0.833; latency was cut down to 6.4951 seconds, which makes it a potential candidate for performance enhancement in VANETs.

KEYWORDS: Clustering, Load Balancing, Intelligent Transportation Systems, Vehicular Ad Hoc Networks.

INTRODUCTION

The merging of vehicular ad hoc networks (VANETs) with fog computing has in recent years provided promising solutions for mitigating the hurdles of vehicular communications, especially about security and efficiency. VANETs are a special case of ad hoc mobile wireless network created to support communications between vehicles, roadside infrastructure, and other entities in the transportation ecosystem [1]. These networks are indeed characterized by dynamic topology structures, high mobility, and are real-time demanding making the conventional routing protocols insufficient for vehicular communication purposes [2-3]. In an attempt to solve these challenges, fog computing concept is facilitated into VANETs [4]. Fog computing allows the distribution of computational tasks, storage, and services close to the source of data, i.e., on the edge of the network. This reduces latency, enhances scalability, and enables faster data processing [5-6].

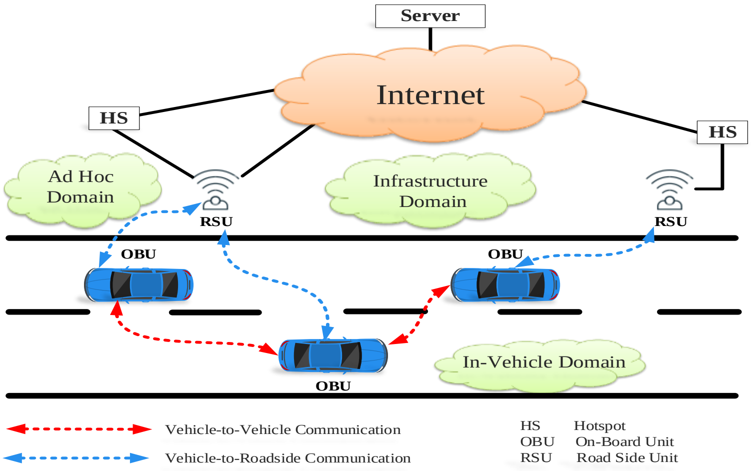


Figure 1. VANET Communication Architecture

The synergistic combination of VANETs and fog computing, namely Fog-Enabled VANETs, has immense potential for advancing intelligent transportation systems (ITS), autonomous driving, and real-time traffic management [7,8]. Illustration of the VANET architecture and vehicle communication with cloud is given in Figure 1 [9]. However, secure and efficient routing in Fog-enabled VANETs is a challenging problem [10,11]. The challenges involved include secure transmission of sensitive data between a car and infrastructure, resource allocation, and managing a highly dynamic network condition [12-13]. This has called for a new class of routing strategies which combine the guarantee of secure communication with increased efficiency of the network.

This paper proposes a clustering-based methodology for the routing of secure and efficient transmission of data in Fog-Enabled VANETs. Clustering operates on the principle of keeping vehicles and infrastructure nodes together in clusters, all managed by a cluster head. This clustering structure produces improved data management and bettering use of resources among the components. In addition, a security layer is integrated into the routing process to protect the confidentiality, integrity, and authenticity of data sent through the network.

RELATED WORK

Recent years have witnessed a notable enhancement in the VANETs and fog computing literature with various approaches evidenced to address security, performance, and efficiency. A review of major studies depicting very important results on such challenges related to routing and security in fog-enabled VANETs, especially stressing clustering-based approaches is given in this section. Wang et al. (2015) put forward 2FLIP, the two-factor lightweight privacy-preserving authentication mechanism for VANETs to present a secure and efficient authentication mechanisms. The significance of maintaining privacy while ensuring efficient communication in VANETs was emphasized, most particularly in high mobile environments. 2FLIP provides reduced overhead on normal authentication mechanisms, and thus it can boast of scalability and strong security in resource-constrained vehicular environments [14]. Zhang et al. (2019) provided reliable multiservice delivery in fog-enabled VANETs by the incorporation of mechanisms that handle misbehavior detection and tolerance. In order to detect malicious vehicles that attempted to disrupt the network, this approach used a combination of trust- and reputation-based modularities. By incorporating misbehavior detection with fog-enabled services, this study guaranteed that the network could continue to communicate and deliver data reliably, tagged with the warnings of malicious nodes [15].

In terms of the preservation of privacy, Han et al. (2020) established an anonymous authentication scheme on fog computing for VANETs. This technique allowed for the identity of vehicles to remain confidential but secure at the same time for communication. Not only could the scheme prevent the unauthorized tracking of vehicles, but it also addressed the issues of privacy protection while maintaining a secure and efficient communication framework. This was supplementary work on the broader front to ensure the simultaneous maintenance of privacy and security in VANETs [16]. The empowerment of fog computing in VANETs also exploits this approach to resolve issues of energy and load balancing. Hameed et al. (2021) provided sufficient focus on energy-and performance-aware load balancing in vehicular fog computing, suggesting algorithms to balance the computational load among fog nodes. The method was aimed at minimizing power consumption while improving performance, thus allowing the efficient usage of resources in such a way as to not diminish system performance [17].

In a similar manner, energy-aware load balancing management techniques for fog-based VANETs were researched and proposed by Qun and Arefzadeh (2021). Their hybrid algorithm encompassed some energy-aware strategies to enhance the load distribution and energy consumption in large-scale vehicular networks [18]. Several studies have pointed out various clustering schemes for enhancing performance in VANET. Khudhair et al. (2023) proposed a clustering approach to a VANET that is intended to create clusters within the networks for a better performance. The authors have focuessed on several aspects however stability of network and scalability was enhanced, minimizing the communication overhead [19]. Devi et al. (2022) has employed the machine learning concept for automatic cluster head selection in fog-enabled VANETs. The proposed approach used machine-learning algorithms to dynamically select cluster heads depending on the network situation, vehicle mobility, and energy efficiency. This included better load balancing, leading to improved overall network performance in fog-assisted VANETs, since it operated towards addressing the problem of ensuring reliable and efficient network infrastructure [20].

Ahmed et al. (2024), having contributed AODV-RL with the BHA Attack Defense by enhancing the AODV routing protocol, called for a secure and dependable routing approach of the IoV-Internet of Vehicles-network. Their writing combined the routing protocol with the defense against Black Hole and Gray Hole attacks. The guaranteed improvement of routing efficiency and security was thus assured in the IoV network, which becomes critical considering that in VANETs and fog computing, attacks on the routing paths can jeopardize the system performance severely [21]. In summary, these studies provide a whole view of several forms of systemic processes regarding security and efficiency problems within VANETs when combined with fog computing. They have given rise to extremely pertinent aspects for augmenting the security and efficiency of VANETs such as privacy-preserving authentication, energy efficiency, misbehavior detection, and clustering mechanisms. Clustering methods have gained more importance in enabling improved load balancing, scalability, and overall robustness for VANETs in holistic integrated environments. Using machine learning and hybrid optimization techniques further addressed some of the dynamic and resource-constrained settings of vehicular networks, and it is one of the focus areas for future exploration in this domain.

PROPOSED METHODOLOGY

The proposed methodology focusses on the improvement of the routing performance and security in fog-enabled VANETs based on three methods: clustering-based routing, curve fitting-based authentication, and dynamic load balancing.

A. *Clustering based Routing*

To minimize routing overhead and enhance network stability, vehicles are grouped into clusters based on their proximity. A Cluster Head (CH) is selected for each cluster to communicating data to the neighboring CHs or fog nodes. The clustering process minimizes communication cost by selecting the CH closest to other vehicles in the cluster and can be formulated mathematically. The clustering process formulated and presented as follows:

$$\boldsymbol{CH = arg\, min_{\{i \in V\}} \Sigma_{j \in C}\, d(i,j)} \quad (1)$$

Where, CH is the selected Cluster Head, V represents the set of vehicles, C is the cluster, and $d(i,j)$ is the Euclidean distance between nodes.

B. *Curve Fitting-Based Authentication*

The proposed methodology focusses on the improvement of the routing performance and security in fog-enabled VANETs based on three methods: clustering-based routing, curve fitting-based authentication, and dynamic load balancing. Authentication is performed using the following equation:

$$\boldsymbol{y = a_n x^n + a_{\{n-1\}} x^{\{n-1\}} + \dots + a_1 x + a_0} \quad (2)$$

Where y represents the expected node behavior, and a_n are coefficients determined through least squares regression.

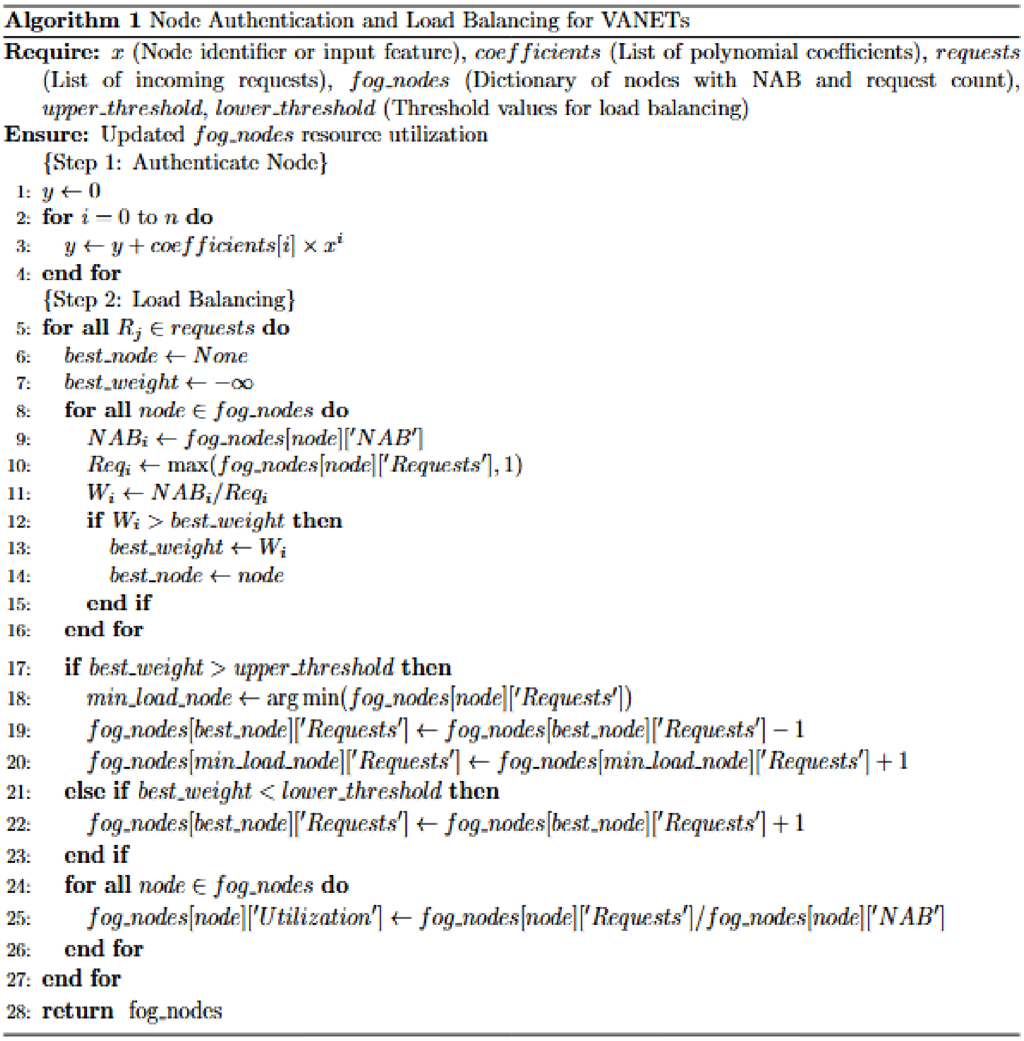
C. *Dynamic Load Balancing*

A dual-threshold policy is used for distributing computational tasks to fog nodes. It minimizes the load there by calculating the Neutralized Available Bandwidth (NAB) of all fog nodes, which redistributes load to maintain maximum proper utilization of resources.

$$\boldsymbol{W_i = \frac{NAB_i}{Req_i}} \quad (3)$$

Where, W_i is the weight assigned to node$i$, NAB_i is the neutralized available bandwidth, and Req_i represents the number of requests at the fog node. The algorithmic steps following in the proposed methodology are summarized in Algorithm 1.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 08 Issue 03 March 2025
DOI: 10.47191/ijcsrr/V8-i3-34, Impact Factor: 8.048
IJCSRR @ 2025
www.ijcsrr.org



```
Algorithm 1 Node Authentication and Load Balancing for VANETs
Require: $x$ (Node identifier or input feature), $coefficients$ (List of polynomial coefficients), $requests$
    (List of incoming requests), $fog\_nodes$ (Dictionary of nodes with NAB and request count),
    $upper\_threshold$, $lower\_threshold$ (Threshold values for load balancing)
Ensure: Updated $fog\_nodes$ resource utilization
    {Step 1: Authenticate Node}
$y \leftarrow 0$
for $i = 0$ to $n$ do
    $y \leftarrow y + coefficients[i] \times x^i$
end for
    {Step 2: Load Balancing}
for all $R_j \in requests$ do
    $best\_node \leftarrow None$
    $best\_weight \leftarrow -\infty$
    for all $node \in fog\_nodes$ do
        $NAB_i \leftarrow fog\_nodes[node]['NAB']$
        $Req_i \leftarrow \max(fog\_nodes[node]['Requests'], 1)$
        $W_i \leftarrow NAB_i / Req_i$
        if $W_i > best\_weight$ then
            $best\_weight \leftarrow W_i$
            $best\_node \leftarrow node$
        end if
    end for
    if $best\_weight > upper\_threshold$ then
        $min\_load\_node \leftarrow \arg\min(fog\_nodes[node]['Requests'])$
        $fog\_nodes[best\_node]['Requests'] \leftarrow fog\_nodes[best\_node]['Requests'] - 1$
        $fog\_nodes[min\_load\_node]['Requests'] \leftarrow fog\_nodes[min\_load\_node]['Requests'] + 1$
    else if $best\_weight < lower\_threshold$ then
        $fog\_nodes[best\_node]['Requests'] \leftarrow fog\_nodes[best\_node]['Requests'] + 1$
    end if
    for all $node \in fog\_nodes$ do
        $fog\_nodes[node]['Utilization'] \leftarrow fog\_nodes[node]['Requests'] / fog\_nodes[node]['NAB']$
    end for
end for
return fog_nodes
```

The algorithm is designed for node authentication and load balancing in VANETs with two components including node authentication and load balancing. In the first step, this algorithm computes polynomial-based authentication for each node given a set of input coefficients and the node identifier to generate a value that guarantees the legitimacy of the node in question. Load balancing is addressed in the next phase by the assessment of each incoming request by which an optimal node is made available to respond to the request. This is done by ordering the nodes based on the NAB and the request count, with advantage given to the node with the least workload imbalance. Should a node receive requests higher than a preconfigured upper threshold, the system will direct the incoming request to a less-loaded node. Conversely, if a node is less loaded (below a lower threshold), the entry load is increased. In the end, resource utilization for every node is recalculated such that resources are fairly distributed. The updated state of the fog nodes with respect to proper load balancing and node availability in their capacity to reply to future requests is then returned by the algorithm.

RESULTS AND ANALYSIS

The effectiveness of the proposed work is evaluated using three performance metrics namely, throughput, packet delivery ratio (PDR), and latency. The comparative analysis involves 300 vehicle nodes and two existing studies namely, Khudhair et al. and Ahmad et al. This serves the purpose of determining how well the proposed algorithm fosters the reliability of the networks, optimizing data transmissions and lowering delays in packet delivery. By virtue of the dynamicity of VANETs, each contributed enhancement towards such metrics impacts the overall efficiency of the network by upholding better communication in real-time traffic contexts. The results provide insights into the scalability and resilience of the proposed methods against other contemporary methods. The three key metrics used for evaluation are as follows:

- Throughput reflects the number of packets that are forwarded successfully per unit time showing the network ability to endure data traffic.
- Packet Delivery Ratio (PDR) is the metric that is used to monitor the ratio of the packets that successfully reached its the destination against the total number of packets that were sent. This reflects the efficiency of the network.
- Latency is another measure that represents the time that the packet takes to reach its destination from the source. This metric is particularly important for real-time applications in VANETs.

The parametric values to reflect the performance of the proposed method, Khudhair et al. [19] and Ahmad et al. [21] is summarized in Table I.

Table I Comparative Analysis

Methods	Throughput (p/s)	PDR	Latency (s)
Proposed	8591.86	0.833	6.4951
Khudhair et al. [19]	7868.00	0.766	7.4943
Ahmad et al. [21]	8218.60	0.778	7.6064

The performance analysis shows that the throughput attained by the proposed cluster-based cooperative approach was 8591.86 p/s, which is superior to 7868.00 p/s Khudhair et al. [19] and 8218.60 p/s by and Ahmad et al. [21]. The elevated throughput reflects the capacity of the topology to group together data transmissions in a way that minimizes overhead by allowing localized traffic within groups, hence reducing contention and repeated transmissions. The complement of this mechanism is fog computing, which processes packets at the edge, reducing burden on the core network and making the transmission more efficient. The increased throughput signifies timely delivering of traffic conditions, warnings, and critical information within an intelligent vehicular network-based traffic transportation system.

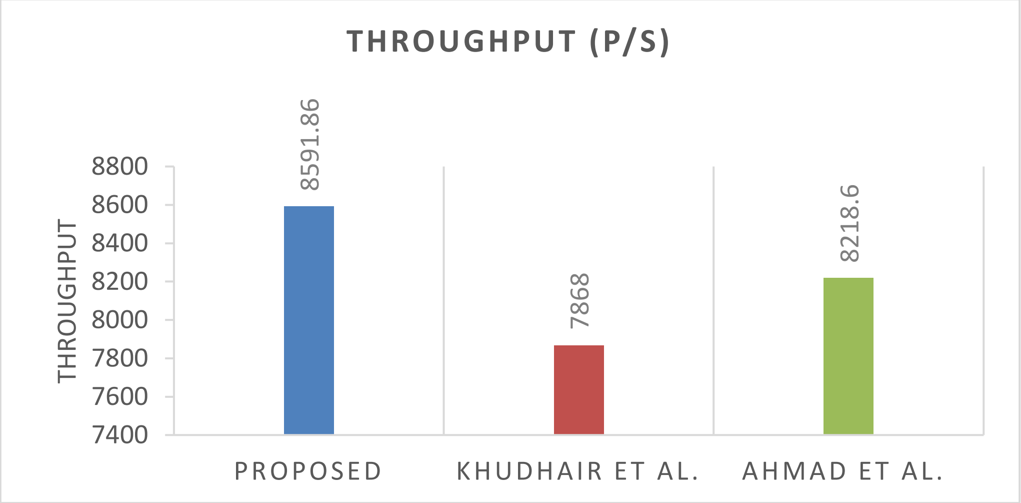


Figure 1 Throughput Comparative Analysis

The packet delivery ratio (PDR) is used to measure the reliability of data transmission in finding a secure and obstruction-free communication within VANET. The PDR attained by the cluster-based cooperative approaches is 0.833 much better than the aforementioned values of 0.766 and 0.778 reported by , Khudhair et al. [19] and Ahmad et al. [21], respectively. PDR increases primarily because of the cluster-based routing algorithm, which reduces the disruptive effects of rapid topology changes on route stability. Also, Fog processing reduces the data packet drop due to efficient in-field transmission and delivery even in dynamic vehicular environments. Higher PDR is thus vital for applications like crash warnings, traffic congestion alerts, and cooperative driving assistance where packet dropping can result in serious implications.

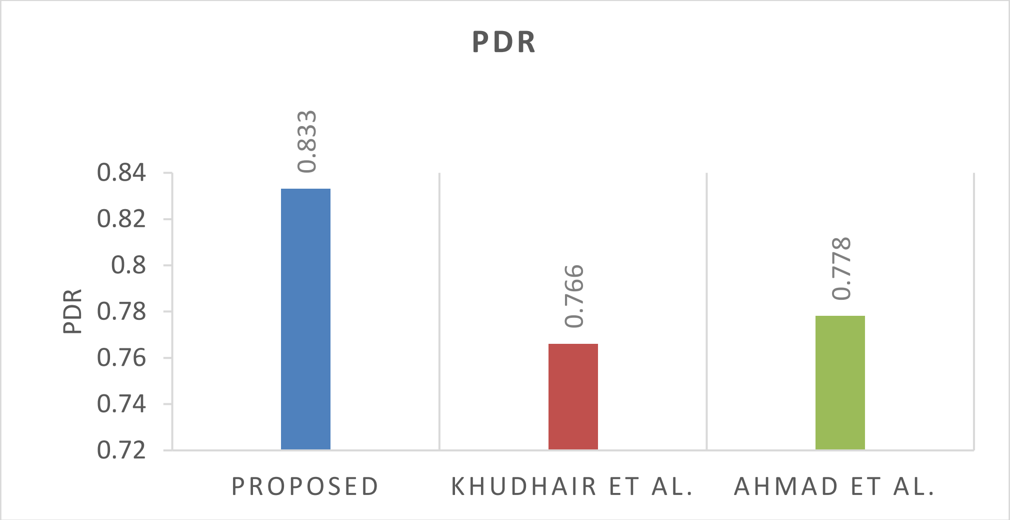


Figure 2 PDR Comparative Analysis

Latency is a key point in VANETs, important for real-time applications wherein timely information exchange is fundamental. The proposed method obtained a latency of 6.4951 seconds, which is very low compared to the measurement of 7.4943 seconds taken , Khudhair et al. [19] and 7.6064 seconds taken for Ahmad et al. [21]. The cause for this lower latency is the use of an efficient hierarchical clustering structure that works to minimize data transmission delays by providing an optimized route for message delivery and minimizing the chances of any broadcast storms. Additionally, fog-enabled computing prevents overwhelming the cloud server during the decision-making process, which further cuts down on decision turn-around time. Thus, the obtained low latency translates to an efficient and timely information delivery mechanism of functionless VANET applications wherein every second is a big deal, such as in accident prevention and emergent vehicle routing.

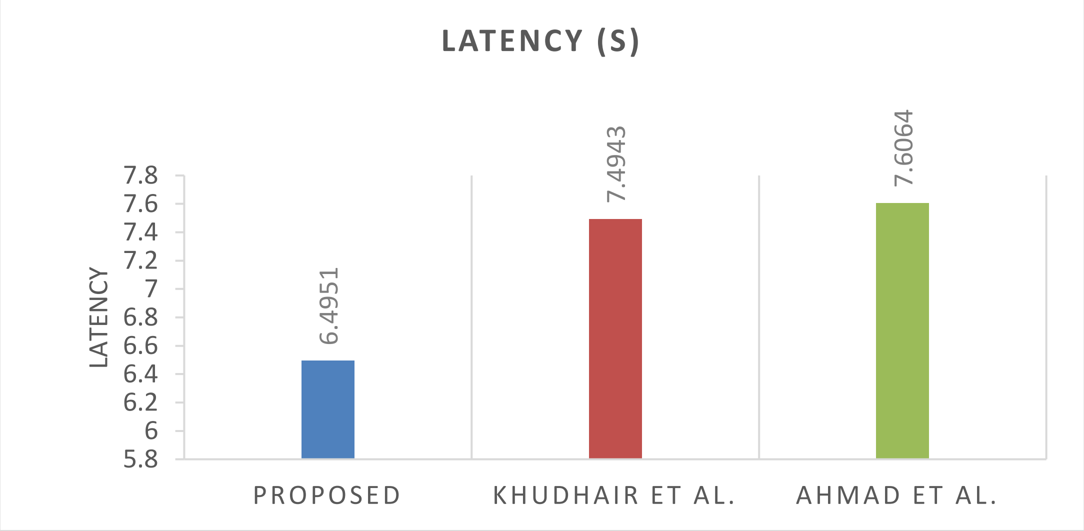


Figure 3 PDR Comparative Analysis

The performance evaluation proved that the clustering-based routing strategy adds a substantial level of safety and efficiency in fog-enabled VANETs. This provides higher throughput; this ensures efficient data handling capacity, the improved PDR guarantees dependable message dissemination, and lower latency favors real-time responsiveness. In addition, this clustering approach provides additional security in that it limits unnecessary data transmission, thus reducing the probability of malicious attacks such as packet drops and data tampering through the non-existence of paths for packet travel. The method combines fog computing to further diminish security threats by providing data authentication and intrusion detection at local fog nodes, thereby reinforcing the network against malicious parties.

Overall, the proposed method provides a good compromise between security and efficiency properties of the system, proving to be a mixture of a scalable and resilient routing protocol for next-generation VANETs. The findings justify the organization onto a clustering-based approach that would increase communication reliabilities capable of improving real-time decision making and safe transmission of data over fog-enabled vehicular networks.

CONCLUSION

The proposed work focusses on authentication and load distribution in VANETs and handles the authentication of nodes with dynamic load balancing supported using NAB and request count. All these permutations ensure the network functions optimally in a secure manner. The simulations proved that it surpasses existing algorithms in terms of throughput, packet delivery ratio (PDR), and latency. If these results are viewed with regards to enhancement, the proposed solution manifests a superior throughput of 8591.86 packets per second PDR of 0.833 and a cut-down latency of 6.4951 seconds. Since any other advancements in this area make this proposition promising correlated to the working field of VANET for real-time applications, it shows an endeavor to enhance the performance of VANETs. Those very results also testifying proving the proposed approach effective in enhancing the job of the networks brings an additional value proposition in the area of VANET optimization. Further areas of work can deal with issues about scalability and integration with other network protocols to enhance more in larger and complex environments.

REFERENCES

1. Karabulut, M. A., Shahen Shah, A. F. M., Ilhan, H., Pathan, A. K., and Atiquzzaman, M., *Ad Hoc Networks*, **150**, 2023, p. 103281.
2. Swetha, K., and Rama Devi, B., *IJITR International Journal of Innovative Technology and Research*, **4**(5), 2016, pp. 4219–4223.
3. Devi, A., Kait, R., and Ranga, V., *Cyber Security and Intelligent Analytics*, 2022, pp. 141–150.
4. Jalali K.A., Z., Mansouri, N., and Khalouie, M., *Computer Science Review*, **48**, 2023, p. 100550.
5. Devi, A., Kait, R., and Ranga, V., *International Journal of Performability Engineering*, **20**(9), 2024, pp. 572–580.
6. Devi, A., Kait, R., and Ranga, V., *Cloud Computing, and Wireless Network Optimization*, 2019, pp. 148–164.
7. Chand, N., Mishra, S., and Kumar, V., *Communications and Network*, **5**(1), 2013, pp. 12–15.
8. Eze, E. C., Zhang, S. J., Liu, E. J., and Eze, J. C., *International Journal of Automation and Computing*, **13**(1), 2016, pp. 1–18.
9. Elias, S. J., Hatim, S. M., Darus, M. Y., Abdullah, S., Jasmis, J., Ahmad, R. B., and Khang, A. W. Y., *Indonesian Journal of Electrical Engineering and Computer Science*, **13**(3), 2019, pp. 1280–1285.
10. Mishra, R., Singh, A., and Kumar, R., *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016, pp. 1050–1055.
11. Taheri-abed, S., Eftekhari Moghadam, A. M., and Rezvani, M. H., *Cluster Computing 2023*, **26**(5), 2023, pp. 3113–3144.
12. Sheikh, M. S., and Liang, J., *Wireless Communications and Mobile Computing*, 2019.
13. Devi, A., Kait, R., and Ranga, V., *International Joint Conference on Advances in Computational Intelligence*, 2022, pp. 705–715.
14. Wang, F., Xu, Y., Zhang, H., Zhang, Y., and Zhu, L., *IEEE Transactions on Vehicular Technology*, **65**(2), 2015, pp. 896–911.
15. Zhang, X., Lyu, C., Shi, Z., Li, D., Xiong, N. N., and Chi, C. H., *IEEE Access*, **7**, 2019, pp. 95762–95778.
16. Han, M., Liu, S., Ma, S., and Wan, A., *PLoS One*, **15**(2), 2020, p. e0228319.
17. Hameed, A. R., ul Islam, S., Ahmad, I., and Munir, K., *Sustainable Computing: Informatics and Systems*, **30**, 2021, p. 100454.
18. Qun, R., and Arefzadeh, S. M., *IET Communications*, **15**(13), 2021, pp. 1665–1676.

19. Khudhair, H. A., Albu-Salih, A. T., Alsudani, M. Q., and Fakhruldeen, H. F., *Bulletin of Electrical Engineering and Informatics*, **12**(5), 2023, pp. 2978–2985.
20. Devi, A., Kait, R., and Ranga, V., *Communication and Intelligent Systems: Proceedings of ICCIS 2021*, Springer Nature Singapore, 2022, pp. 1169–1179.
21. Ahmad, N., Mohammadani, K., Bashir, A. K., Omar, M., Jones, A., and Hassan, F., *CMES-Computer Modeling in Engineering & Sciences*, **139**(1), 2024, pp. 1–20.

Cite this Article: Devi, A., Kait, R., Ranga, V. (2025). Secure and Efficient Routing in Fog-Enabled VANETs: A Clustering-Based Approach. International Journal of Current Science Research and Review, 8(3), pp. 1304-1311. DOI: https://doi.org/10.47191/ijcsrr/V8-i3-34