Indonesian Journal of Electrical Engineering and Computer Science
Vol. 42, No. 1, April 2026, pp. 252~262
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v42.i1.pp252-262

Enhancing AODV protocol for black hole attack detection and mitigation in VANETs: a lightweight dual-confirmation approach

Ahmed Abderraouf[1,2], Ramdane Taglout[3,4], Sofiane Boukli-Hacene[2]
[1]Department of Sciences and Technology, University of Tamanrasset, Tamanrasset, Algeria
[2]Evolutionary Engineering and Distributed Information Systems Laboratory, Djilali Liabes University, Sidi Bel Abbes, Algeria
[3] Department of Computer Science, Faculty of Exact Sciences, University of Bouira, Bouira, Algeria
[4]LIM Laboratory, Faculty of Exact Sciences, University of Bouira, Bouira, Algeria

Article Info

Article history:

Received Jun 26, 2025
Revised Dec 21, 2025
Accepted Mar 4, 2026

Keywords:

AODV protocol
Black hole attack
Network security
VANETs network

ABSTRACT

Vehicular ad hoc networks (VANETs) represent a specialized category of Mobile ad hoc networks that are specifically designed to enable communication among autonomous (self-driving or partially self-driving) vehicles. These vehicles are equipped with onboard computers, network interfaces, and sophisticated sensors for data capture and processing. Within a VANET, vehicles have the ability to communicate with each other as well as with surrounding infrastructure, thereby exchanging critical messages aimed at enhancing road safety, reducing traffic congestion, and enabling new services and applications for drivers and passengers. Due to its unique characteristics, VANETs have succeeded in enhancing transportation efficiency and safety. However, VANETs are vulnerable to black hole attacks, where malicious nodes discard packets, compromising safety. Existing solutions suffer from high overhead or infrastructure dependence. We propose a lightweight enhancement to AODV using dual-confirmation (RepAck/Info packets) to detect and isolate attackers in real time. Simulations show a 98% improvement in packet delivery ratio under attack, with minimal protocol modifications. While routing overhead increases by 25%, this trade-off ensures reliable communication in dynamic VANETs.

Corresponding Author:

Abderraouf Ahmed
Department of Sciences and Technology, Faculty of Sciences and Technology, University of Tamanrasset
Tamanrasset, Algeria
Email: abde3raouf@gmail.com

1. INTRODUCTION

Over the past decade, mobile ad hoc networks (MANETs) have gained significant attention due to their decentralized architecture and ability to support dynamic, infrastructure-less communication. Within this domain, VANETs have emerged as a specialized subset, enabling autonomous communication between vehicles and between vehicles and infrastructure nodes, such as roadside units (RSUs) [1]. VANETs are designed to improve traffic safety, reduce congestion, and support intelligent transport applications by enabling real-time information sharing among vehicles through onboard sensors, computing units, and wireless communication devices [2].

VANET communication is typically categorized into vehicle-to-vehicle (V2V) and Vehicle-to-Infrastructure (V2I) modes. V2V allows direct communication between vehicles without the need for fixed infrastructure [3], while V2I relies on RSUs for extended communication coverage and centralized coordination [4]. However, the high mobility of vehicles and frequent changes in network topology make the design of efficient

and adaptive routing protocols particularly challenging. Consequently, many routing protocols originally designed for MANETs, such as the ad hoc on-demand distance vector (AODV) protocol, have been adapted for VANET environments [5], [6]. Yet, these protocols often lack built-in mechanisms to handle emerging security threats [7]. One of the most critical security challenges in VANETs is the black hole attack, where a malicious node falsely advertises optimal routes to attract data packets and then discards them, causing data loss and compromising network integrity [8]. Given VANETs' reliance on shared information for real-time decision-making, such attacks have severe consequences for road safety and can result in loss of life. Compromised safety systems may fail at critical moments, directly causing accidents, collisions, and fatalities [9], [10].

Numerous studies have proposed mechanisms to detect and mitigate black hole attacks. Gautham and Shanmughasundaram [11] developed a two-phase detection scheme using RSUs. In the first phase, RSUs verify routing responses against a master routing table to identify inconsistencies; the second phase uses dummy (route request) RREQ packets to confirm malicious behavior. This approach leverages collaboration between RSUs and vehicles for rapid threat elimination. Cherkaoui *et al.* [12] proposed a statistical process control (SPC)-based method to monitor real-time metrics such as throughput and delay, using variable control charts to detect anomalies without modifying routing protocols. Kancharakuntla and El-Ocla [13] developed the enhanced blackhole resistance (EBR) protocol for MANETs, which uses test requests and round-trip time measurements to isolate malicious nodes based on a trust metrics strategy adaptable to VANETs.

Other notable approaches include Stępień's smart intelligent nodes (SIN) algorithm [9], which periodically verifies node identities and routes to isolate suspicious nodes. Krundyshev *et al.* [14] adapted the Intelligent water drops (IWD) swarm intelligence algorithm to handle vehicular mobility and detect routing anomalies. Hassan *et al.* [15] proposed the intelligent black hole detection algorithm (IDBA), which combines hop count, sequence number, packet delivery ratio, and end-to-end delay to enhance reliability in autonomous vehicle networks. Despite these advancements, a gap remains in developing unified, lightweight solutions that balance security and efficiency in dynamic VANET environments. While prior work [9], [11]-[19] has proposed detection mechanisms, many rely on centralized RSUs or introduce significant computational overhead, rendering them unsuitable for highly mobile VANETs. A lightweight, decentralized solution is urgently needed for real-time attack mitigation without compromising network performance.

This paper proposes the lightweight dual-confirmation approach (LDCA), a lightweight method for black hole attack detection and mitigation. LDCA implements a dual-confirmation mechanism where intermediate nodes send both a route reply (RREP) to the source and an acknowledgment (ACK) to the destination. If the destination receives the ACK but no data packet within the timeout period, it marks the route as suspicious, alerts the source, and initiates malicious node isolation. Additionally, these dual-confirmation packets (RepAck and Info) provide secondary benefits for QoS and energy optimization. The RepAck packet enables additional route discovery, while the Info packet delivers fresh route information, reducing redundant route discovery processes and conserving energy and memory. Table 1 in APPENDIX provides a summary of the literature review of mitigate black hole attacks in VANET

2. PROPOSED METHODOLOGY

This approach is distinguished from others [9], [11]-[19] by several characteristics. Most notably, its capability is not limited to detecting black hole attacks alone; rather, it is scalable to cover multiple types of attacks, in particular, those that lead to denial of service such as: (Wormhole attack, Sybil attack, Jellyfish attack and Grayhole attacks…), because it is helped by the destination node, in contrast to most approaches that operate only on the source and intermediate nodes. This solution also improves routing efficiency by eliminating the need for route rediscovery. Instead of initiating a new route discovery process when a link failure occurs due to an attack, it exploits an alternative route traced by the info packet, avoiding the time and resource costs typically associated with traditional route rediscovery mechanisms.

To achieve this purpose, the proposal approach requires modifying the standard AODV protocol by introducing two new control AODV packets: the reply acknowledge (RepAck) packet and the Information (info) packet. The RepAck packet is generated by the intermediate node at the same time it generates the RREP packet, but it is sent toward the destination node. While the Info packet, on the other hand, is generated by the destination node if it does not receive the expected data packet, and it is sent to the source node.

The following is a description of the steps and the events for implementing this proposal approach:

- In the context of the route discovery process, when an intermediate node receives an RREQ packet and has a fresh route to the destination node, it simultaneously generates an RREP packet to send toward the source node and a RepAck packet to send toward the destination node. The RepAck packet informs the destination node that it will receive a data packet after a timeout from the source node indicated by the ID address included in the RepAck packet (Algorithm 1).

- While the route request timeout (rt_req_timeout) is defined as the time that a source node must wait after broadcasting a RREQ to receive a RREP before retrying or declaring route discovery failure. To account for additional delays such as data packet transmission, intermediate node processing, and network congestion, the total expected timeout can be conservatively estimated as:

$$\text{timeout} = \frac{3}{2} \times (\text{rt\_req\_timeout}) \quad (1)$$

- When a destination node receives a RepAck packet, it waits for the timeout to expire. If a destination node does not receive a data packet during this timeout, it generates an information (Info) packet and sends it to the source node to inform it that the awaited data packet did not arrive.
- When a source node receives an Info packet from the destination node, it concludes that its data packet did not reach the destination, and that the intermediate node that generated the RREP packet is a malicious node that drops the data packets. Therefore, it generates and broadcasts an alarm packet throughout the network to isolate the attacking node.

Figure 1 presents the Flowchart of LDCA in urban VANET scenarios.

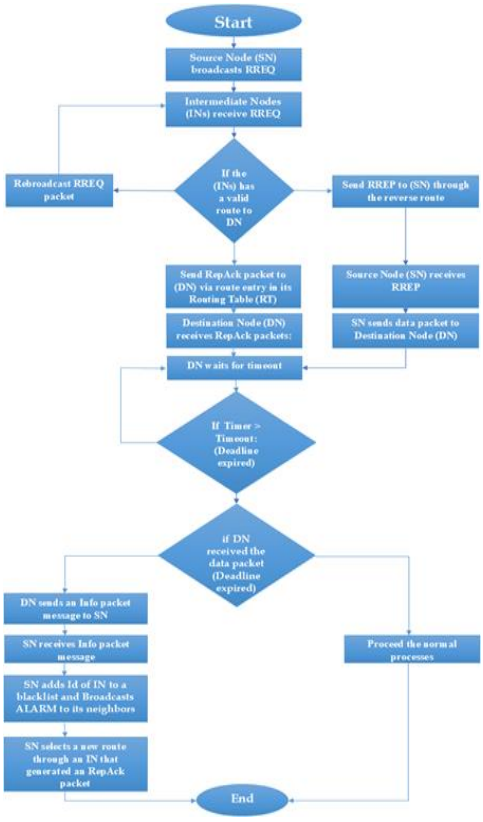

Figure 1. Flowchart of LDCA in urban VANET scenarios

Algorithm 1. Algorithmic Pseudocode

```
// SN:- The Source Node
// DN:- The Destination Node
// IN:- The Intermediate Nodes
// RepAck :- The Reply Acknowledge packet
// Info :- The Information packet
1. start
2. Source Node (SN) broadcasts RREQ
3. Intermediate Nodes (INs) receive RREQ
4. Intermediate Nodes:
  ├── a. Send RREP to SN through the reverse route
  └── b. Send RepAck packet to DN via route entry in its Routing Table (RT)
5. Source Node (SN) receives RREP
6. SN sends data packet to (DN) through (IN)
7. When Destination Node (DN) receives RepAck packets:
```

```
  └── a. DN waits for timeout
8. If Timer > Timeout:
  └── Check if DN received the data packet
  ├── If No:
  │  ├── i. DN sends an Info packet to SN through the reverse route of RepAck packet
  │  ├── ii. SN receives Info packet
  │  ├── iii. SN adds ID of IN to a blacklist
  │  ├── iv. SN broadcasts ALARM to its neighbors
  │  ├── v. SN removes that route
  │  └── vi. SN selects a new route through an IN that generated an RepAck packet
  └── If Yes:
  └── Proceed to end
9. end
```

3. SIMULATION RESULTS

3.1. Parameters and Scenarios of Simulation

Figure 2 illustrates a geographic card of urban VANET scenarios from the town of Malaga [20] that is composed of three areas U1(small), U2(middle) and U3(large). Detailed parameters of the geographic area is presented in the Table 2.

We conducted simulations using ns-2.35, with a maximum of 45 simulated vehicles. The number of connected vehicles varied between 10, 15, 20, 30, and 40, while employing the AODV protocol for routing. Our simulation consisted of three parts: a) Baseline Scenario (No Attack): This part involved simulating the network without any attacks to establish a reference point for comparison; b) AODV under Black Hole Attack with Two Malicious Nodes: In this part, we introduced two black hole nodes into the network to observe the effects of the attack on network performance; c) AODV under Black Hole Attack with Three Malicious Nodes: Here, we increased the number of black hole nodes to three to assess the heightened impact on network performance.

In the scenario used, there is 40 vehicles are simulated, with using AODV routing protocol to simulate data transmission between pairs of communicating nodes during 900s. The primary simulation parameters are presented in Table 3.

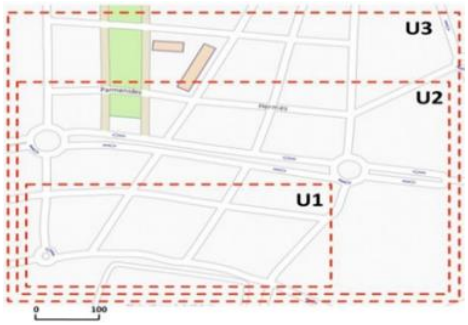

Figure 2. Geographic card of urban VANET scenarios

Table 2. VANET scenarios details

Scenario	Area size	Number of vehicules	Number of connections
urban-small	120,000m^2	40	10,15,20,30,40
urban-middle	240,000m^2	40	10,15,20,30,40
urban-large	360,000m^2	40	10,15,20,30,40

Table 3. Simulation parameters

Parameters	Value
Propagation Model	Nakagami
PHY layer	IEEE 802.11p 5(Phy/WirelessPhyExt)
MAC layer	IEEE 802.11p (Mac/802_11Ext)
Simulation time	900 s
Number of malicious nodes	2, 3
Number of vehicules	40
Number of vehicules connected	10, 15, 20, 30, 40
Area size	120000m^2
timeout	3/2*(rt_req_timeout).
Routing layer	Normal AODV, AODV under black hole, AODV enhanced by our solution

To obtain more accurate simulation results, the Nakagami model is widely used in VANETs because it better reflects real-world wireless channel conditions in vehicular environments [21]. On the other hand, IEEE 802.11p is considered a suitable standard for vehicular communication, specifically for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, as it is designed to handle rapid topology changes caused by high-speed vehicle movement in VANETs [22].

3.2. Performance metrics

In order to measure the efficacy of our proposed solution, we evaluate its performance based on the following four metrics [23], [24]:

- Packet delivery ratio (PDR): refers to the proportion of successfully delivered packets compared to the total number of packets sent in a network communication.
- Average end to end delay (AE2ED): This metric measures the average time required for a data packet to travel from the source node to the destination node across the network, capturing the total transmission delay experienced by packets.
- Drop packets (DP): refers to a mechanism or action in computer networking where packets of data are dropped discarded or not forwarded to their intended destination.
- Routing overhead: This metric quantifies the proportion of routing control packets (RREQ, RREP, RERR, etc.) transmitted relative to the total data packets sent.

4. RESULTS AND DISCUSSION

4.1. Packet delivery ratio

Figure 3 illustrates the packet delivery ratio (PDR) evolution in a VANET under three conditions: standard AODV, AODV under black hole attack, and AODV enhanced with our black hole mitigation solution. These evaluations examine varying numbers of communicating nodes (10 to 40 nodes).

In standard AODV without attacks, PDR remains consistently high (97.16%–98.33%), demonstrating the protocol's robustness in mobile environments even with 40 connected nodes. However, introducing black hole nodes severely degrades performance: PDR drops to 30.97% with one malicious node and further to 29.27% with three malicious nodes. This degradation is most pronounced at maximum network density (40 nodes), where attack impact is amplified.

The proposed solution significantly restores PDR to near-normal levels across all scenarios, even with three malicious nodes. This effectiveness stems from its ability to detect and isolate malicious nodes, thereby enhancing overall network reliability.

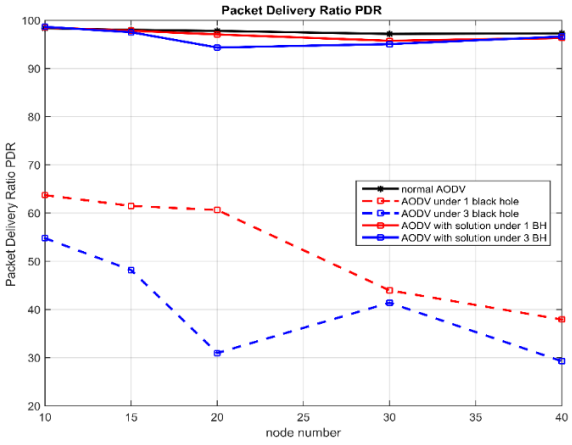

Figure 3. Packet delivery ratio PDR

4.2. Average end to end delay

Figure 4 presents the AE2ED for varying numbers of connected vehicles under three scenarios: standard AODV, AODV subjected to black hole attacks, and AODV fortified with our security solution. In the absence of attacks, normal AODV maintains moderate AE2ED values, ranging from 3.53 ms with 10 vehicles to 29.36 ms with 30 vehicles, averaging 15.89 ms at 20 vehicles. Notably, black hole attacks particularly with three malicious nodes cause a sharp decline in AE2ED, reaching as low as 1.86 ms.

This apparent improvement is deceptive, however, as malicious nodes respond instantly to RREQ packets without routing table verification or updates, unlike legitimate nodes that perform necessary routing table maintenance before responding. The reduced delay actually indicates packets being discarded early by attackers rather than being successfully routed. When our proposed security measures are applied, AE2ED increases noticeably, sometimes exceeding normal values (e.g., 97.01 ms at 20 vehicles). This additional latency results from destination nodes waiting for a timeout period to notify source nodes of missing data packets, ensuring route validation. Although this introduces a delay, it represents a worthwhile trade-off for reliable, secure communication during attack scenarios.

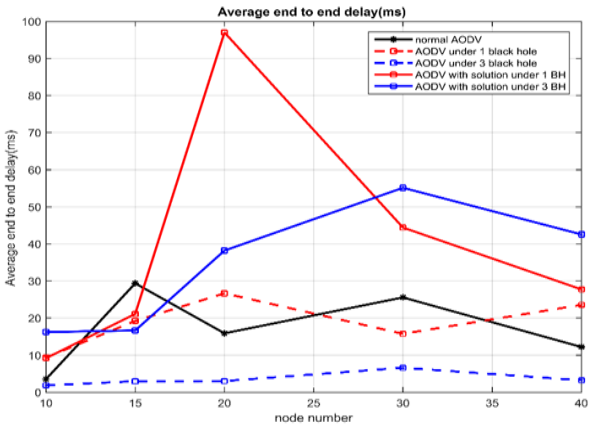

Figure 4. Average end-to-end delay(ms)

4.3. Total packet dropped (TDP)

Figure 5 depicts packet drops in a VANET using AODV routing across multiple scenarios: standard AODV (no attacks), AODV under black hole attacks (one and three malicious vehicles), and AODV enhanced with our security solution during attacks. In standard AODV without attacks, packet drops remain moderate, gradually increasing with network size from 10 to 40 vehicles across all scenarios. Total Packet Dropped (TPD) rises from 5,092 packets at 10 vehicles to 20,610 packets at 40 vehicles, as expected due to higher traffic load and routing complexity in larger networks.

As shown in Figure 5, black hole attacks cause dramatically higher packet drops compared to normal AODV, since malicious nodes position themselves to intercept all communications and absorb forwarded packets between communicating vehicles. With one black hole node, TPD increases sharply from 6,125 packets at 10 vehicles to 41,411 packets at 40 vehicles. With three black hole nodes, the situation worsens significantly, reaching 47,294 dropped packets at 40 vehicles. This trend demonstrates the severe impact of coordinated black hole attacks, which cause massive packet loss through malicious interception and discarding.

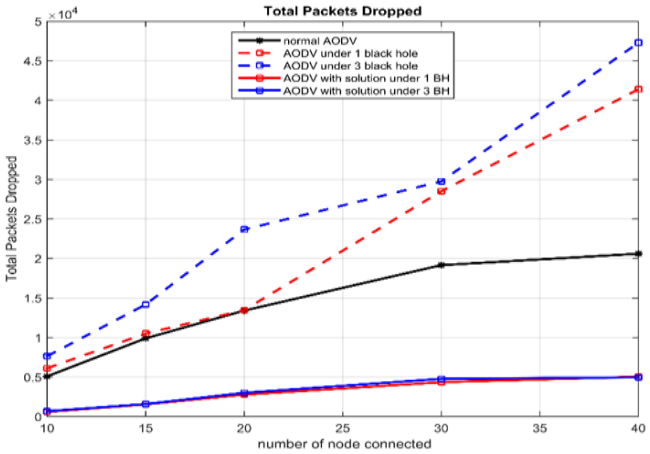

Figure 5. Total packets dropped

However, implementing the enhanced AODV protocol substantially reduces packet drops even under attack conditions. At 40 vehicles with one black hole, TPD drops from 41,411 to 5,047 packets (87.8% reduction). Similarly, with three black holes at 40 vehicles, TPD decreases from 47,294 to 4,975 packets (89.5% reduction). These results indicate that our solution effectively mitigates attack impact and provides reliable packet delivery even in hostile environments.

4.4. Routing overhead

Figure 6 presents simulation results for a VANET network across multiple scenarios: baseline AODV without attacks, AODV under black hole attacks (one and three malicious nodes), and AODV enhanced with our proposed security solution during attacks. In standard AODV, routing overhead exhibits a gradual increase as the number of vehicles grows.

For 10 communicating vehicles, as shown in Figure 6, the routing overhead begins at 127.50 and reaches a peak of 280.69 at 30 vehicles. This pattern is anticipated due to greater control packet generation for route discovery and maintenance in denser networks. Notably, it slightly decreases to 249.68 at 40 vehicles, likely due to route stabilization in more established topologies.

Under black hole attacks, routing overhead drops sharply compared to normal AODV. With one black hole at 10 vehicles, it falls to 34.73; with three black holes, it reaches 83.47. This apparent reduction is misleading, as it stems from disrupted routing processes where malicious nodes issue premature fake route replies, preventing proper route establishment. Consequently, fewer legitimate control packets are generated, but at the cost of invalid routes and substantial data loss.

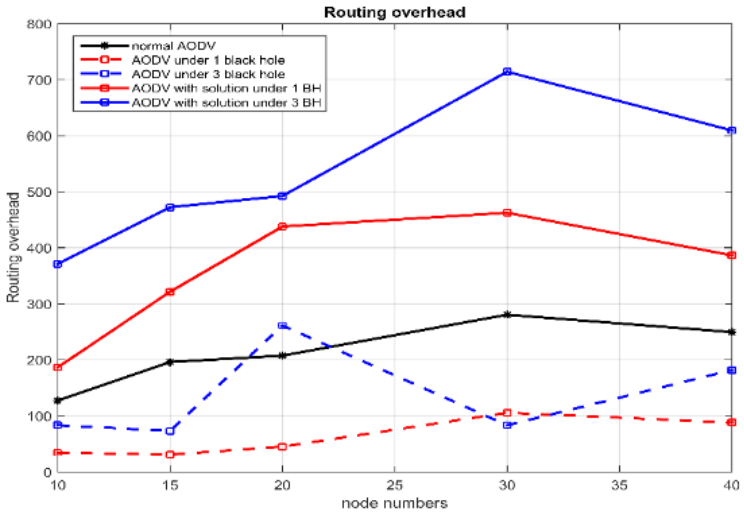

Figure 6. Routing overhead

However, implementing the proposed solution results in substantially higher routing overhead compared to both standard AODV and AODV under attack conditions. For instance, at 20 connected vehicles with one or three malicious nodes, the enhanced AODV shows routing overhead values of 438.03 and 492.60, respectively significantly higher than both normal and attack scenarios. This increase is anticipated and justified by the introduction of two additional control packets, along with supplementary processes including routing verification, path validation, and security mechanisms for detecting and isolating black hole nodes. Despite this overhead, the solution improves packet delivery and network resilience, as evidenced by previous performance metrics.

To assess the effectiveness of the proposed LDCA scheme, Table 4 compares its performance against existing methods EBR [13], DPBHA [25], and AODV_BH_CBAA [26] across key metrics including packet delivery ratio, end-to-end delay, and routing overhead. Table 4 results clearly demonstrate that our proposed LDCA outperforms competing schemes across all metrics. In Packet Delivery Ratio (PDR), LDCA achieves the highest performance at 98%, exceeding DPBHA (95%) and substantially outperforming EBR (80%) and AODV_BH_CBAA (81%). This superiority stems from its precise malicious node detection mechanism, which effectively prevents packet loss due to black hole behavior.

For Average End-to-End Delay, LDCA records an impressively low value of 30 ms far superior to EBR's 5,000 ms, DPBHA's 1,170 ms, and AODV_BH_CBAA's 423.45 ms while maintaining robust

security. Regarding Routing Overhead, LDCA exhibits a manageable value of 4,000, which could be further optimized by leveraging AOMDV's inherent multipath capabilities. Although DPBHA achieves slightly lower overhead (3,500) and AODV_BH_CBAA reports a 3.69% reduction, both suffer from substantially higher delays and inferior PDR. EBR's estimated 45% overhead increase, combined with its prohibitive 5,000 ms latency, renders it unsuitable for real-time applications.

Table 4. Comparison between the proposed scheme and existing schemes

Scheme	year	PDR	E2E delay (average value)	Overhead (average value)
DPBHA [25] (threshold+bait scheme)	2022	95%	1170ms	3500
EBR [13] (trust scheme)	2022	80%	5000ms	Estumed by 45%
AODV_BH_CBAA [26] (cryptographic scheme)	2025	81%	423.45ms	19,693 Reduced by 3.69%
LDCA (our approach)	//	98%	30ms	4000

Unlike existing black hole mitigation schemes, which lack a comprehensive roadmap for overcoming limitations, our LDCA provides a forward-looking framework. It can be extended to AOMDV by utilizing multipath routing: data packets travel the primary path while check packets traverse the secondary path, mitigating delay and overhead increases without compromising security.

5. CONCLUSION

The obtained results clearly demonstrate that the proposed mechanism provides effective and efficient routing security in VANETS against blackhole attacks by effectively detecting and eliminating blackhole attacks, significantly improving the packet delivery ratio (PDR), restoring it to levels close to or better than natural AODV. However, on the other hand, this solution causes an increase in end-to-end delay and routing overhead compared with the original AODV protocol. The increase in term delay is due to the security measures added in our proposal to secure routing, where destination nodes wait a timeout period to inform source nodes if they do not receive a data packet. While the increased routing overhead is due to the additional new control packets, as well as additional consequences such as routing checks, path validation, and security mechanisms introduced to detect and isolate blackhole nodes.

These costs of routing overhead and delay represent a classic security-performance trade-off in network design, it is a worthwhile trade-off for achieving reliable and secure communication in the presence of attacks. Furthermore, this proposed solution offers an applicable future vision for addressing network attacks without negative consequences. This is achieved by applying our approach to the AOMDV protocol, which creates multiple paths for each destination. This feature is used to send a data packet through the first path while simultaneously sending a check packet through the second path. The check packet includes information about the first route. This future vision enables us to overcome all the drawbacks that were faced in the initial proposal based on the AODV protocol, such as increased delay and overhead, as well as detecting attacks accurately and efficiently.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ahmed Abderraouf	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	
Ramdane Taglout		✓				✓			✓	✓	✓	✓		
Sofiane Boukli-Hacene	✓		✓	✓			✓			✓	✓		✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

Data availability does not apply to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] G. Goyal and S. Goel, "A comparative review on state-of-the-art clustering techniques for vehicular ad-hoc networks," in *PDGC 2022 - 2022 7th International Conference on Parallel, Distributed and Grid Computing*, IEEE, Nov. 2022, pp. 276–279. doi: 10.1109/PDGC56933.2022.10053111.

[2] M. J. Patil and K. P. Adhiya, "A Comprehensive study on VANET security," in *Advancements in Smart Computing and Information Security*, 2024, pp. 363–382. doi: 10.1007/978-3-031-59100-6_25.

[3] N. Firdissa, K. A. Gemeda, S. Mishra, D. S. Rathee, R. S. Singh, and T. Darejew, "Disseminating a fair emergency message with V2V communication technology in VANET," *Security and Communication Networks*, vol. 2025, no. 1, Jan. 2025, doi: 10.1155/sec/8882649.

[4] A. K. Sangaiah, A. Javadpour, C. C. Hsu, A. Haldorai, and A. Zeynivand, "Investigating routing in the VANET network: review and classification of approaches," *Algorithms*, vol. 16, no. 8, p. 381, Aug. 2023, doi: 10.3390/a16080381.

[5] M. ul Hassan *et al.*, "ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) using enhanced AODV," *Sensors*, vol. 24, no. 3, p. 818, Jan. 2024, doi: 10.3390/s24030818.

[6] F. S. Sowdagar and K. N. Karamtot, "Design and simulation of cooperative vehicular communication network using enhanced AODV protocol," *Wireless Personal Communications*, vol. 139, no. 2, pp. 985–1012, Nov. 2024, doi: 10.1007/s11277-024-11650-x.

[7] L. P. Pratama, D. Andriyani, A. O. Putri, A. A. Hapsari, D. J. Vresdian, and M. Aldiansyah, "Evaluation performance and routing on VANET architecture: a narrative review," in *Proceedings of Third Emerging Trends and Technologies on Intelligent Systems*, 2023, pp. 233–248. doi: 10.1007/978-981-99-3963-3_19.

[8] S. U. Masruroh, Y. S. Farghani, A. Kusdaryono, A. Fiade, R. A. Putri, and L. A. Pratiwi, "Comparative analysis of testing black hole attack and rushing attack on VANET (vehicular ad-hoc network) with AOMDV routing protocol," in *8th International Conference on Engineering and Emerging Technologies, ICEET 2022*, 2022. doi: 10.1109/ICEET56468.2022.10007272.

[9] K. Stepien and A. Poniszewska-Maranda, "Security methods against black hole attacks in vehicular ad-hoc network," in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, IEEE, Nov. 2020, pp. 1–4. doi: 10.1109/NCA51143.2020.9306724.

[10] J. Lyu, C. Chen, and H. Tian, "Secure routing based on geographic location for resisting blackhole attack in three-dimensional VANETs," in *2020 IEEE/CIC International Conference on Communications in China (ICCC)*, IEEE, Aug. 2020, pp. 1168–1173. doi: 10.1109/ICCC49849.2020.9238997.

[11] P. S. Gautham and R. Shanmughasundaram, "Detection and isolation of black hole in VANET," in *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, IEEE, Jul. 2017, pp. 1534–1539. doi: 10.1109/ICICICT1.2017.8342799.

[12] B. Cherkaoui, A. Beni-hssane, and M. Erritali, "Variable control chart for detecting black hole attack in vehicular ad-hoc networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 11, pp. 5129-5138, 2020, doi: 10.1007/s12652-020-01825-2.

[13] D. Kancharakuntla and H. El-Ocla, "EBR: Routing Protocol to Detect Blackhole Attacks in Mobile Ad Hoc Networks," *Electronics*, vol. 11, no. 21, p. 3480, Oct. 2022, doi: 10.3390/electronics11213480.

[14] V. Krundyshev, M. Kalinin, and P. Zegzhda, "Artificial swarm algorithm for VANET protection against routing attacks," in 2018 IEEE Industrial Cyber-Physical Systems (ICPS), IEEE, May 2018, pp. 795–800. doi: 10.1109/ICPHYS.2018.8390808.

[15] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, "Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles," *IEEE Access*, vol. 8, pp. 199618–199628, 2020, doi: 10.1109/ACCESS.2020.3034327

[16] A. Kumar *et al.*, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors and Microsystems*, vol. 80, p. 103352, Feb. 2021, doi: 10.1016/j.micpro.2020.103352.

[17] M. Kumar, V. Jain, A. Jain, U. S. Bisht, and N. Gupta, "Evaluation of black hole attack with avoidance scheme using AODV protocol in VANET," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 2, pp. 277–291, Feb. 2019, doi: 10.1080/09720529.2019.1585635.

[18] A. Malik, M. Z. Khan, S. M. Qaisar, M. Faisal, and G. Mehmood, "An efficient approach for the detection and prevention of gray-hole attacks in VANETs," *IEEE Access*, vol. 11, pp. 46691–46706, 2023, doi: 10.1109/ACCESS.2023.3274650.

[19] S. Younas, F. Rehman, T. Maqsood, S. Mustafa, A. Akhunzada, and A. Gani, "Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs," *Applied Sciences (Switzerland)*, vol. 12, no. 23, p. 12448, Dec. 2022, doi: 10.3390/app122312448.

[20] J. Toutouh, J. García-Nieto, and E. Alba, "Intelligent OLSR routing protocol optimization for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1884–1894, May 2012, doi: 10.1109/TVT.2012.2188552.

[21] R. Peng, X. Zhang, and P. Shi, "Multi-representation domain adaptation network with duplex adversarial learning for hot-rolling mill fault diagnosis," *Entropy*, vol. 25, no. 1, p. 83, Dec. 2023, doi: 10.3390/e25010083.

[22] M. Sepulcre, M. Gonzalez-Martin, J. Gozalvez, R. Molina-Masegosa, and B. Coll-Perales, "Analytical models of the performance of IEEE 802.11p vehicle to vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 1, pp. 713–724, Jan. 2022, doi: 10.1109/TVT.2021.3124708.

[23] E. Ngatunga, M. Kissaka, and A. T. Abdalla, "Performance evaluation of cluster-based schemes for message dissemination in a vehicle-to-vehicle communication in urban environment," *Cogent Engineering*, vol. 11, no. 1, Dec. 2024, doi: 10.1080/23311916.2024.2348885.

[24] L. Mohaisen and L. Joiner, "Towards delay tolerant networking for connectivity aware routing protocol for VANET-WSN communications," *Applied Sciences*, vol. 13, no. 6, p. 4008, Mar. 2023, doi: 10.3390/app13064008.

[25] A. Malik, M. Z. Khan, M. Faisal, F. Khan, and J. T. Seo, "An efficient dynamic solution for the detection and prevention of black hole attack in VANETs," *Sensors*, vol. 22, no. 5, p. 1897, Feb. 2022, doi: 10.3390/s22051897.

[26] M. Ghute and Y. Suryawanshi, "Discovering authentic routes using a cryptographic approach against blackhole attack," *Eurasip Journal on Wireless Communications and Networking*, vol. 2025, no. 1, p. 86, Oct. 2025, doi: 10.1186/s13638-025-02494-5.

APPENDIX

Table 1. Summarized literature review of VANET

References	Year	Approach description	PDR	Delay	Overhead	Advantage	Disadvantage (Limitations)
Kumar *et al*. [17]	2020	Modified AODV with cryptographic security measures for source and destination node verification. Enhanced RREQ and RREP packets with encryption/decryption functions.	The average PDR for the proposed approach is 75.28%, which is improved compared to standard AODV	The average end-to-end delay of this proposed approach is 0.03375, which shows decrease compared to standard AODV	Routing request overhead measured	Better packet delivery ratios and reduced delays compared to traditional methods	Higher computational overhead due to cryptographic operations
Kumar *et al*. [18]	2019	Anomaly-based intrusion detection system comparing destination sequence numbers. Uses threshold-based detection where constant DSN indicates malicious behavior. Mitigation discards packets with DSN greater than normal threshold.	City: ~60-80% (with mitigation), Highway: ~40-60% (with mitigation), Random: ~70-85% (with mitigation)	City: ~25ms reduction, Highway: ~100ms increase during attack, Random: ~50ms average	Low overhead because it do not generate significant additional costs in a AODV protocol and a simple computation of comparison operations.	Simple implementation, effective in different mobility scenarios, 25% delay reduction with mitigation	Position and timing of malicious node affects performance, requires threshold calibration
Malik *et al*. [19]	2023	Detection and Prevention of Gray Hole Attacks (DPGHA) mechanism combining trust-based evaluation and efficient routing. Uses dynamic threshold values of abnormal differences in received, forwarded, and generated packets.	The average PDR for this proposed is estimed as 87.75%. improved by 3.0% compared to other schemes	Decreased by 6.13% compared to existing methods	Reduced by 3.69% compared to traditional approaches	Proactive prevention, improved security and dependability, high detection accuracy	Complex trust calculation, may have higher computational requirements
Younas *et al.* [20]	2022	Neural network-based collaborative detection system for both black hole and gray hole attacks. Emphasizes timely detection to prevent data loss and systematic reactions against dangerous behavior.	The average PDR for this proposed is assumed to be a high ratio due to the packet drop rate being much less	leads to optimal end-to-end delay	Optimized routing overhead due to lower processing overhead	Superior performance, handles both attack types, timely detection, enhanced security	Neural network training complexity, computational overhead

BIOGRAPHIES OF AUTHORS

Abderraouf Ahmed is an assistant professor in the Department of Sciences and Technology, University of Tamanrasset, Algeria. He received an engineering degree from Dr Moulay Tahar University of Saida in 2007, the M.S. (new information and communication technologies) degree from the Djillali Liabes University (U.D.L) of Sidi Bel Abbes, Algeria in 2009. The Ph.D. (Routing Security in the Network) degree from U.D.L in 2024. His research interests include network security, including mobile ad hoc networks, sensor networks, and vehicular networks. He can be contacted at email: abde3raouf@gmail.com.

Ramdane Taglout received his B.Sc in 2012 from the Computer Science and Technology of Information Department, Faculty of New Information Technologies and Communication, Kasdi Merbah University, Ouargla, Algeria. He is currently a Ph.D. student at the Department of Computer Science, University of Bouira. His research interests include visual tracking, computer vision, machine learning, and deep learning. He can be contacted at email: r.taglout@univ-bouira.dz.

Sofiane Boukli-Hacene is an associate professor in the Computer Science Department of Djillali Liabes University (U.D.L) of Sidi Bel Abbes, Algeria. He received an engineering degree (first class honours) from U.D.L in 2002, the M.S. degree from Al Al Bayt University at Mafraq, Jordan in 2005, the Ph.D. degree from U.D.L in 2012, and the habilitation to supervise research (HDR) in 2014. He is the head of the Advanced Networks research team and "Evolutionary Engineering and Distributed Information Systems Laboratory" at the U.D.L. His research interests are in networking, including wireless ad-hoc, sensor networks, vehicular networks, network security, and QoS. He can be contacted at email: boukli@gmail.com.