

Evaluation of Wormhole Attacks using Network Performance Metrics on AODV Routing Protocol in VANET

Mariyam Mohamad, Ahmad Yusri Dak*
College of Computing, Informatics and Mathematics,
University of MARA Technology, Perlis Branch
*Email: ahmadyusri@uitm.edu.my

Keywords: VANET, AODV, Wormhole.

1. Introduction

This research aims to explore and simulate network layer attacks in Vehicular Ad-Hoc Networks (VANETs) using comprehensive network performance metrics. The primary research objectives are to analyse the impacts of these attacks on bandwidth, goodput, response time, and packet loss rate within the VANET framework. The novelty of this research lies in its focus on evaluating the resilience of VANETs against wormhole attacks, which exploit routing protocols like Ad Hoc On-Demand Distance Vector (AODV) (Al-Ahwal & Mahmoud, 2023) and pose significant threats to communication integrity and vehicle safety. By conducting simulations and measuring their effects, this research aims to provide valuable insights into enhancing the security and reliability of future autonomous vehicular networks.

2. Methodology

This research employs the Ad Hoc On-Demand Distance Vector (AODV) routing protocol within the NS-2 simulator to simulate network layer attacks in Vehicular Ad-Hoc Networks (VANET) (Mahdi et al., 2021). The simulations are conducted over a period of 10 seconds within a simulation area of 1000 meters x 1000 meters, involving varying numbers of mobile nodes (10, 20, 30, 40, 50). Utilizing the Random Way Point mobility model, each node moves randomly throughout the simulation area. Performance is evaluated using metrics such as bandwidth,

goodput, packet loss rate, and response time to assess the impact of wormhole attacks on VANET communication integrity and efficiency.

3. Results & Discussion

In VANET using the AODV protocol, response times initially increased with network size up to 20 nodes in normal conditions, suggesting potential congestion, but decreased beyond 20 nodes, indicating enhanced communication efficiency. Conversely, during a wormhole attack, response times spiked for smaller networks but decreased for larger ones, highlighting adaptive behaviors. Bandwidth performance showed an initial peak at 10 nodes, followed by significant drops at 20 nodes, and varying trends with further increases, indicating congestion issues. Under wormhole attacks, bandwidth generally improved, particularly in larger networks, potentially due to more efficient routing paths mitigating congestion. Goodput fluctuated with network size under normal conditions, peaking at 40 nodes and dropping at 50 nodes, while increasing overall under wormhole attacks, especially in larger networks, implying enhanced routing efficiency amid security risks. Packet loss rates were minimal up to 40 nodes without attacks but increased at 50 nodes; under wormhole attacks, they consistently rose, particularly in smaller networks, underscoring vulnerability and the need for robust security measures.

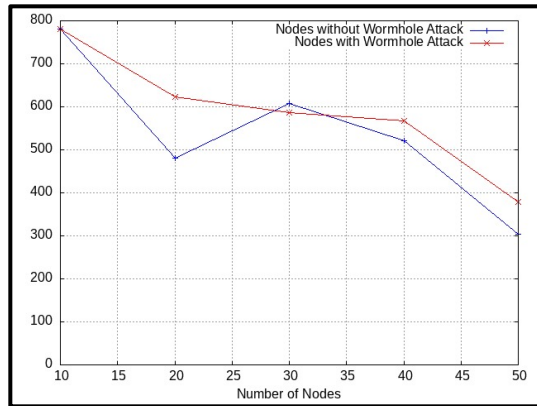


Figure 1. Number of nodes vs Bandwidth

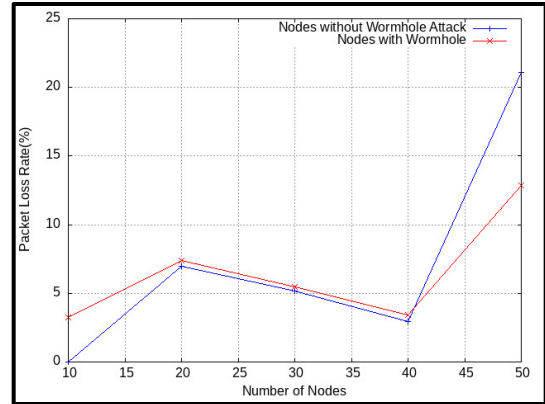


Figure 2. Number of nodes vs Packet Loss Rate

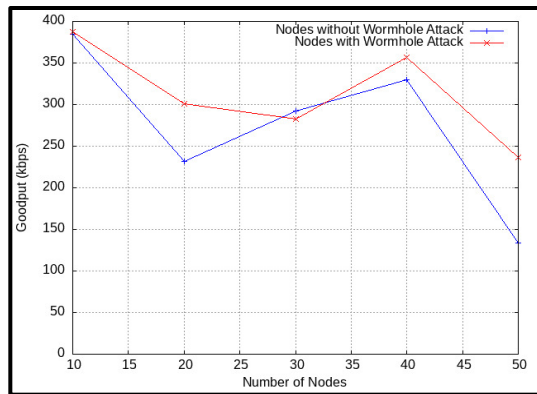


Figure 2. Number of nodes vs Goodput

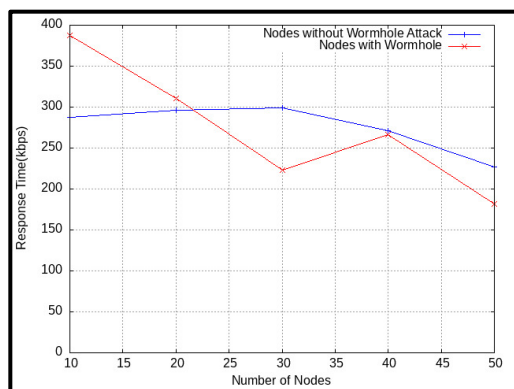


Figure 2. Number of nodes vs Response Time

4. Conclusion (max 50 words)

This research underscores the significant impact of wormhole attacks on the AODV routing protocol in VANET, highlighting response time as the most sensitive metric. Future studies should expand on network parameters and employ machine learning for enhanced detection, aiming to develop adaptive routing protocols for robust network security.

References (max 6 references, APA 7th)

- Al-Ahwal, A., & Mahmoud, R. A. (2023). Performance Evaluation and Discrimination of AODV and AOMDV VANET Routing Protocols Based on RRSE Technique. *Wireless Personal Communications*, 128(1), 321–344. <https://doi.org/10.1007/s11277-022-09957-8>
- Mahdi, H. F., Abood, M. S., & Hamdi, M. M. (2021). Performance evaluation for vehicular ad-hoc networks based routing protocols. *Bulletin of Electrical Engineering and Informatics*, 10(2), 1080–1091. <https://doi.org/10.11591/EEI.V10I2.2943>