UNIVERSITI TEKNOLOGI MARA

PERFORMANCE EVALUATION OF AODV USING BLACKHOLE ATTACK IN MANET

MUHAMMAD IDHAM BIN PADIL

BACHELOR OF COMPUTER SCIENCE (HONS.) DATA COMMUNICATION AND NETWORKING

AUGUST 2022

Universiti Teknologi MARA

Performance Evaluation of AODV Using Blackhole Attack in MANET

Muhammad Idham bin Padil

Thesis submitted in fulfilment of the requirements for Bachelor of Computer Science (Hons) Data Communication and Networking Faculty of Computer and Mathematical Science

August 2021

PERFORMANCE EVALUATION OF AODV USING BLACKHOLE ATTACK IN MANET

By

MUHAMMAD IDHAM BIN PADIL

2019406088

This thesis was prepared under the supervision of the project supervisor, Dr. Ahmad Yusri bin Dak. It was submitted to the Faculty of Computer and Mathematical Sciences and was accepted in partial fulfilment of the requirements for the degree of Bachelor of Computer Science (Hons) Data Communication and Networking.

Approved by

Dr. Ahmad Yusri bin Dak

Project Supervisor

JULY 14, 2022

STUDENT DECLARATION

I certify that this thesis and the project to which it refers is the product of my own work and that any idea or quotation from the work of other people, published or otherwise are fully acknowledged in accordance with the standard referring practices of the discipline.

MUHAMMAD IDHAM BIN PADIL

2019406088

JULY 14, 2022

ABSTRACT

MANET are self-contained, multi-hop, wireless, transitory networks that operate under throughput, power, and energy constraints. Mobile wireless networks are more prone to attacks than fixed wireless networks. These networks are vulnerable to security due to unprotected and open wireless broadcast channels and inadequate physical security. Blackhole attacks are active attacks in which the attacking node continuously declares that it has the quickest route to any desired network node, although it does not. Consequently, all packets will travel through it, enabling the blackhole node to forward or delete packets during data transfer. As most studies examine reactive, proactive, or hybrid routing protocols, such as AODV and DSDV or AODV and ZRP, there is also a lack of study comparing AODV with different nodes and simulation time. This research simulates and compares the performance of the AODV routing protocol with and without a blackhole attack. Moreover, the throughput, packet delivery ratio, and end-to-end delay of AODV and AODV with blackhole are compared to evaluate their respective performance. Using Network Simulator 2 (NS2), two scenarios with varying numbers of nodes beginning at 10, 20, 30, 40, and 50 are simulated for a total of 60 seconds. With a lower throughput of 60.82 Kbps, a poorer packet delivery ratio of 16.27%, and a more significant end-to-end delay of 1531.36 milliseconds, the results show that AODV with blackhole attack performs worse than without blackhole attack for all performance criteria. This project also could be enhanced for future work by examining or suggesting other network and transport layer security techniques used to prevent these attacks.