Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 9, S. 218-222, 7, 2025
© Telif hakkı IJANSER'e aittir
Araştırma Makalesi

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN:2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 9, pp. 218-222, 7, 2025
Copyright © 2025 IJANSER
Research Article

Performance and Security Analysis of ACO-AODV Protocol in Urban VANET Environments

Neila Berrekhchi Berrahma[1*], Merahi Bouziani[1], Sofiane Boukli-Hacene[2], Chahinaz Kandouci[1]

[1]*Telecommunications and Digital Signal Processing Laboratory, Djillali Liabes University, Sidi Bel Abbes, Algeria*
[2]*Evolutionary Engineering and Distributed Information Systems Laboratory, Djillali Liabes University, Sidi Bel Abbes, Algeria.*

neilabekhchiberrahma@gmail.com

(Received: 15 July 2025, Accepted: 21 July 2025)

(5th International Conference on Scientific and Innovative Studies ICSIS 2025, July 15-16, 2025)

ATIF/REFERENCE: Berrahma, N. B., Bouziani, M., Boukli-Hacene, S. & Kandouci, C. (2025). Performance and Security Analysis of ACO-AODV Protocol in Urban VANET Environments, *International Journal of Advanced Natural Sciences and Engineering Researches*, 9(7), 218-222.

Abstract – Vehicular Ad Hoc Networks (VANETs) play a central role in the development of Intelligent Transportation Systems (ITS) by enabling efficient communication between vehicles (V2V) and with road infrastructure (V2I). Although they offer significant advantages in terms of security, traffic management and mobility, their highly dynamic structure makes them vulnerable to attacks, especially the Blackhole attack, which seriously compromises communications reliability.

In previous work, we proposed ACO-AODV, an enhanced version of the AODV protocol that incorporates Ant Colony Optimization (ACO) principles. This bio-inspired mechanism improves route selection by considering signal strength, latency, and available bandwidth.

In this study, we compare the performance of the ACO-AODV protocol under normal conditions with that of the ACO-AODV-B protocol, exposed to a Blackhole attack.

Our objective is to evaluate the endurance of the ACO-based approach against malicious behavior by analyzing key performance metrics such as packet delivery rate (PDR), average end-to-end delay and normalized routing load.

Simulation results reveal a marked degradation in performance under attack, highlighting the limitations of the current protocol and emphasizing the need for integrated detection and mitigation techniques to strengthen VANET security.

Keywords –VANET, AOD, ACO, BLACKHOLE, NS2.

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) play a crucial role in the evolution of intelligent transport of intelligent transport systems (ITS), facilitating communication between vehicles (V2V) and with the road infrastructure (V2I)[1]. Although they enhance safety, optimize traffic management and facilitate mobility, VANETs remain vulnerable to attacks due to their dynamic topology[2]. One of the most dangerous is the black hole attack, in which a malicious node falsely advertises the shortest path and drops intercepted packets[3].

In a previous work, we proposed ACO-AODV, an enhancement of the AODV protocol based on Ant Colony Optimization (ACO), integrating parameters such as bandwidth, latency and signal strength for more efficient route selection.

This study evaluates the impact of Blackhole attacks on ACO-AODV. Unlike prior research that generally compares AODV and ACO-AODV, our main contribution lies in a detailed performance comparison of ACO-AODV under normal conditions and under Blackhole attack.

The remainder of this article is organized as follows: Section 2 presents our simulation methodology, Analysis of the experimental results obtained is analyzed in detail in Section 3. Finally, section 4 concludes this work and proposes possible improvements to enhance the security of VANET networks against Blackhole attacks.

II. METHODOLOGY

In this study, we implement an approach combining the analysis of a Blackhole attack and the use of the enhanced ACO-AODV protocol for VANETs.

In a blackhole attack, a malicious node intercepts a source node's RREQ request and responds with a fake RREP containing a high sequence number, posing as the optimal path. The source node then updates its routing table and transmits its data via this false path, enabling the blackhole to intercept and then drop the packets.

To enhance the robustness of routing against this type of attack, we employed ACO-AODV, an optimized version of AODV incorporating the principles of Ant Colony Optimization (ACO). This protocol selects routes by taking into account signal strength, latency and bandwidth, through a fitness function that evaluates the quality of each link. Pheromone values, reflecting this quality, are updated in RREQ packets and routing tables. The path with the highest pheromone value is chosen to transmit the data, and an evaporation mechanism enables routes to be dynamically adapted to the evolution of the network. This methodology enables us to compare the performance of the ACO-AODV protocol under normal conditions and in the presence of a blackhole attack, in order to evaluate its resilience.

Nguyen Duy Tan et al [4]. examine the impact of Blackhole attacks on the AODV protocol in MANET networks. Their study highlights network performance degradation due to packet loss and increased energy consumption in the presence of malicious nodes. However, their analysis remains limited to a generic MANET environment and does not integrate the specificities of VANETs, such as high mobility, fast topology variation or urban environment constraints. In contrast, our work focuses precisely on vehicular networks and takes into account more realistic dynamic parameters, such as signal strength, latency and bandwidth.

Ankit Kumar et al[1]. have proposed a secure version of the AODV protocol for VANETs, based on the modification of RREQ and RREP packets and the addition of cryptographic techniques for node authentication. Although this approach enhances security, it also introduces an additional computational load due to encryption, without addressing the optimization of routing performance under normal conditions. Our work is therefore distinguished by a bio-inspired approach, ACO-AODV, which not only improves routing efficiency under normal conditions, but also makes it possible to assess its robustness against a blackhole attack, without resorting to heavyweight security mechanisms.

Thus, unlike these two works, our study proposes a dual contribution: an optimization of routing via ACO based on link quality parameters, and an in-depth analysis of the protocol's resilience to blackhole attacks, in a realistic urban context.

III. SIMULATION AND RESULTS

A. Simulation environments

In our work We simulated urban VANET scenarios based on the real road topology of downtown Malaga, Spain [5], [6], using NS-2 (version 2.35). The physical layer uses the IEEE 802.11p (802.11ext) standard, and the Nakagami model was used for radio propagation [7]. AODV was used for the network layer. Simulations were carried out on a geographical area of 2 km × 1 km with 10 to 40 vehicles. Table 1 summarizes simulation parameters.

Table 1. Parameters used in simulation

Parameters	**Value**
Propagation Model	Nakagami
PHY layer	IEEE 802.11p
Routing layer	ACO-AODV , ACO-AODV-B
Transport layer	TCP
Area size	2000mx1000m
Number of Vehicles	10,15,20,30,40
Packet size	512 bytes
Simulation time	180s

B. Analysis of the experimental results

This section compares the performance of the enhanced ACO-AODV protocol under normal conditions with ACO-AODV under blakhole attack (ACO-AODV-B). The evaluation is based on three key performance metrics: packet delivery rate, end-to-end delay and normalized routing overhead.

Table2. Performance analysis of delay

Number of vehicle	**AODV-ACO**	**AODV-ACO-B**
10	42,3723ms	2083,33 ms
15	66,3256ms	1545,45 ms
20	55,028 ms	328,767 ms
30	55,3364 ms	1141,03 ms
40	67,5022 ms	1360,66 ms

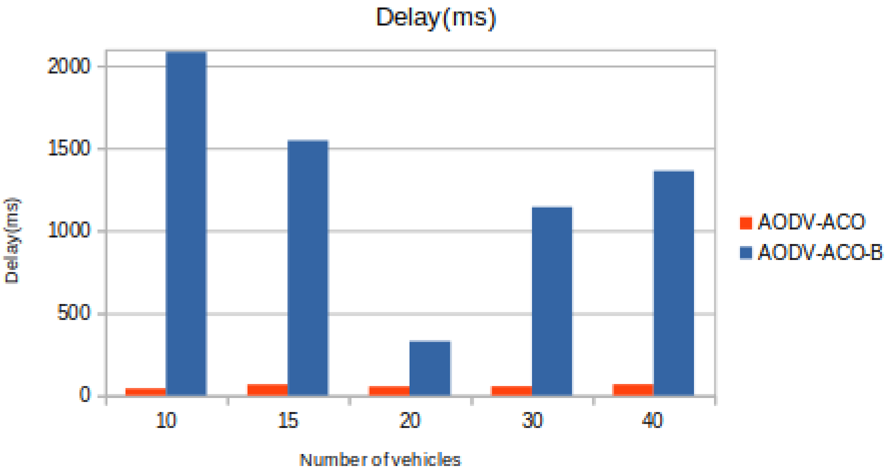

Figure 1. Delay(ms)

Fig.1 and table2 present a comparison of the average delay between the AODV-ACO protocol (without attack) and AODV-ACO-B (under Blackhole attack) as the number of vehicles in the VANET increases. It is evident that AODV-ACO consistently maintains a very low delay across all network sizes, demonstrating its efficiency in selecting stable and fast routes by considering signal strength, latency, and available bandwidth. In contrast, under a Blackhole attack, the delay increases significantly. This is due to disrupted communications caused by the malicious node, which intercepts and drops packets, forcing repeated route discoveries. A temporary drop in delay at 20 vehicles may be attributed to increased path redundancy, but the delay rises again with larger network sizes, indicating that the impact of the attack worsens in denser networks. These results highlight that while AODV-ACO performs well under normal conditions, its performance is considerably degraded in the presence of a Blackhole attack.

Table3. Performance analysis of PDR

Number of vehicle	AODV-ACO	AODV-ACO-B
10	98,4774%	48,4375%
15	98,6164%	20%
20	99,2129%	50%
30	99,0059%	39,42%
40	97,9627%	20,75%

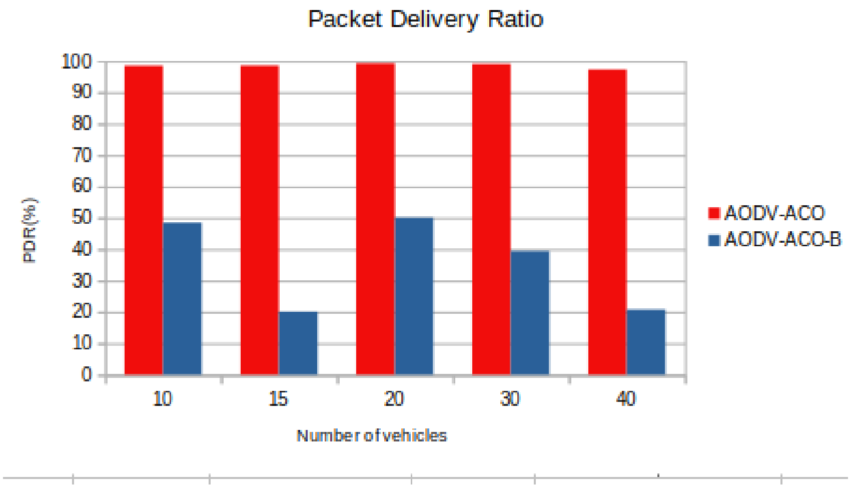

Figure2. Packet delivery ratio

Fig.2 and table3 show the evolution of PDR for two protocols ACO-AODV protocol, under normal conditions, and its version ACO-AODV-B, under a Blackhole attack, in a VANET network with a variable number of vehicles. We observe that the ACO-AODV protocol maintains a high PDR, close to 100%, demonstrating its effectiveness in ensuring reliable transmission thanks to its routing strategy based on ant colonies. On the other hand, when the network is exposed to a Blackhole attack (ACO-AODV-B), the PDR drops significantly. This drop is due to the behavior of the malicious node, which attracts traffic to itself by using the best route, before dropping the intercepted packets.

Table4. Performance analysis of NRL

Number of vehicle	AODV-ACO	AODV-ACO-B
10	0.006	1,5
15	0.038	3,6
20	0.02	1,22
30	0.048	1,556
40	0.197	6,143

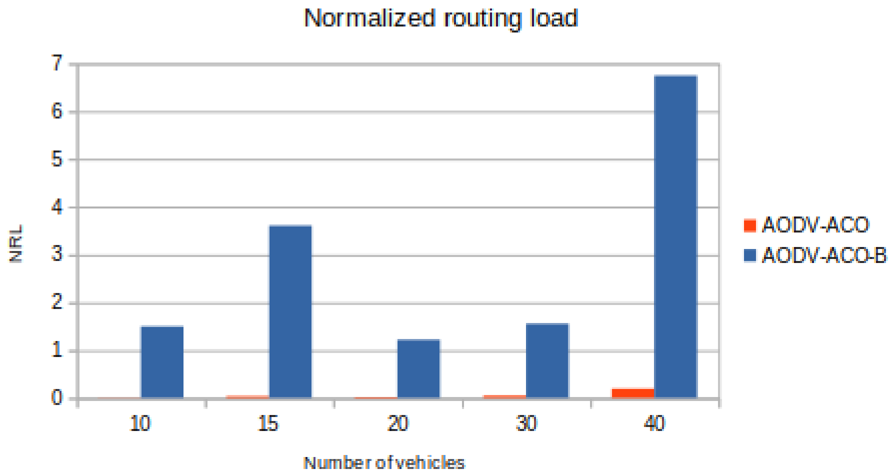

Figure 3. Normalized routing load

Fig.3 and table 4 show a clear difference in performance in terms of normalized routing load (NRL) between the ACO-AODV protocol, under normal conditions, and ACO-AODV-B, exposed to a Blackhole attack. In the case of ACO-AODV, the routing load remains low and stable, reflecting efficient use of control packets and optimized route management. On the other hand, in the presence of a malicious node, the ACO-AODV-B version registers a significant increase in NRL. The presence of a blackhole node disrupts route stability, forcing nodes to frequently initiate new path discoveries. This considerably increases the volume of control traffic compared with the data packets effectively delivered.

IV. CONCLUSION

In this study, we evaluated the impact of blackhole attacks on the performance of the ACO-AODV protocol, an improved version of the AODV protocol incorporating a bio-inspired ant colony optimization (ACO) approach. Through a series of simulations in an urban VANET environment, we compared the protocol under normal conditions (ACO-AODV) and in the presence of a malicious node (ACO-AODV-B). The results clearly show that the blackhole attack severely degrades protocol performance, causing a significant drop in packet delivery rate (PDR), an increase in transmission delay, as well as significant routing overhead (NRL). These findings underline the vulnerability of VANET networks to this type of attack, and highlight the need to integrate detection and prevention mechanisms. The addition of a detection module based on sequence number tracking could make the ACO-AODV protocol even more robust to internal threats.

REFERENCES

[1] Kumar, A., Varadarajan, V., Kumar, A., Dadheech,. P., Choudhary, S., S., Ambeth Kumar, V.D. Panigrah, B.K, & Veluvolu g, K. C. (2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. Microprocessors and Microsystems, 80, 103352.
[2] Prabhakar Reddy, B., Bhaskar Reddy, B. & Dhananjaya, B. (2021), The AODV routing protocol with built-in security to counter blackhole attack in MANET. Materials Today: Proceedings, https://doi.org/10.1016/j.matpr.2021.08.039
[3] Bensaid, C., Boukli Hacene, S., & Faraoun, K. M. (2016). Detection and Ignoring of Blackhole Attack in Vanets Networks. International Journal of Cloud Applications and Computing, 6.
[4] Tan, N. D., Van Tan, L. (2020). Implementation of black hole attack on aodv routing protocols in manet using ns2. UTEHY Journal of Science and Technology, 25, 45–51.
[5] Toutouh, J., Alba, E. (2011). An efficient routing protocol for green communications in vehicular ad-hoc networks. In Proc, the 13th annual conference companion on Genetic and evolutionary computation, 719-726.
[6] Malaga city downtown scenario .http://neo.lcc.uma.es/staff/jamal/VANET/?q=node/11
[7] Issariyakul, T., Hossain, E. (2011). Introduction to network simulator NS2, Springer.