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

DETECTION OF WORMHOLE ATTACKS USING AODV ROUTING PROTOCOL IN VANET

Muhammad Khairul Fahmi Jasmi and Ahmad Yusri Dak
College of Computing, Informatics and Mathematics,
Universiti Teknologi MARA, Perlis Branch
2020847152@student.uitm.edu.my and ahmadyusri@uitm.edu.my

ABSTRACT - VANET (Vehicular Ad-Hoc Network) is a sort of wireless communication network intended exclusively for intelligent cars to interact and create a dynamic network that supports a variety of applications and services. The growing popularity of autonomous vehicles makes VANET vulnerable to cyber-attacks. The attacker could intercept, edit, inject, and control traffic messages used to direct road vehicles. They also allow for the modification of messages and the spread of misleading road information, resulting in traffic congestion and road risks. Therefore, the objective is to investigate and simulate wormhole attacks using AODV routing protocol. Furthermore, network performance parameters such as Packet Delivery Ratio, Throughput, and End to End Delay are simulated under two different scenarios using the NS2 simulation tool. The simulation parameter covers 1000 x 1000 meters geographical area, with an increasing number of nodes. The results reveal that Packet Delivery Ratio (PDR) provides a significant detection rate of Wormhole attacks with an average of 92.52% when compared to Throughput and End to End Delay as the number of cars that represent congestion level increases. Wormhole attacks, as a result, constitute a substantial danger to network security and can negatively impair network performance and operation. Wormhole attacks, in general, highlight the significance of maintaining robust network security and raising awareness about potential vulnerabilities.

Keywords: VANET, routing protocol, AODV, NS2

1. INTRODUCTION

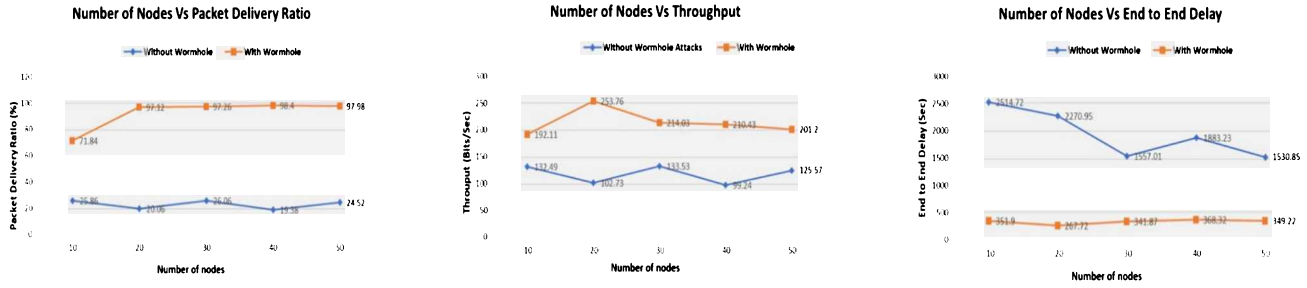
VANET stands for Vehicular Ad-Hoc Network. It is a type of wireless communication network specifically designed for vehicles on the move. VANETs enable vehicles to communicate with each other and with roadside infrastructure, creating a dynamic network that supports various applications and services. A vehicle network differs from a mobile ad hoc network in that a vehicular network node is free to join and exit the network at any time. The aim of this research is to investigate and simulate wormhole attacks using AODV routing protocol in a VANET environment by using NS2, a network simulator tool and then compare the results of the performance test under two different scenarios that reflects the real-time implementation of the protocol in VANET. The scope of this research focused on the performance of AODV routing protocol with the presence and absence of wormhole attacks in the VANET environment.

2. METHODOLOGY

There are six phases in total of making this project successful which are information gathering, planning, design and development, experimentation and simulation, data collection and analysis, and documentation. The method that was used to carry out this research is a simulation model that represents an ad-hoc network with AODV routing protocol implementation approach and the presence and absence of wormhole attackers. The simulation model is presented in the form of a network topology that consists of beacon frames to represent VANET vehicles. There is one source node, one destination node and two malicious nodes that represent wormhole attacks are wirelessly linked together in order to simulate wireless communication in VANET environments. The whole simulation of this project is carried out under two different simulation scenarios which are increasing the number of nodes and simulation time. The results obtained from the simulation are then analyzed to understand the behavior of wormhole attacks in the network.

3. RESULTS AND DISCUSSION

Based on the results and analysis of the simulations in NS2, as the number of nodes and simulation time increases, network performance in terms of average Packet Delivery Ratio (PDR) shows a significant rate of Wormhole attacks with 92.52%. Besides that, the average Throughput also increases as the number of nodes increases but then continues to decrease after a certain number of nodes. However, End to End Delay remains lower even though the number of nodes increases. To conclude, results of the performance analysis indicate that Wormhole attacks pose a significant threat to network security and can have a huge impact on network performance and functionality.



4. NOVELTY OF RESEARCH / PRODUCT

Throughout the years, there have been several studies that conducted performance analysis on detecting Wormhole attacks using NS-2, measuring the PDR, Throughput and EED as the number of nodes increases, such as (Kumar et al., 2019). There is also previous research on Blackhole Attacks and the performance between secure AODV algorithm and existing AODV routing protocol that measures the performance of the protocol in terms of PDR, Throughput and EED rate using NS-2 as the number of nodes increases (Kumar et al., 2021). Other than that, there is also research that analyzed the performance of different protocols which are TCP and UDP in the VANET environment in terms of PDR and packet loss with number of nodes varied (Khalid et al., 2022). Finally, research by (Saini et al., 2018) conducted performance analysis on presence of wormhole attacks, measuring PDR, Throughput and EED under the scenario of increasing simulation time.

5. CONCLUSION

As a conclusion, wormhole attacks constitute a substantial danger to network security and can negatively impair network performance and operation. Wormhole attacks, in general, highlight the significance of maintaining robust network security and raising awareness about potential vulnerabilities.

REFERENCES

Khalid, A. A., Shuhaimi, N. I., Mohamad, R., Abdullah, E., Norsyafizan, W., & Muhamad, W. (2022). *The Implication of Different Transmission Protocols for Vehicular Networks Using NS-2*. http://TuEngr.com

Kumar, A., Galety, M. G., Nuru, M., & Adam, T. (2019). WCBAODV: An efficacious approach to detect wormhole attack in VANET using CBAODV algorithm. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(1), 20–25. https://doi.org/10.30534/ijatcse/2019/0481.22019

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

Saini, P. K., Kumar Verma, P., & Sohal, J. S. (2018). DAPS for detecting Wormhole Attacks in IEEE 802.11 networks using Ad hoc On-demand Distance Vector routing protocol. *International Journal of Research in Advent Technology*, *6*(4). www.ijrat.org