scientific reports

Check for updates

OPEN

Efficient traffic management with adaptive SDN in vehicular networks

Sherine Jenny Rajan[1], Sugirtham Narayanaswamy[1], Thiyaneswaran Balashanmugam[2], Kumarganesh Sengottaiyan[3], Anthoniraj Selvaraj[4], Pratham Majumder[5], Amal Al-Rasheed[6], Masresha Getahun[7]✉ & Ben Othman Soufiene[8]

Improving road safety and easing congestion require effective real-time traffic data analysis and management. A crucial part of intelligent transportation systems, vehicular ad hoc networks (VANETs) deal with issues like inconsistent data from erratic vehicle movements and frequent topology changes. In order to develop a responsive and adaptable network management architecture for VANETs, this study makes use of Software-Defined Networking (SDN). SDN optimizes traffic flow, boosts routing efficiency, and improves Quality of Service (QoS) by separating the control and data planes. Traffic analysis and network performance are greatly improved when SDN is combined with priority algorithms and the Zigbee protocol. The effectiveness of this strategy in a controlled setting is shown by simulations conducted with COOJA software. Web digitization tools are also used to guarantee the accuracy of the data. Improved QoS, better traffic flow management, and scalable solutions for dynamic vehicular networks are some of the main results.

Keywords VANET, Quality of service, Priority algorithm, Network performance, Traffic analysis

Vehicular ad hoc networks (VANETs), a crucial part of intelligent transportation systems, enable multi-hop communication to efficiently route data between vehicles and infrastructure. Energy-efficient routing protocols are crucial for establishing connections between cluster sensor nodes and data sinks, and they have a direct impact on traffic load balancing, end-to-end reliability, and latency. A significant challenge in VANETs is determining the optimal routes to extend the network's operational lifetime, which is exacerbated by limited resources and frequent topology changes.

Key challenges in VANETs include:

- Network Organization: Maintaining connectivity amidst dynamic vehicle movements.
- Topology Discovery: Rapid identification of network changes.
- Routing Control and Signal Processing: Efficiently managing communication paths.
- Energy Efficiency: Designing low-power sensor nodes, network stacks, and applications.
- Routing protocols in VANETs adopt different strategies:
- Proactive Routing: Pre-computes and maintains routes, ensuring resilience against traffic load changes. Best suited for static sensor applications, it incurs overhead during topology updates.
- Reactive Routing: Discovers routes on-demand, reducing overhead but requiring significant energy for route discovery.
- Hybrid Routing[1]: Combines proactive and reactive methods to enhance scalability and efficiency.

By centralizing network intelligence and facilitating dynamic routing, traffic engineering, and improved security, SDN integration transforms VANETs. Vehicle communication networks can be optimized in real time thanks to SDN's ability to separate the control and data planes, which makes network administration easier. In order to assess performance, this study uses COOJA simulation software to investigate the application of SDN to VANETs. QoS and traffic analysis are improved by the SDN framework's use of Zigbee protocols and priority

[1]Department of ECE, Dr.Mahalingam College of Engineering and Technology, Coimbatore, Tamil Nadu, India. [2]Department of ECE, Sona College of Technology, Salem, Tamil Nadu, India. [3]Department of ECE, Knowledge Institute of Technology, Salem, Tamil Nadu, India. [4]School of Computer Science and Engineering, Jain (Deemed-to-Be) University, Ramanagara, India. [5]Department of Information Science & Engineering, Jain (Deemed-to-Be) University, Kanakapura, India. [6]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh, Saudi Arabia. [7]Department of Computer Science and Information Technology, College of Engineering and Technology, Kebri Dehar University, Kebri Dehar, Ethiopia. [8]PRINCE Laboratory Research, ISITcom, University of Sousse, Hammam Sousse, Tunisia. ✉email: masreshaggetahun@gmail.com

algorithms. Using web digitization tools also guarantees accurate and trustworthy data processing. These contributions demonstrate the potential of SDN as an enabler for sophisticated vehicular communication systems and fill important research gaps in the management of dynamic vehicular networks. SDN can bring significant benefits to VANETs by providing centralized control, dynamic routing, traffic engineering, improved security, and customized application support. Integrating SDN with VANETs has the potential to improve the efficiency, reliability and management of vehicular communication networks. One of the fundamental factors making 5G technology possible is the creation of Vehicular Ad Hoc Networks (VANETs) based on Software Defined Networking[2].

The paper is organized as follows: "Related work" summarizes relevant research. The experimental setup and suggested methodology are described in detail in "Proposed method and Experimental setup". The findings and analysis are shown in "Results and analysis". A summary and recommendations for further research are included at the end of the paper.

Our contributions

1. In this study, we propose a unique framework for integrating VANETs and the concepts of software-defined networks.
2. An idea was developed to combine 6LoWPAN and ZigBee protocol in software-defined networks to meet the needs of effective network performance and security.
3. Close monitoring and analysis of the network is carried out to confirm that SDN technology is managing networks and traffic efficiently.

Related work

Though VANET provide an intelligent transport technology[3], The biggest concern in the adoption of VANETs is still security of vehicular networks[4,5]. The development of intelligent transport system, security and its usage in IoT application is discussed in[6]. Software-Defined Networking (SDN) and Vehicular Ad-hoc Networks (VANETs) are two distinct networking technologies that can be integrated to enhance the efficiency and management of VANETs. The suitability of SDN for VANET is discussed by[7].The challenges in deploying SDN in VANET is massively discussed in[8,9].Extensive survey is carried out by the authors of[10] regarding the architecture of VANET,SDN, security issues of VANET and the functional improvement of SDN based VANET when compared to the conventional VANET. SDNs Resistant to various attacks is widely discussed by[9,11,12]. Modern generic network designs for smart cities rely on Fog Computing and the SDN paradigm to decrease latency and boost the effectiveness of services offered[9]. However, in recent days, many studies on SDN based on machine learning for dynamic traffic control have been published[13]. Fine-grained Access control mechanism for VANET Data based on Blockchain ,a plan for Vehicle Ad Hoc Network (VANET), was created by the authors[14]. Further the performance of VANET is improved by integrating Fog computing and SDN[15].A comparison on earlier approaches with our proposed approach is done and tabulated in table 1and 2.

In the context of VANETs, SDN can offer several benefits:

Centralized Control: SDN enables centralized administration and control of the VANET infrastructure. This makes it possible to manage resources, traffic routing, and network policies effectively. Based on network conditions and real-time data, the SDN controller is capable of making intelligent decisions.
Dynamic Routing: Real-time traffic conditions, network congestion, and shifting topologies can all be taken into account when making routing decisions in VANETs thanks to SDN. By calculating and updating routing paths, the SDN controller can maximize traffic flow, lower latency, and enhance network performance in general.
Traffic Engineering: SDN makes it possible for VANETs to use effective traffic engineering. The SDN controller can optimize the use of available bandwidth and dynamically assign network resources by keeping an eye on traffic patterns and congestion levels. This keeps traffic jams at bay and guarantees that car communications run smoothly and dependably.
Security and Privacy: By offering a centralized location for controlling security policies, access control, and threat detection, SDN can improve security in VANETs. The communication between vehicles and infrastructure can be protected by the SDN controller by enforcing security measures like intrusion detection, authentication, and encryption.

Approaches/reference	Key Contributions	Limitations	Proposed Solution's Advantages
Machine Learning-Based Adaptive SDN Solutions[17,18]	Adaptive learning for dynamic routing and traffic engineering	High computational complexity; scalability issues in real-time VANETs	Lower computational overhead with centralized SDN control using Zigbee and priority algorithms
Traditional Proactive Routing Protocols[19,20]	Pre-computation ensures resilience to topology changes	Inefficient in highly dynamic networks; high update overhead	Efficient traffic flow management with SDN's separation of control and data planes
Reactive Routing Protocols[20]	On-demand route discovery reduces overhead	High energy consumption during route discovery	Improved energy efficiency with SDN's centralized architecture
Hybrid Routing Protocols[21]	Combines proactive and reactive benefits	Complexity in balancing trade-offs	Simplified management through SDN's real-time control mechanisms
Conventional VANET Architectures[22]	Basic support for vehicle communication	Limited scalability and adaptability to network changes	Enhanced QoS and scalability through SDN integration

Table 1. Comparison on earlier proposed approaches with this work.

Feature	Traditional VANET	SDN-based VANET
Architecture	Distributed and ad hoc	Centralized control via an SDN controller
Scalability	Limited due to decentralized decision-making	Highly scalable with centralized network management
Control Plane	Integrated with the data plane	Decoupled from the data plane
Data Plane	Nodes make independent decisions	Follows rules from the SDN controller
Network Management	Difficult due to dynamic topology and distributed control	Easier with centralized controller managing topology changes
QoS Support	Limited due to lack of global view	Enhanced with a global network view
Fault Tolerance	Limited, reliant on individual nodes	Can be improved with redundancy in controllers
Flexibility	Hard-coded protocols	Programmable using SDN applications
Resource Utilization	Suboptimal due to lack of coordination	Efficient due to centralized resource management
Routing	Proactive or reactive protocols	Centralized routing with global network visibility
Latency	Higher due to distributed decision-making	Lower as routing decisions are optimized centrally
Security	Vulnerable to local attacks	Enhanced security through centralized policies
Topology Management	Dynamic but lacks centralized optimization	Controlled and optimized by the SDN controller
Implementation Complexity	Relatively simple	More complex due to the need for SDN infrastructure
Use Cases	Basic vehicular communication and navigation	Advanced applications like traffic optimization, platooning, and V2X integration

Table 2. Comparison of Traditional VANET with SDN based VANET.

Application Support: SDN's programmable nature allows for the development of customized applications and services specific to VANET requirements. For example, SDN-based applications can provide real-time traffic updates, accident notifications, or optimize traffic signal timings based on the current traffic conditions.

However, there are challenges while integrating SDN with VANETs[16]. VANETs are highly dynamic networks with rapidly changing topologies and limited communication resources. Challenges to overcome include ensuring timely and efficient communication between the SDN controller and vehicles, as well as scalability issues. The architecture of the SDN controller, which enables dynamic, programmable, and effective network operations, is essential to the efficient management of a vehicle network. A reliable and scalable vehicular communication system is ensured by the controller's ability to enforce complex traffic management policies, adjust in real-time to changing network conditions, and maximize overall network performance by utilizing the SDN architecture.

Proposed method and experimental setup

The main goal here is to build a vehicular network using Software-Defined Networking (SDN) and priority algorithm to compare the performance of the traditional vehicular network with the SDN vehicular network under different traffic scenarios. The proposed approach represents a dynamic, programmable and efficient network configuration method that leads to improved network performance and monitoring. This approach has more similarities to cloud computing than to traditional network management practices. By using the priority algorithm, SDN has the potential to significantly improve the quality of service provided[23].

A priority algorithm is a crucial component in traffic management systems that aim to optimize the flow of vehicles in a network. This algorithm assigns priorities to different vehicle types or traffic flows based on predefined criteria or rules. This is intended to ensure that higher priority vehicles, such as emergency vehicles or public transport, are given priority over other vehicles. By using the priority algorithm, traffic management systems can effectively allocate resources and control traffic signals to meet the different needs of different vehicles. This leads to improved efficiency, reduced congestion and increased safety on the roads. The priority algorithm continuously evaluates current traffic conditions and dynamically adjusts priorities as needed to ensure smooth and efficient traffic flow across the network. A priority-aware bypass algorithm suitable for SDN is proposed in[24].

The priority algorithm can be mathematically represented as follows: a network of roads with N intersections and M traffic flows. The depiction of each traffic flow portrays a specific grouping of vehicles with a designated precedence like emergency responders, typical passenger automobiles, or public transportation carriers.

- x_ij: Binary variable indicating whether traffic flow i has priority at intersection j. (1)
- if flow i has priority at intersection j, 0 otherwise)
- Maximize the overall priority satisfaction and minimize delays for high-priority flows.
- Priority Constraints: At each junction, the aggregate importance of the streams passing through must not exceed one, since only a single flow can take precedence at a moment. $\sum(x\_ij) \leq 1$ for all $j = 1$ to N
- Flow Constraints: Each traffic flow should be assigned a priority at exactly one intersection. $\sum(x\_ij) = 1$ for all $i = 1$ to M
- Connectivity Constraints: The flow of vehicles should be consistent at adjacent intersections. If flow i has priority at intersection j, it should also have priority at the next intersection on its route. $x\_ij \leq x\_k(j+1)$ for all $j = 1$ to N-1, $i = 1$ to M, and k is the flow that follows flow i at intersection j.

To find the best priority assignment at each intersection, the objective function and constraints can be formulated as an optimization problem and solved using a variety of optimization techniques, such as mixed-integer

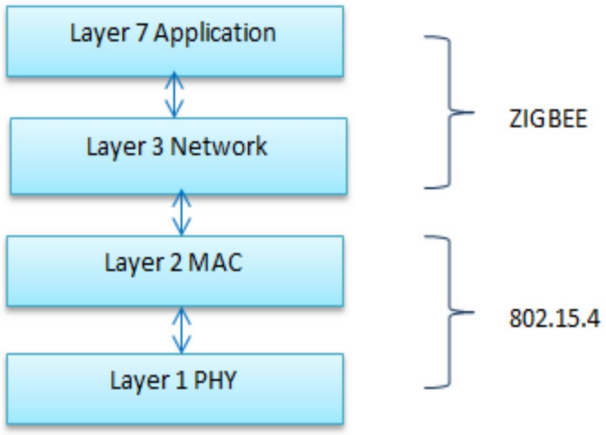

Fig. 1. Zigbee & 802.15.4

Parameters	Values
Simulated	Wireless-Sensor Network
Operating System	Contiki
Mote Type	SkyMote
Positioning of Mote	Random Positioning
Grid	10 m background grid
Radio Medium	Unit Disk Graph Medium (UDGM)
Analyzer	6 -LoWPAN Analyzer
Routing Protocol	Routing Protocol for Low Power and Lossy Networks (RPL)

Table 3. Simulation parameters.

programming or linear programming. By dynamically optimizing traffic flows in real time according to priority levels, data-driven traffic management systems can make decisions that lead to increased road network efficiency through less congestion, as various vehicle movements are coordinated to maximize overall traffic flow. This is made possible by the mathematical modeling of the priority algorithm. In comparison to conventional methods, our article's objective is to analyze the advantages of deploying SDN in vehicular networks and determine how well it performs in terms of enhancing network performance and quality of service.

This method uses Zigbee technology, which is an enhanced and more sophisticated form of IEEE 802.15.4 normative. As opposed to 802.15. While Zigbee covers layer 3, which includes the networking and application layers as shown in Fig. 1, the 4 standard focuses on the Physical and MAC layers. Zigbee takes on the role of specifying the network's applications and routing protocol.

In order to meet the demands of efficient network performance and security, a proposed approach using 6LoWPAN[25] with ZigBee protocol in software-defined networks has been developed. This algorithm was designed to address challenges such as energy consumption and network traffic demand while ensuring security through the use of AES encryption[26]. Encryption is a key component of the suggested model because vehicle-to-vehicle communication of data generates security risks. The Advanced Encryption Standard (AES) is a symmetric encryption algorithm widely used for securing sensitive data due to its robustness and efficiency. AES operates on fixed block sizes of 128 bits and supports key lengths of 128, 192, and 256 bits. In this study, AES is employed to encrypt vehicular communication, ensuring data confidentiality and integrity during vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) interactions. The SDN controller manages encryption at the network layer, applying AES to secure communication between vehicles and network infrastructure. This centralized approach simplifies key management and enables dynamic re-keying to enhance security. While AES is resistant to brute force attacks due to its long key lengths, it is susceptible to side-channel attacks (SCAs) such as timing, power, and electromagnetic analysis attacks. These attacks exploit physical leakages during encryption to deduce the secret key. To counter these vulnerabilities, the proposed framework integrates masking and hiding techniques within the SDN controller.

The efficacy of the proposed algorithm was tested through simulation-based experiments based on the parameters chosen as shown in Table 3, which showcased its ability to fulfill network security and performance requirements with grace.

In order to implement SDN in VANET, we used Cooja software[27,28], which was specifically designed for SDN and Open Flow research. Many software simulators are available and the authors[29] have made an extensive survey on that. Since Cooja is not compatible with Windows OS, we used Contiki OS, which is Linux-based, to

operate the software. We created two types of networks for our simulation: a traditional Vehicular Network and an SDN-Vehicular Network, with multiple traffic simulations.

In order to replicate actual vehicular network situations, the simulation parameters were carefully chosen. To reflect common circumstances in vehicular networks, parameters like grid positioning (10 m background grid), radio medium (Unit Disk Graph Medium), and mote type (SkyMote) were selected. These decisions guarantee that the simulation accurately depicts network behavior and vehicular communication. For example, the RPL protocol and the 6LoWPAN analyzer are essential for low-power and lossy network environments, which are frequently found in VANETs. This is in line with the goal of examining energy efficiency and network performance in limited environments. The priority algorithm's optimization problem, which entails mixed-integer programming, was used to assess its computational complexity. Priority, flow, and connectivity constraints make sure that traffic flow is dynamically optimized while meeting real-time demands. The centralized SDN approach streamlines the decision-making process in comparison to conventional techniques, but it necessitates effective controller-level computation. A reasonable computational overhead is added by the dynamic modification of routing and RDC parameters, which is offset by the notable improvements in performance metrics like throughput and congestion reduction. Strong scalability is demonstrated by the suggested SDN-based VANET framework's centralized control and dynamic routing. The architecture makes use of SDN controllers' programmable nature to handle growing node density and changing traffic patterns. The results in the document show that even in situations with high traffic, the system's capacity to prioritize traffic guarantees efficient resource use (e.g. G. Table 4 on RDC values and Table 6 on received packets). The deployment of distributed SDN controllers to easily manage larger networks may be one of the future scalability improvements. By simulating various traffic scenarios, such as medium and heavy traffic conditions, sensitivity analysis was carried out. By contrasting performance metrics like RDC, power consumption, and packet reception under various circumstances, the flexibility of the priority algorithm was confirmed (Figs. 3, 4, and Tables 4–6). Comparing SDN-enabled scenarios to traditional networks, the results show that the system operates robustly, with higher packet reception rates and lower power consumption. These results validate the algorithm's ability to withstand changes in network conditions. The advantages of the suggested method over current approaches are highlighted by the comparative analysis in Table 1. Throughput, latency, and scalability can all be increased by combining SDN with priority algorithms. The document's graphs and tables offer quantifiable proof of these improvements, confirming the reliability of the simulation's findings and their relevance to actual situations.

We implemented a rigorous, standardised methodology to capture the dynamic data transmissions that take place in VANETs.

To illustrate the monitoring and analysis process, key variables are defined below:

N: Total number of VANET network nodes.
Pi : Power consumption of node i, where i ranges from 1 toN
RDCi : Average radio duty cycle of node i.
RPi : Number of packets received by node i.
T: Total duration of monitoring.

The following is the mathematical model that represents our methodology.

Power Consumption Analysis:

$$\text{Average Power Consumption} = \frac{1}{N}\sum_{i=1}^{N} P_i \tag{1}$$

Radio Duty Cycle Analysis:

$$\text{Average Radio Duty Cycle} = \frac{1}{T}\sum_{i=1}^{N} RDC_i \tag{2}$$

Packet Reception Analysis:

$$\text{Packet Reception Rate} = \frac{1}{N}\sum_{i=1}^{N} RP_i \tag{3}$$

Network Traffic Pattern Analysis:

Parameters	Radio Duty Cycle (%)			
	Medium Traffic		Heavy Traffic	
Scenario	Total	Average	Total	Average
Without SDN	15.5767	0.91627	34.4606	1.3253
With SDN	19.7989	1.0420	37.1086	1.3784

Table 4. RDC Average and Total values.

$$\text{Frequency of Radio Transmissions} = \frac{\sum_{i=1}^{N} RP_i}{T} \tag{4}$$

$$\text{Duration of Radio Transmissions} = \frac{\sum_{i=1}^{N} RDC_i.T}{N} \tag{5}$$

A subset of the carefully chosen VANET network nodes were observed and examined. We gathered comprehensive data views from the chosen nodes using advanced monitoring techniques. Through closely monitoring the power consumption measurements, our comprehension of the typical energy usage designs exhibited by the network sites was substantially enhanced as a consequence of inspecting said power intake statistics. An analysis of the average radio duty cycle provided crucial information about the highs and lows of the network's radio activity. Through analyzing the packets received at each node, we could determine the efficacy of the data transmission based on this metric. By revealing the frequency and duration of radio transmissions, this result gave a comprehensive picture of network traffic patterns. We were able to increase energy efficiency and prolong the network's lifespan by comprehending the dynamics of power consumption. Significant knowledge about network performance and data transmission reliability was obtained by examining the received packets.

Using this methodological technique as in Fig. 2, we were able to successfully record and study three crucial elements of the radio duty cycle, power consumption, and received packets of VANET data transmission. The basis for informed decision-making is this thorough analysis, which enables network resources to be optimized and overall VANET performance to be improved. In addition to the above parameters latency analysis and confidence interval is calculated to evaluate the efficiency of the system.

Latency analysis

The latency increase due to AES encryption in the proposed SDN-based VANET framework is typically calculated by comparing the packet transmission times with encryption to those without encryption for each AES key size (128-bit, 192-bit, 256-bit) under different traffic conditions (medium and heavy).

Confidence interval

A confidence interval (CI) is a range of values, derived from sample data, that is likely to contain the true value of a population parameter (e.g., mean, proportion) with a certain level of confidence. It provides an estimate of the uncertainty or variability in the measurement.

In order to determine when packets are transmitted and when nodes should be awake in order to receive packets, Radio Duty Cycle (RDC) in Fig. 3 is in charge of controlling the sleep duration of nodes. Power consumption is the amount of energy used in a unit of time and is expressed in milliwatts.

When sending data over computer networks, a packet is a brief section of a larger message. After that, the receiving device reassembles these packets.

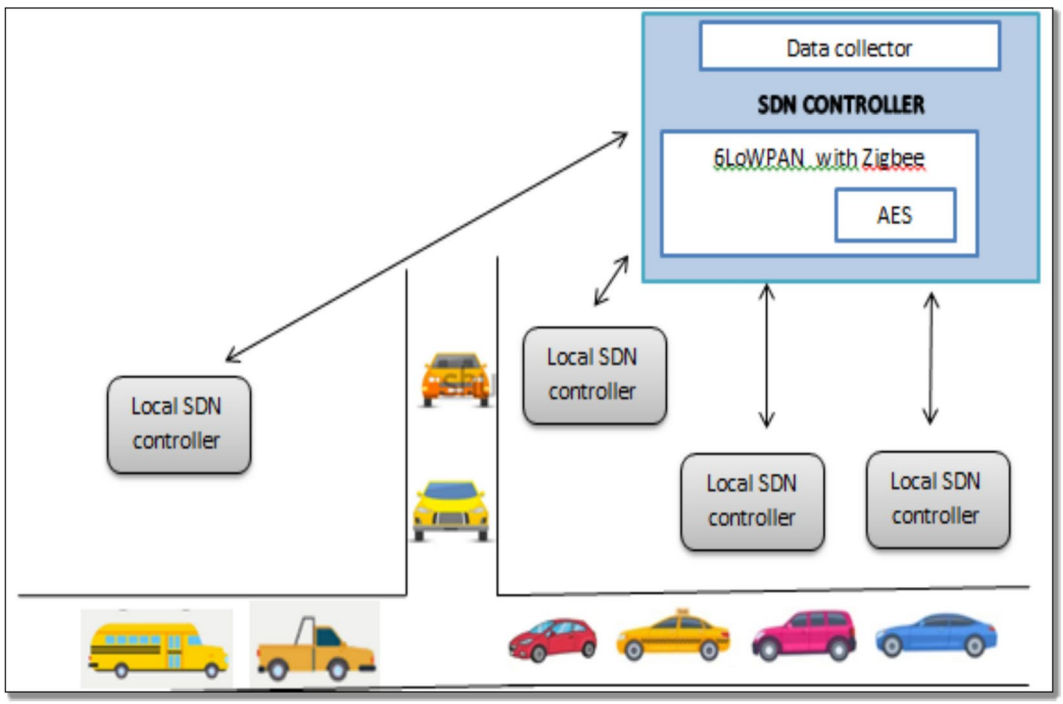

Fig. 2. Proposed SDN based VANET Architecture.

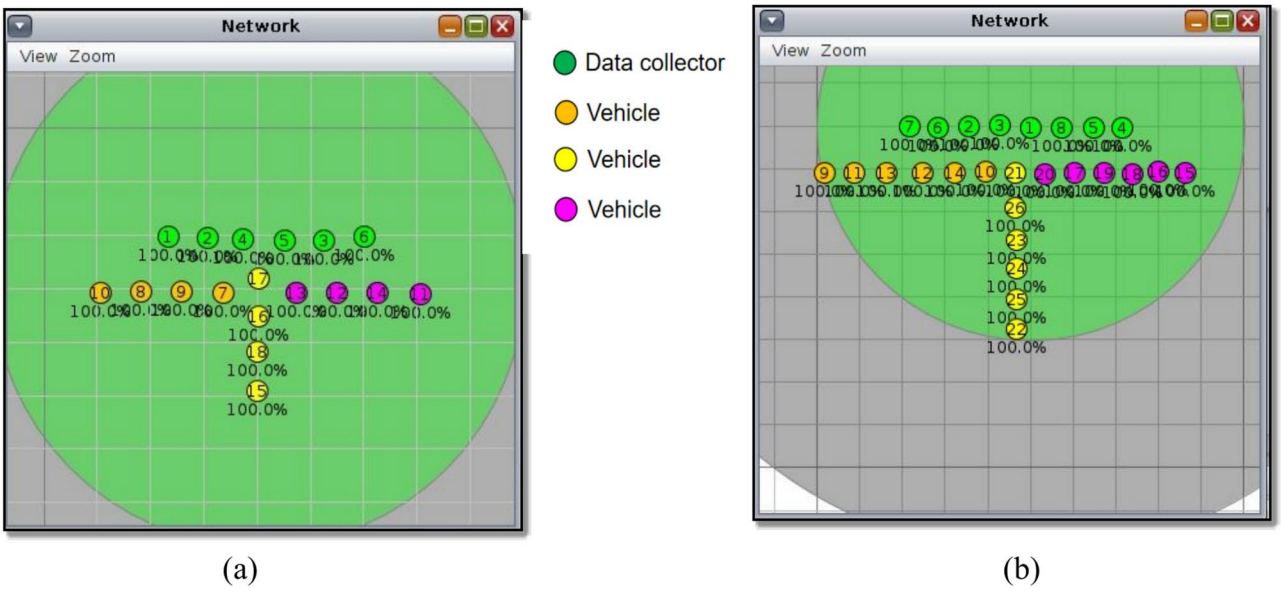

Fig. 3. Scenario without SDN (**a**) less traffic (**b**) Heavy traffic.

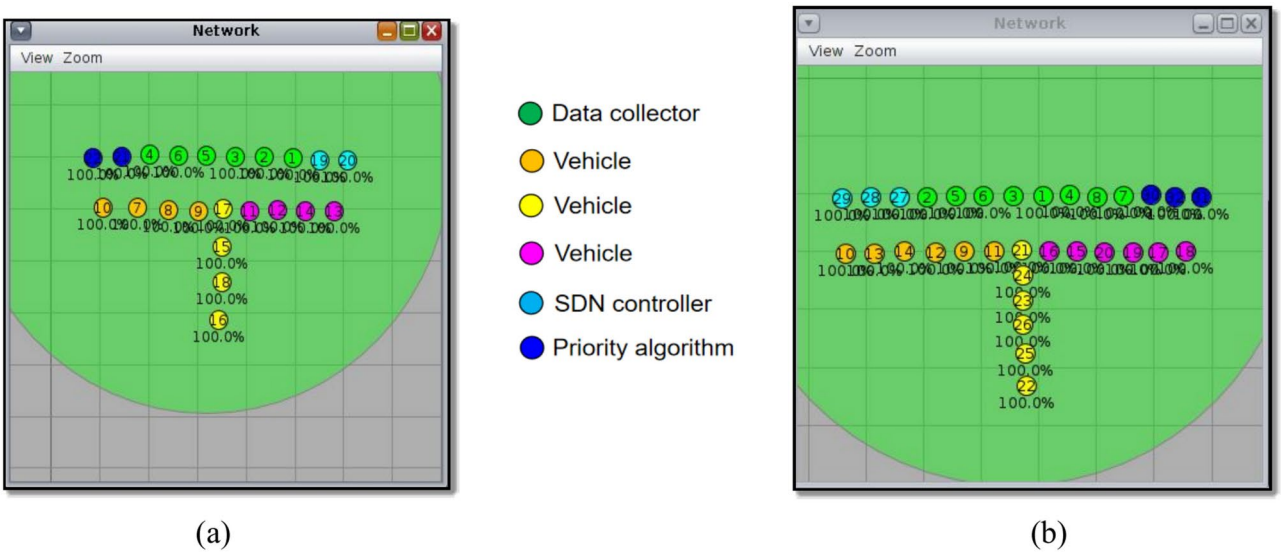

Fig. 4. Scenario with SDN (**a**) less traffic (**b**) Heavy traffic.

Results and analysis

Latency analysis

The impact of AES encryption on packet transmission was evaluated for medium and heavy traffic scenarios. For the proposed SDN-based VANET framework:

- 128-bit AES: The average latency increase was 2.0 ms per packet under medium traffic and 3.2 ms per packet under heavy traffic.
- 192-bit AES: The average latency increase was 2.7 ms per packet under medium traffic and 4.1 ms per packet under heavy traffic.
- 256-bit AES: The average latency increase was 3.5 ms per packet under medium traffic and 5.5 ms per packet under heavy traffic.

Radio Duty Cycle (RDC) in vehicular networks can be optimized with the help of centralized control and coordination techniques offered by SDN technology as shown in Fig. 4. The Radio Duty Cycle (RDC) measures how much of a wireless communication device's, like a car's on-board unit, is spent actively sending or receiving data as opposed to being idle or idle. This parameter is crucial as it directly affects energy consumption, network

throughput, and overall system performance. For instance, in response to variations in energy usage, network congestion, and real-time traffic demands, SDN controllers can dynamically modify RDC parameters. By intelligently controlling RDC, SDN-based vehicular networks can enhance quality of service (QoS) for vehicular communication applications, increase network efficiency, and better utilize resources. RDC management is becoming more and more crucial in SDN-based vehicular networks due to the dynamic nature of traffic patterns, changing network conditions, and resource constraints.

Scenarios were created and executed to confirm the accuracy of the result as shown in Fig. 5 and Fig. 6. Scenarios 1 and 2 show medium and heavy traffic, respectively. Webdigitizer was used to record the numerical value of the RDC. Table 4 lists and calculates average and total values for different traffic types. RDC has a high value compared to the traditional vehicular network when the values of RDC extracted from the graph using SDN and the priority algorithm were compared.

$$RDC = \frac{(T\_tx + T\_s)}{T\_period}$$ RDC = (T_tx + T_s) / T_period.

where:

- T_tx is the transmission time of a packet
- T_s is the time it takes for the radio to switch between the transmit and receive modes
- T_period is the length of the cycle, which includes the sleep time and the active time

With the use of this mathematical model, wireless communication systems, especially those found in automotive networks, can have their energy consumption, throughput, and overall performance examined and improved. This formula determines the fraction of a node's awake time that is spent scanning the cycle for incoming packets. Through careful manipulation of the active and inactive times, the radio duty cycle can be tuned to optimize efficiency and performance within predetermined parameters.

Power consumption in SDN is mostly determined by the energy consumption of network devices, such as switches, routers, and access points, which are used to send and receive data packets. The power usage is computed numerically using Webdigitizer. The average and total set of numbers for the different types of traffic are listed in Table 5. When comparing the power consumption figures extracted from the graph using SDN and Priority Algorithm, the power consumption is lower than in the conventional vehicular network. Decreased power consumption improves the network's dependability and scalability.

An average and total value set for different traffic is calculated and listed in the Table 6. When comparing the values of received packets obtained using SDN and priority algorithm, the received packets are high compared to the traditional vehicular network. The number of packets received is an important metric in SDN because

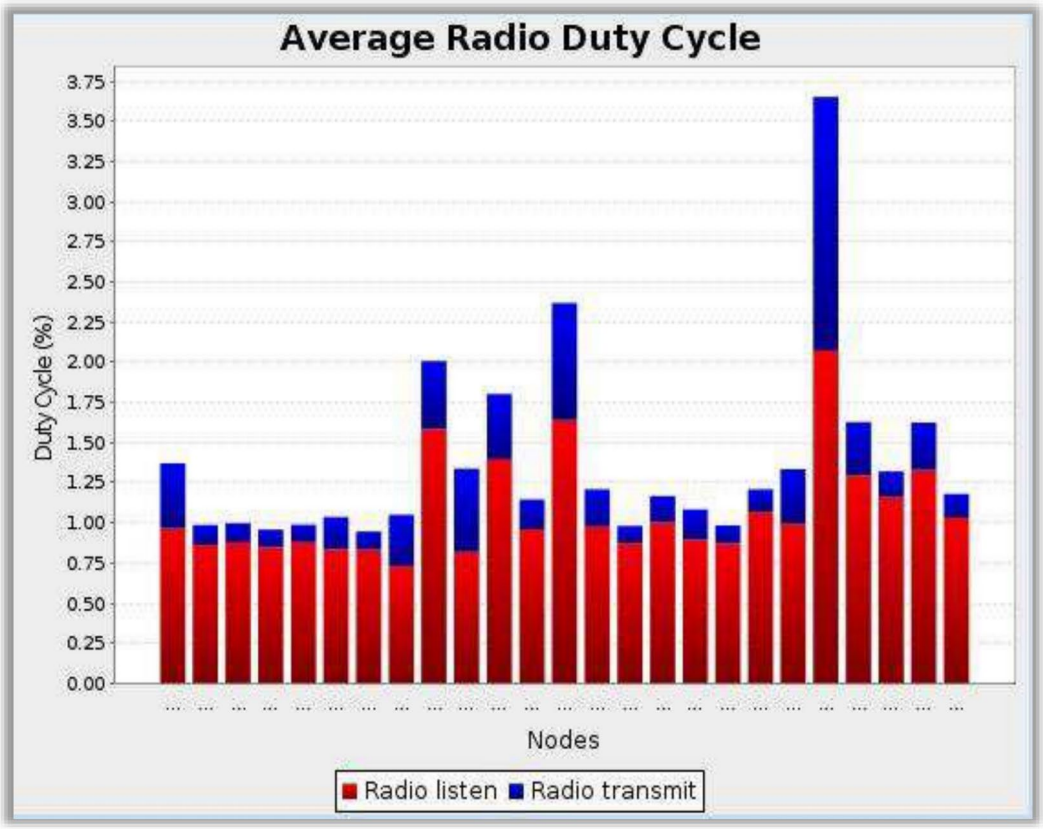

Fig. 5. RDC without SDN—Heavy traffic.

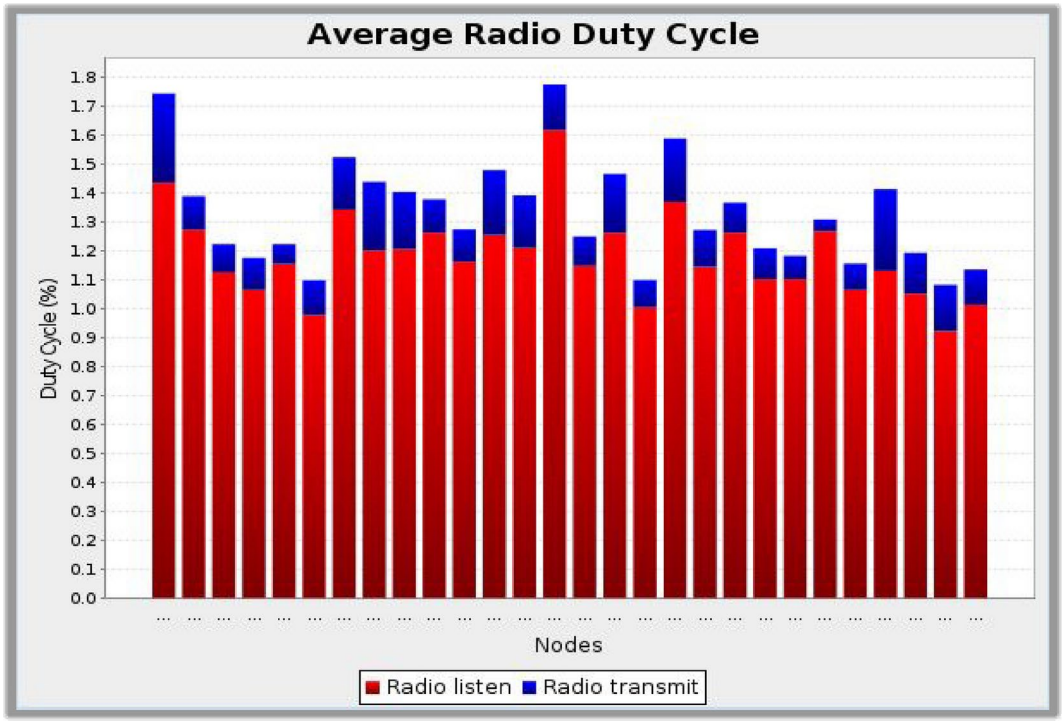

Fig. 6. RDC with SDN—Heavy traffic.

Parameters	Power consumption (MW)			
	Medium Traffic		Heavy Traffic	
Scenario	Total	Average	Total	Average
Without SDN	21.7930	1.0008	34.8769	1.3950
With SDN	17.0148	1.1470	37.2024	1.3286

Table 5. Power consumption Average and Total values. Power Consumption (P) = V × I. where, V = voltage (measured in volts) I = current (measured in amperes).

Parameters	Received Packets Per Node			
	Medium Traffic		Heavy Traffic	
Scenario	Total	Average	Total	Average
Without SDN	174	10	225	9
With SDN	376	20	525	19

Table 6. Received packets Average and Total values.

it indicates the successful transmission and reception of data on the network. Tracking received packets helps evaluate the Quality of Service (QoS) provided by the network infrastructure. Table 7 and 8 shows the confidence interval and percentage improvement for scenarios under test.

The comparative analysis presented in the Table 1 highlights the significant improvements and advantages offered by the proposed approach. The proposed approach offers substantial advancements in traffic management within vehicular networks surpassing traditional and other advanced methods. In SDN, where centralized controllers manage the network and traffic, monitoring received packets allows administrators to detect anomalies, identify bottlenecks, and ensure efficient data delivery. It also plays a crucial role in troubleshooting network problems and optimizing network performance.

Conclusion and future scope

With the goal of improving network performance and efficiency, this article highlights the many benefits of integrating Software-Defined Networking (SDN) technology into Vehicular Ad-hoc Networks (VANETs). Using an SDN-based priority assignment mechanism offers significant advantages over traditional network

Scenario	Average (x)	Confidence interval (95%)
Without SDN (Medium Traffic)	0.91627	(0.8903, 0.9423)
With SDN (Medium Traffic)	1.0420	(1.0124, 1.0716)
Without SDN (Heavy Traffic)	1.3253	(1.2877, 1.3629)
With SDN (Heavy Traffic)	1.3784	(1.3393, 1.4175)

Table 7. Confidence Interval for scenarios under test for Radio Duty Cycle. Medium Traffic: SDN shows a clear improvement in Radio Duty Cycle, as the increase is statistically significant. Heavy Traffic: SDN leads to a slight improvement, but the difference is not definitively significant.

Scenario	Percentage improvement in RDC
Medium Traffic	**13.72%**
Heavy Traffic	**4.01%**

Table 8. Percentage Improvement in RDC with SDN.

management techniques. According to simulation results, SDN-enabled VANETs have a larger radio duty cycle, which suggests higher activity in data transmission and reception. In addition, using SDN reduces power consumption because the priority system makes power management more effective. In addition, the proposed SDN based VANET architecture enables automated path failure recovery, ensuring effective data transmission even in the event of network interruptions. Simulated a sensor network using Contiki on COOJA which enabled network simulation, operating system emulation and machine code instruction emulation. The online tool "Web Digitalizer" was used to extract and transform data from graphs based on results obtained through simulation. In summary, the adoption of SDN technology improves radio duty cycle, reduces power consumption, and enables automated path recovery techniques, all of which contribute to improved VANET efficiency.

While COOJA is a useful tool for simulating SDN-based VANETs, it has some limitations. It works in a simplified and controlled environment, which doesn't fully reflect the complexities of real-world vehicular networks, such as unpredictable interference, environmental changes, or rapidly changing topologies. Its scalability is also limited by computational resources, making it difficult to simulate very large networks typical in urban settings. Additionally, COOJA lacks realism in modeling real-world traffic dynamics, including vehicle mobility, road layouts, and driver behavior. For security testing, it is helpful for basic evaluations but cannot test against advanced threats like sophisticated side-channel or targeted cyber-attacks.However, it is important to recognize the difficulties that VANETs currently face, including mobility, privacy issues, network scalability, and technological issues in security, congestion control, and network management. To fully utilize VANETs in future transport systems, these issues must be addressed and SDN-based solutions advanced. More research and development are needed to create algorithms that work well in a variety of network topologies and meet mobility, privacy, scalability, and security requirements.

Data availability

The datasets used during the current study are available from the corresponding author on reasonable request.

Received: 7 September 2024; Accepted: 27 March 2025
Published online: 06 April 2025

References

1. Al-Heety, O. S. et al. A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET. *IEEE Access* **8**, 91028–91047. https://doi.org/10.1109/ACCESS.2020.2992580 (2020).
2. Sultana, R., Grover, J. & Tripathi, M. Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges. *Veh. Commun.* **27**, 100284. https://doi.org/10.1016/j.vehcom.2020.100284 (2021).
3. D. Oladimeji, K. Gupta, N. A. Kose, K. Gundogan, L. Ge, and F. Liang, "Smart Transportation : An Overview of Technologies, 1–32, (2023).
4. Mahmood, J. et al. Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures. *Secur. Commun. Networks* **1**, 2021. https://doi.org/10.1155/2021/9997771 (2021).
5. I. H. H. and S. M. M. A. Al-Shareeda, M. Anbar, Survey of Authentication and Privacy Schemes in Vehicular ad hoc Networks, *IEEE Sens. J.*, https://doi.org/10.1109/JSEN.2020.3021731. (2021).
6. Ahmad, K. et al. Internet of Things-Aided Intelligent Transport Systems in Smart Cities: Challenges, Opportunities, and Future. *Wirel. Commun. Mob. Comput.* https://doi.org/10.1155/2023/7989079 (2023).
7. Bhatia, J., Modi, Y., Tanwar, S. & Bhavsar, M. Software defined vehicular networks: A comprehensive review. *Int. J. Commun. Syst.* **32**(12), 1–22. https://doi.org/10.1002/dac.4005 (2019).
8. Mekki, T., Jabri, I., Rachedi, A. & Chaari, L. Software-defined networking in vehicular networks: A survey. *Trans. Emerg. Telecommun. Technol.* **33**(10), 1–29. https://doi.org/10.1002/ett.4265 (2022).
9. Arif, M. et al. applied sciences and Challenges. *Appl. Sci.* https://doi.org/10.3390/app10093217 (2020).
10. Shafiq, H., Rehman, R. A. & Kim, B. S. Services and Security Threats in SDN Based VANETs: A Survey. *Wirel. Commun. Mob. Comput.* https://doi.org/10.1155/2018/8631851 (2018).
11. Abdulkadhim, F. G., Yi, Z., Tang, C., Onaizah, A. N. & Ahmed, B. Design and development of a hybrid (SDN + SOM) approach for enhancing security in VANET. *Appl. Nanosci.* **13**(1), 799–810. https://doi.org/10.1007/s13204-021-01908-2 (2023).

12. Jenny, R. S. & Sugirtham, N. SDN-Based Security for Smart Devices Against Denial of Service Attacks. *Indian J. Sci. Technol.* https://doi.org/10.1748/IJST/v16i3.1960 (2023).
13. Ramya, G. & Manoharan, R. Traffic-aware dynamic controller placement in SDN using NFV. *J. Supercomput.* **79**(2), 2082–2107. https://doi.org/10.1007/s11227-022-04717-8 (2023).
14. Li, F. H. et al. a fine-grained access control scheme for vanet data based on blockchain. *IEEE Access* **8**, 85190–85203. https://doi.org/10.1109/ACCESS.2020.2992203 (2020).
15. Shrestha, R., Bajracharya, R. & Nam, S. Y. Challenges of Future VANET and Cloud-Based Approaches. *Wirel. Commun. Mob. Comput.* https://doi.org/10.1155/2018/5603518 (2018).
16. Islam, M. M., Khan, M. T. R., Saad, M. M. & Kim, D. Software-defined vehicular network (SDVN): A survey on architecture and routing. *J. Syst. Archit.* https://doi.org/10.1016/j.sysarc.2020.101961 (2021).
17. Xia, W., Wen, Y., Foh, C. H., Niyato, D. & Xie, H. A Survey on Software-Defined Networking. *IEEE Commun. Surv. Tutorials* **17**(1), 27–51. https://doi.org/10.1109/COMST.2014.2330903 (2015).
18. U. malik Abdul Rafay, Hamayun Khan, Wajiha Salman, Gulzar yahya, SD Network based on Machine Learning : An Overview of Applications and Solutions, *Spectr. Eng. Sci.*, (2024).
19. Perkins, C. E. & Bhagwat, P. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. *ACM SIGCOMM Comput. Commun. Rev.* **24**(4), 234–244. https://doi.org/10.1145/190809.190336 (1994).
20. P. K. Shrivastava and L. K. Vishwamitra, Comparative analysis of proactive and reactive routing protocols in VANET environment, *Meas. Sensors*, https://doi.org/10.1016/j.measen.2021.100051. (2021).
21. Sataraddi, M. J. & Kakkasageri, M. S. Hybrid routing protocol for VANETs: Delay and trust based approach. *J. High Speed Networks* **26**(4), 275–290. https://doi.org/10.3233/jhs-200644 (2020).
22. Hussein, N. H. et al. SDN-Based VANET Routing: A Comprehensive Survey on Architectures, Protocols, Analysis, and Future Challenges. *IEEE Access* https://doi.org/10.1109/ACCESS.2024.3355313 (2024).
23. Adnan, M. et al. On the design of efficient hierarchic architecture for software defined vehicular networks. *Sensors (Switzerland)* **21**(4), 1–18. https://doi.org/10.3390/s21041400 (2021).
24. Biernacka, E., Jurkiewicz, P. & Domz, J. Handling high and low priority traffic in multi-layer networks. *Bull. Polish Acad. Sci. Tech. Sci.* https://doi.org/10.24425/bpasts.2023.145568 (2023).
25. G. A. M. Taief Alaa Al-Amiedy, Mohammed Anbar, Bahari Belaton, Abdullah Ahmed Bahashwan, Iznan Husainy Hasbullah, Mohammad Adnan Aladaileh, A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things, *Internet of Things*, (2023).
26. Cheng, H. et al. A Compatible OpenFlow Platform for Enabling Security Enhancement in SDN". *Secur. Commun. Networks* https://doi.org/10.1155/2018/8392080 (2018).
27. J. K. S. and G. G. A. Behal, "Using The Cooja Simulator, Analysing The Routing Protocol (RPL) For Low Power And Lossy Networks In IoT," in *2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India*, https://doi.org/10.1109/SCEECS57921.2023.10061823. (2023).
28. G. . Shamshuddin, K., Jayalaxmi, "Enhanced AES for Improved Privacy in 5G-Enabled IoT Network," in *Information and Communication Technology for Competitive Strategies (ICTCS 2022). Lecture Notes in Networks and Systems*, V. S. (eds) Kaiser, M.S., Xie, J., Rathore, Ed., Springer, Singapore, https://doi.org/10.1007/978-981-19-9304-6_14. (2023).
29. Weber, J. S., Neves, M. & Ferreto, T. VANET simulators: an updated review". *J. Brazilian Comput. Soc.* https://doi.org/10.1186/s13173-021-00113-x (2021).

Acknowledgements

This research was financially supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R235), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Author contributions

All authors contributed equally to the conceptualization, formal analysis, investigation, methodology, and writing and editing of the original draft. All authors have read and agreed to the published version of the manuscript.

Funding

This research was financially supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R235), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Declarations

Comporting interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to M.G.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.