Research Exhibition in Mathematics and Computer Sciences (REMACS 6.0)/
ISBN: 978-629-97440-5-4

DETECTION OF BLACKHOLE ATTACK USING AODV ROUTING PROTOCOL IN VANET

Arinah Sumayyah Zulkifli, Ahmad Yusri Dak and Hafizah Hajimia
College of Computing, Informatics and Mathematics,
Universiti Teknologi MARA, Perlis Branch
arinahzulkifli@gmail.com, ahmadyusri@uitm.edu.my and hafizah.hajimia@gmail.com

ABSTRACT - Vehicular ad-hoc network (VANET) is widely used in applications like highway automation, traffic management, and intelligent transportation systems due to its advantages over traditional communication systems. VANET enhances road safety by transmitting vehicle data to the Roadside Unit (RSU). However, VANET's decentralized architecture requires robust security measures to protect against attacks. Thus, this project is carried out to investigate and simulate a Blackhole attack using the Ad-hoc On-Demand Distance Vector (AODV) routing protocol in VANET and evaluate its impact using performance metrics. The metrics used are End-to-End Delay (EED), Packet Delivery Ratio (PDR), and throughput, simulated in NS-2. Two scenarios are examined: one compares performance with and without a Blackhole attack, while the other compares AODV and Destination Sequenced Distance Vector (DSDV) routing protocols. Results show that the Blackhole attack significantly affects the VANET environment, causing a delay of 175.05 ms with increasing nodes. By studying these aspects, improved security measures and protocols can be developed to safeguard VANET and ensure the reliability and safety of intelligent transportation systems.

Keywords: VANET, AODV, Blackhole attack

1. INTRODUCTION

The popularity of wireless connectivity has enabled the development of numerous internet-based apps and services, improving the quality of life. VANET is employed in various applications, such as traffic management and intelligent transportation systems, offering advantages like scalability and up-to-date information exchange. However, VANET is vulnerable to security threats like the Blackhole attack, which can cause data interruptions and manipulation. To protect against these attacks, suitable security measures and the AODV routing protocol are crucial. This project aims to investigate and simulate the Blackhole attack using the AODV routing protocol in VANET and evaluate its impact using performance metrics. The simulation will be conducted using Network Simulator (NS-2) version 2.35. Two scenarios will be simulated without and with the Blackhole attack, and performance metrics such as EED, PDR, and throughput will be measured. This project's significance lies in enhancing VANET security, understanding defenses against the Blackhole attack, and developing improved safety methods and protocols for intelligent transportation systems.

2. METHODOLOGY

The method includes data collection, planning, design, simulation, performance evaluation, and documentation. 20, 30, 40, 50, and 60 nodes are simulated within a 1000 x 1000 meter network area. Two scenarios are simulated: The first scenario compares network performance between without and with a Blackhole attack, while the second scenario compares the AODV and DSDV routing protocols. Experiments are conducted in each scenario to evaluate EED, PDR, and throughput. The simulation process comprises setting up the environment, configuring nodes and protocols, executing TCL scripts, analyzing network behavior, generating trace files and NAM visualizations, and evaluating performance metrics with AWK scripts. NS-2 and BonnMotion are helpful instruments for understanding VANET networks and researching the detection of Blackhole attacks. Microsoft Word is used for project documentation, facilitating accurate record-keeping and future reference. Overall, the methodology and simulation process contribute to a thorough evaluation of the behavior of VANET networks and the efficacy of detection mechanisms in the presence of Blackhole attacks.

3. RESULTS AND DISCUSSION

In a VANET, the presence of Blackhole attacks significantly degrades network performance. In the absence of Blackhole attacks, EED ranges from 8.65 ms to 63.08 ms. The PDR is also severely impacted, falling from 36.43 % to 10.01 % with the Blackhole attacks compared to a range of 36.43 % to 99.78 % without them. With Blackhole attacks, throughput ranges between 6.84 Kbps and 29.37 Kbps, whereas it ranges between 29.37 Kbps and 51.19 Kbps without. AODV consistently outperforms DSDV in terms of latency, PDR, and throughput. These results demonstrate the detrimental effect of Blackhole attacks on VANET performance and the efficacy of the AODV routing protocol in mitigating such attacks.

4. NOVELTY OF RESEARCH / PRODUCT

This study offers new insights into Blackhole attacks in VANETs and proposes a secure AODV routing algorithm to detect and mitigate these attacks (Kumar et al., 2021). By synthesizing existing knowledge and conducting an in-depth analysis, the research provides a comprehensive overview of the field (Bamhdi, 2020) and identifies research gaps. Incorporating performance metrics and simulation tools adds novelty to the methodology (Oberoi, 2020). In contrast, the research's practical implications contribute to developing more reliable and secure VANET systems (Fatemidokht & Kuchaki, 2020). This study makes a significant and novel contribution to VANETs and network security.

5. CONCLUSION

In conclusion, this project successfully investigated Blackhole attacks in VANET utilizing the AODV routing protocol. The evaluation of performance metrics revealed a substantial effect on network throughput, emphasizing the need for comprehensive security measures. Future research can concentrate on advancing detection techniques and bolstering VANET's resistance to Blackhole attacks.

REFERENCES

Bamhdi, A. M. (2020). Efficient dynamic-power AODV routing protocol based on node density. Computer Standards and Interfaces, 70. https://doi.org/10.1016/j.csi.2019.103406

Fatemidokht, H., & Kuchaki Rafsanjani, M. (2020). QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks. Journal of Systems and Software, 165. https://doi.org/10.1016/j.jss.2020.110561

Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. D. A., Panigrahi, B. K., & Veluvolu, K. C. (2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. Microprocessors and Microsystems, 80. https://doi.org/10.1016/j.micpro.2020.103352

Oberoi, V. (2020). Enhancement of QoS in Security Algorithm for Blackhole Attack in VANET. 2020 IEEE Pune Section International Conference, PuneCon 2020, 33–37. https://doi.org/10.1109/PuneCon50868.2020.9362444