Analysis of Blackhole Attack using Network Performance Metrics on AODV Routing Protocol in VANET

Siti Nurulaina Mazlan, Ahmad Yusri Dak*
College of Computing, Informatics and Mathematics,
Universiti Teknologi MARA, Perlis Branch
*Email: ahmadyusri@uitm.edu.my

Keywords: Blackhole; AODV; VANET

1. Introduction

Wireless technology, including VANET, is widely used today for vehicle-to-vehicle communication to prevent road accidents. This study uses the Ad Hoc On-Demand Distance Vector (AODV) routing protocol to investigate network layer attacks in VANET. The research involves simulating blackhole attack and evaluating network performance metrics such as bandwidth, response time, packet loss rate, goodput, and energy efficiency. Various node configurations are tested under normal and blackhole attack conditions.

A network layer attack is an attempt to gain unauthorized access to an organization's network, steal data, or perform other malicious activity. This can lead to problems with inaccurate routing decisions, potentially causing accidents and worsening traffic problems (Fiade et al., 2020).

2. Methodology

The simulation is conducted using the Random Waypoint (RWP) mobility model with diverse numbers of nodes 10, 20, 30, 40, and 50. The simulation involves transmitting data traffic using the AODV routing protocol without and with blackhole attack. The performance metrics are analyzed to evaluate the RWP model's effectiveness in the AODV routing protocol. The results of this simulation scenario are recorded.

3. Results & Discussion

Based on the result obtained, the critical importance of network security measures in mitigating the disruptive effects of malicious like blackhole attack. Efficient detection and mitigation strategies are essential to maintain optimal network performance and ensure reliable data transmission across varying network conditions and node densities. Future research should focus on enhancing the resilience of routing protocols against such attacks to bolster network security and performance under challenging operational environments. The efficiency of the routing protocol in handling increased nodes and mitigating the effects of a blackhole attack can influence the parameters.

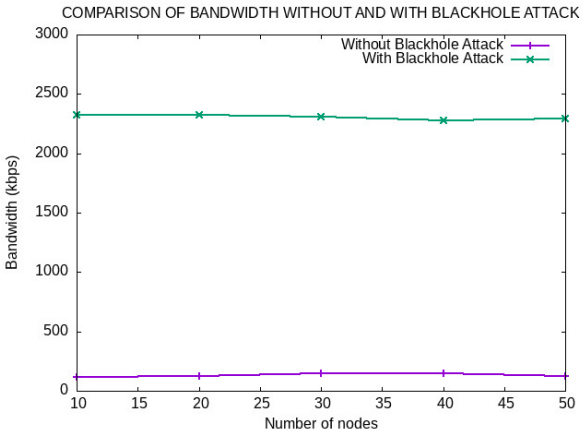

Figure 1. Graph comparison of bandwidth without and with blackhole attack

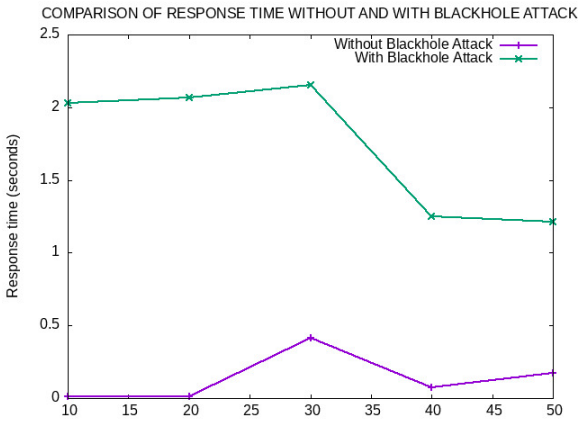

Figure 2. Graph comparison of response time without and with blackhole attack

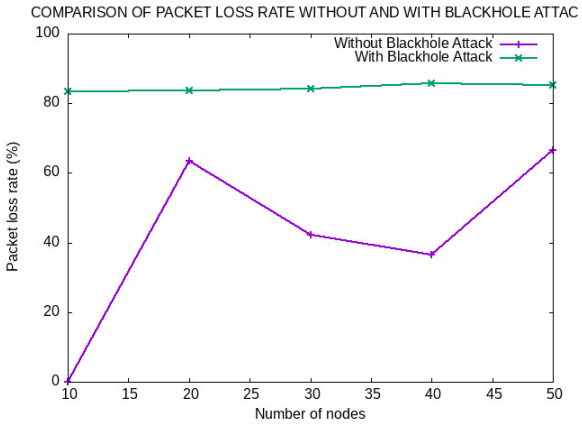

Figure 3. Graph comparison of packet loss rate without and with blackhole attack

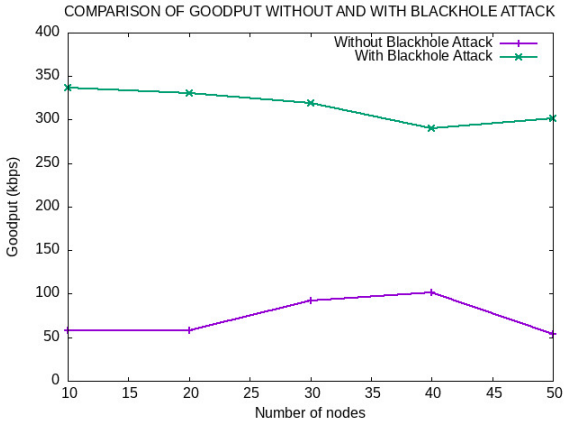

Figure 4. Graph comparison of goodput without and with blackhole attack

4. Conclusion

This project successfully meets its objectives, it was found that the presence of a blackhole attack significantly degrades network performance. The analysis reveals that the AODV routing protocol can maintain acceptable performance in networks without blackhole attack but suffers considerable performance loss when blackhole attack are introduced.

References

Adam, T., (2024, 9 February). *Can electric cars be hacked more easily than other cars?*. Drive. https://www.drive.com.au/caradvice/can-electric-cars-be-hacked-more-easily-than-other-cars/

Deepali, V., Ankita, S., Nikhil, B. (2021). Reliability Analysis to overcome Black Hole Attack in Wireless Sensor Network. *ArXiv*. https://arxiv.org/pdf/1401.2540

Margaret, R. (2022, April 10). *Ad Hoc On-Demand Distance Vector*. Techopedia. https://www.techopedia.com/definition/2922/ad-hoc-on-demand-distance-vector-aodv

Datta, R., & Marchang, N. (2012). Security for mobile ad hoc networks. In S. K. Das, K. Kant, & N. Zhang (Eds.), *Handbook on securing cyber-physical critical infrastructure* (pp. 147-190). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-415815-3.00007-8

Issariyakul, T., & Hossain, E. (2012). Introduction to network simulator 2 (NS2). In *Introduction to network simulator NS2*. Springer. https://doi.org/10.1007/978-1-4614-1406-3_2