Open Access Research Journal of
Engineering and Technology
Journals home page: https://oarjpublication/journals/oarjet/
ISSN: 2783-0128 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(REVIEW ARTICLE)

Black-hole and DoS attack detection analysis and isolation mechanism for black-hole in MANET

Hothefa Shaker Jassim [1], Rahil Khamis AL Majizi [1], Zeyad Tariq Sharef [2, *] and Seemaa Abbas Jawdat [2]

[1] Modern College of Business and Science, Department of Graduate Studies, Muscat, Sultanate of Oman.
[2] Ninevah University, College of Electronics Engineering, Mosul, Iraq.

Open Access Research Journal of Engineering and Technology, 2024, 07(01), 001–013

Publication history: Received on 30 April 2024; revised on 25 June 2024; accepted on 28 June 2024

Article DOI: https://doi.org/10.53022/oarjet.2024.7.1.0026

Abstract

A mobile ad-hoc network is a network without infrastructure where communication between nodes occurs in an open medium, such as the air. This makes it susceptible to eavesdropping and various attacks, which can be categorized as data traffic attacks (such as black-hole, grey-hole, DoS, etc.) and control traffic attacks (such as worm-hole, hello flood, man-in-the-middle, etc.). This NS2 experimental simulation compares the disruption effects of black-hole and DoS attacks in an identical network using the AODV routing protocol. The simulation aims to observe and analyze parameters such as packet delivery fraction, end-to-end delay, normalized overhead, and residual energy in HKI-Reader. Additionally, it demonstrates how malicious nodes are detected, removed, or isolated from the network to restore it to its original state. HKI-Reader is a software application developed using PHP and JavaScript. It is designed to read simulation results files for attacks and display them in a graphical user interface (GUI) for improved analysis and visual observation.

Keywords: Black-hole attack; DoS attack; MANET; NS2

1. Introduction

MANET, also known as Mobile Ad-hoc Network, operates independently without relying on any infrastructure or base station to establish, control, and secure communication. It is a cellular network in which all the nodes are connected wirelessly and may be modified while in motion [2]. Therefore, it is susceptible to attacks because of its inherent qualities. In addition to those above, "open medium, distributed nodes, the autonomy of nodes participation in the network, lack of centralized authority which can enforce security on the network and distributed coordination and cooperation are the reasons behind the inability to use the existing protocols [5]. Therefore, many protocols have been devised in MANET [16].

Ad-Hoc On-Demand Distance Vector Routing protocol is a famous and widely used protocol in MANET. AODV belongs to the reactive taxonomy of MANET routing protocols, and it's developed as an improvement to the sequenced Distance Vector routing algorithm [9][7]. As a result, AODV uses a simple request-reply mechanism to discover routes [17]. The transmission primarily relies on three packets from the source to the destination. The routing request (RREQ) establishes a packet's path from the source to the destination. Once the route is established, the destination sends a route reply (RREP) to the source. If no path to the destination or the link in the valid path breaks, an intermediate node or the destination sends a route error (RERR) message [6][18].

Attacks in MANET vary from data traffic attacks to control traffic attacks, and one of the most famous data traffic attacks is a black-hole attack. A Black-hole is a malicious node that publicizes its routing protocol as the short path to the destination node with a publicizing of fresh routes regardless of checking its routing table, which attracts the source node to send the packet towards it and, as a consequence, all the received packets will be dropped causes disruption in

[*] Corresponding author: Zeyad Sharef

the network and disconnecting the communication between the source and destination [8]. In contrast, a DoS attack is when the malicious node keeps sending packets, trying to consume as much bandwidth as possible to obstruct network availability [3].

The structure of this paper is as follows: In the first section, titled "Related work," the paper explores the ongoing research on Ad-Hoc networks, including the associated protocols and attacks. The second section, "Methodology," explains the specific mechanism and process used to achieve the paper's objectives based on a series of simulations. The third section, "Results and Analysis," presents the results of these simulations and provides an analysis based on these results. Section four will serve as the concluding part of the paper [21] [23].

2. Related work

A lot of research has been conducted in MANET for several reasons. One of the most important reasons is the very challenging routing protocols used in MANET compared to well-known protocols in a traditional network, whether it’s wired or wireless, and that’s due to the MANET fundamental structure [1][3][13]. These protocols are classified into specific categories, and each category has particular features and drawbacks. The figure below shows the classification of MANET protocols [2]:

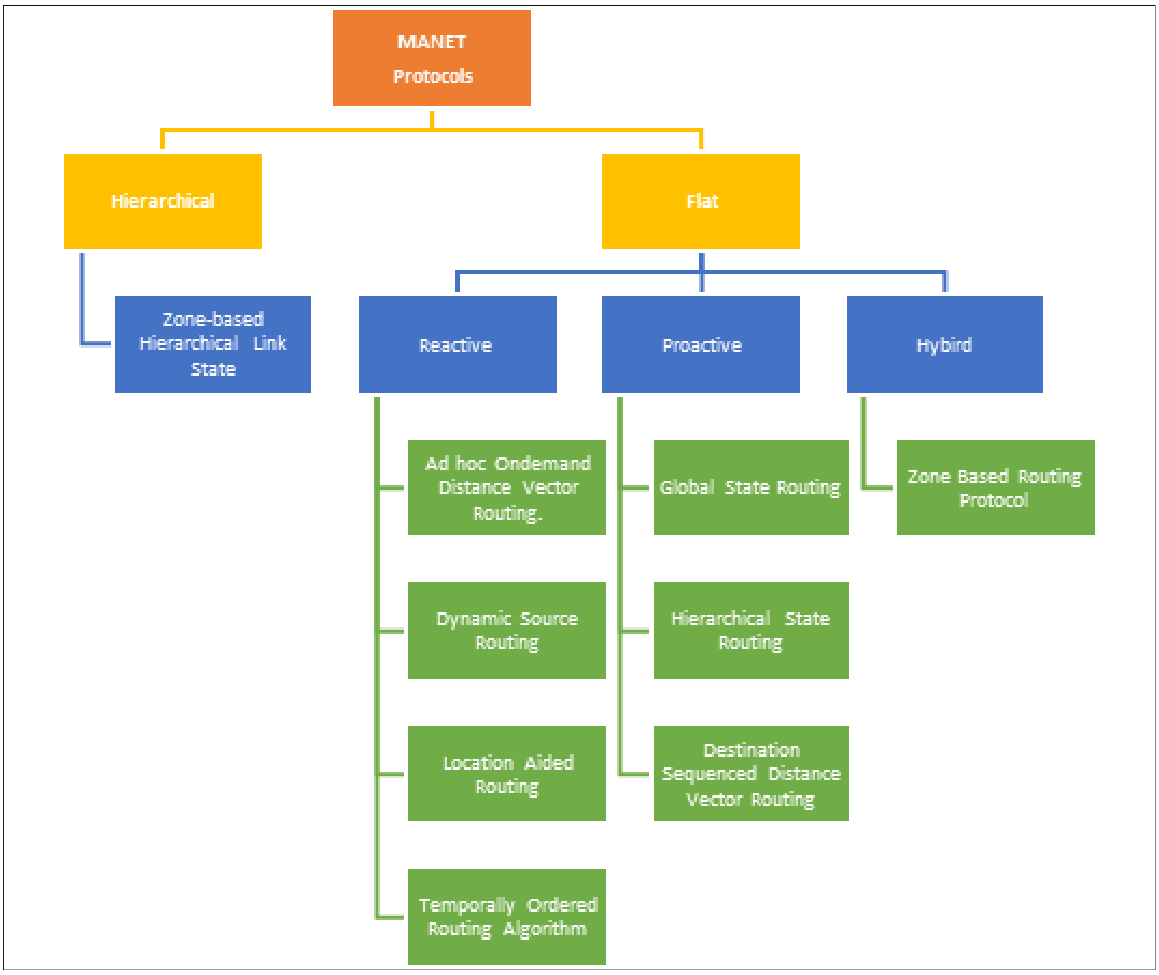

MANET Protocols
Hierarchical
Flat
Zone-based Hierarchical Link State
Reactive
Proactive
Hybird
Ad hoc Ondemand Distance Vector Routing.
Dynamic Source Routing
Location Aided Routing
Temporally Ordered Routing Algorithm
Global State Routing
Hierarchical State Routing
Destination Sequenced Distance Vector Routing
Zone Based Routing Protocol

Figure 1 Routing Protocol in MANET

The subcategories underneath the flat class are the most widely used protocols in MANET where proactive, known as table-driven routing protocols make the mobile node maintain a separate routing table or topology information which contains the information of the routes to all the possible destination mobile nodes, which is updated periodically since the movement nature of the topology [1][24]. Therefore, it doesn’t work well for large networks as the entries in the routing table become too large since they need to maintain the route information to all possible nodes, which also consumes high energy levels of the nodes [11]. Still, the delay time in small or medium networks is minimal since all the nodes are always up to date. In contrast, reactive, known as on-demand routing protocol, the route is discovered only when it is required/needed [4]. Route discovery occurs by flooding the route request packets throughout the mobile network [14][25]. It consists of two major phases: route discovery and route maintenance. Unlike proactive routing protocols, reactive routing protocols consume less bandwidth and energy, but the delay time in small or medium networks is a bit greater than that of proactive protocols. In contrast, in large networks, reactive performs much better [15]. Hybrid routing protocol combines the advantages of both reactive and proactive routing protocols. These protocols are adaptive and adapt according to the source and destination mobile node's zone and position. These protocols are susceptible to attacks due to the communication mechanism and the structure of the MANET [23].

In traditional networks, attacks are categorized into two types: Active attacks refer to situations where the targeted network is penetrated, resulting in a breach of its integrity or availability. Examples of such assaults include run-somewhere attacks, data wiping, and DDoS attacks [19]. A passive assault is an attack that does not immediately hurt or impact the victims. It involves breaching confidentiality through identifying and scanning activity, traffic analysis, reading logs, spying, or eavesdropping. The primary distinction between active and passive assaults is in the actions taken by the attacker. In active attacks, the attacker intercepts the connection and alters the information. In contrast, in passive attacks, the attacker intercepts the transmitted information solely to read and analyze it without making any modifications [10].

3. Methodology

To successfully execute the simulation and achieve the experiment's objective (identify the attack behavior, detect the malicious node, and isolate the malicious node), modification of AODV.cc and AODV.h is a must. Modifying these files makes the NS2 compatible with the (.tcl) file in which all the declaration of the nodes, type of nodes (malicious or not), connection type, node movements, etc [12]. Exist. Moreover, the old trace file output of the simulation will exclude the energy level consumption [22]. To include it, one line of code is added in the (.tcl) file to inform the simulation that the results wanted to be in a new form. Hence, the energy model can be added to the (.tcl) file as well; the final step is to put in place the necessary formulas for energy calculation along with other parameters calculations (PDF, Delay, overhead, etc.) in the (.awk) file. It is worth noting that once the trace file is changed from old to new, it will cause a significant alteration in the (.tr) file where all the results of the simulation exist; therefore, it’s a must to change the column values in (.awk) file otherwise it will be a mess in term of data integrity upon each parameter [20].

In this experiment, ten scenarios (five for each attack) have been successfully conducted, and the number of malicious nodes in both attacks is identical in sequence (non-malicious, 1, 3, 5, and 8). Moreover, the simulation was performed in a similar network (15 nodes in size of 750*750), and the traffic type used was CBR. The only difference is the (.tcl) file configuration, which harmonizes with the two attacks conducted.

For both attacks, the performance properties or metrics used to compare two attacks:

The performance metrics used are	
1	No of Packets Send
2	No of Packets Received
3	Packets Delivery Ratio
4	Control Overhead
5	Normalized Routing Overheads
6	Delay
7	Throughput
8	Dropping Ratio
9	No of Packets Dropped
10	Total Energy Consumption
11	Average Energy Consumption
12	Overall Residual Energy
13	Average Residual Energy

The subsequent figures depict an instance illustrating the simulation steps in NAM of a single malicious node in a black-hole attack, elucidating the sequence and mechanism of the attack.

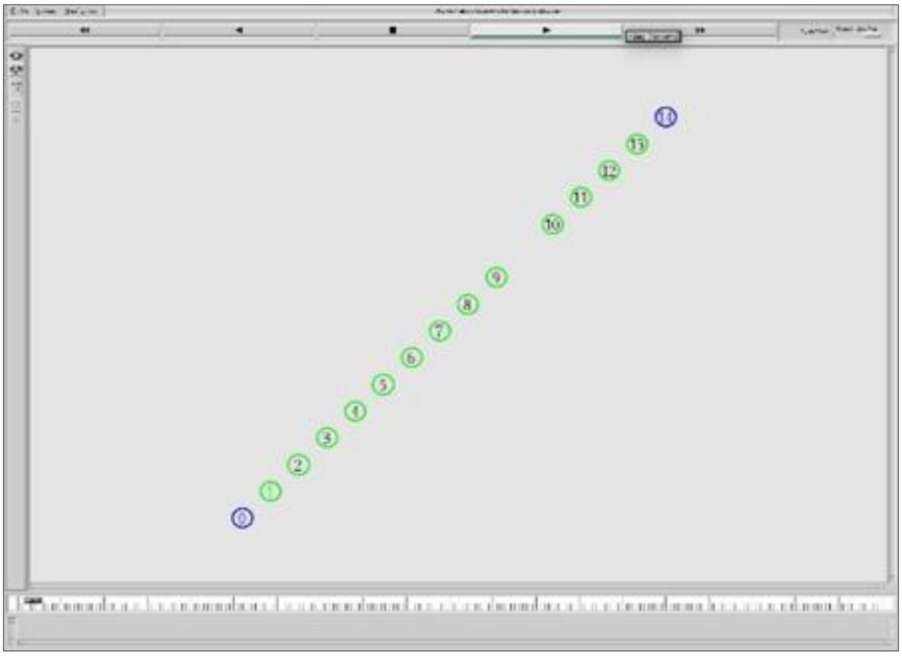


Figure 2 Start | Nodes are distributed in the network area

The third figure clarifies the communication between nodes, from node 0 to node 14, using CBR traffic.

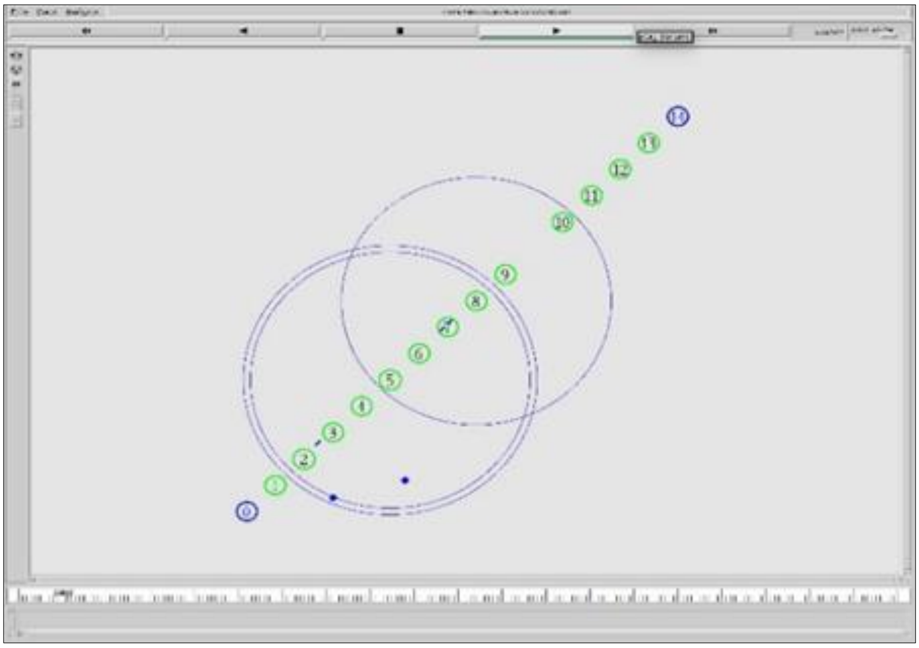


Figure 3 Node communication

Then, if the node is malicious and drops many packets, it is detected as a black hole and isolated, as shown in Figures 4 &5.

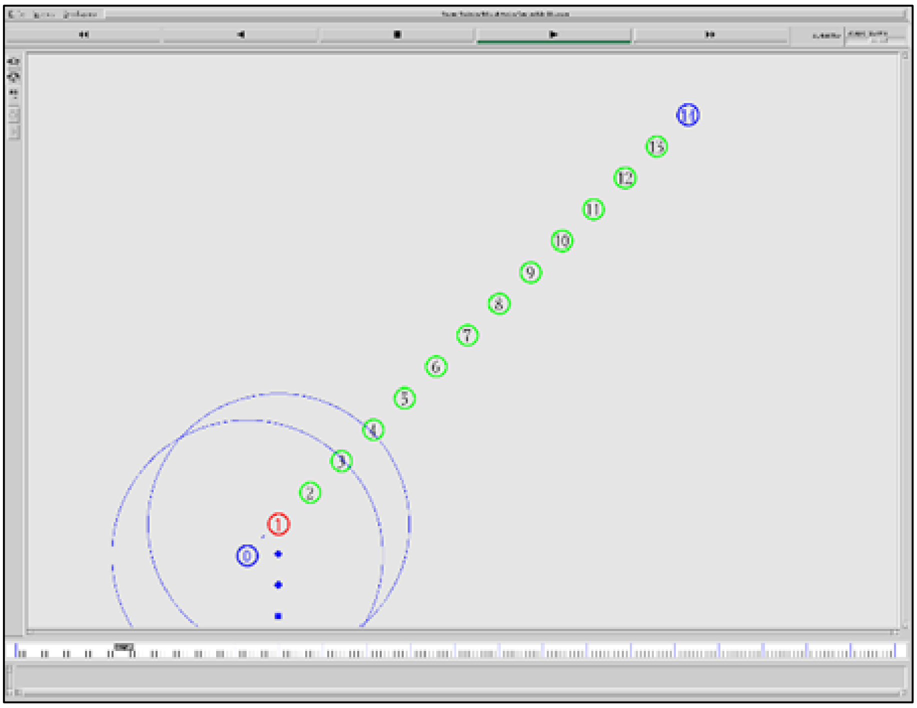


Figure 4 Detect black hole node with dropping packets.

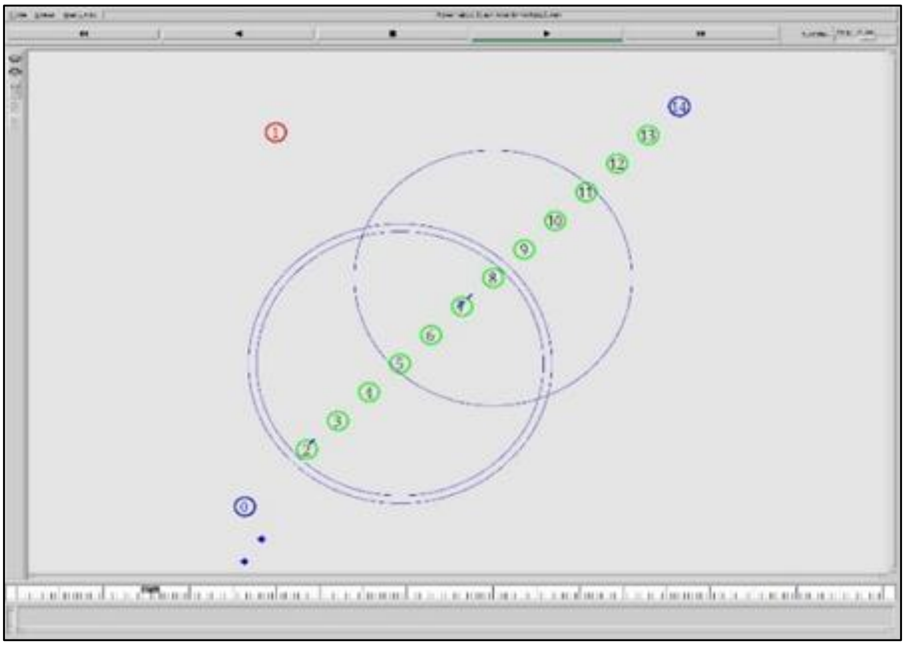


Figure 5 Isolation of black hole node

After the Black Hole is isolated, the network returns to its normal state, and communication is established with all nodes, as depicted in the accompanying figure.

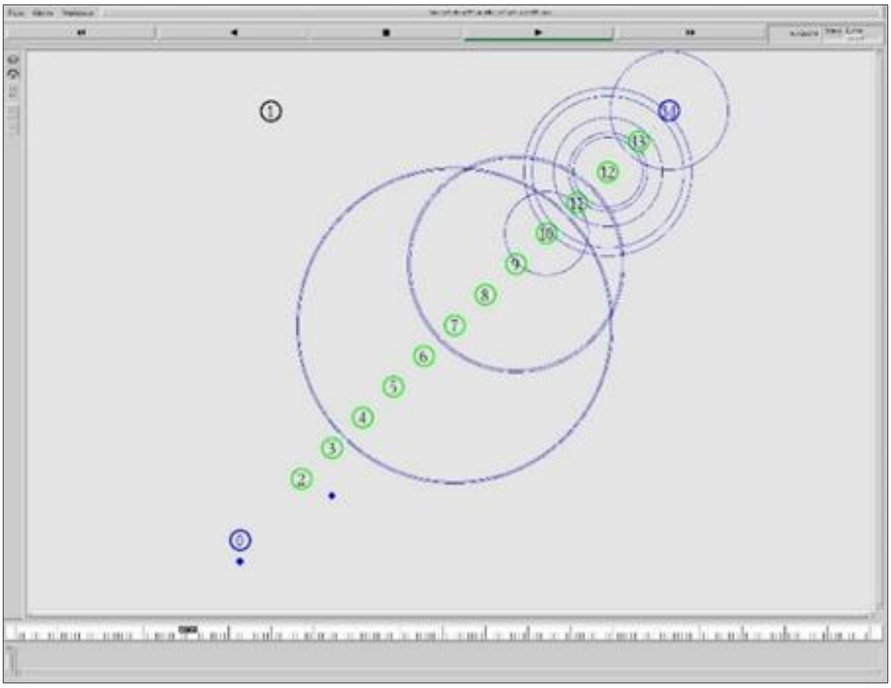


Figure 6 The communication back to normal after the isolation

In the following figure, an example will illustrate three malicious nodes engaging in a DoS attack, demonstrating the transmission of numerous packets from these nodes to disrupt the network.

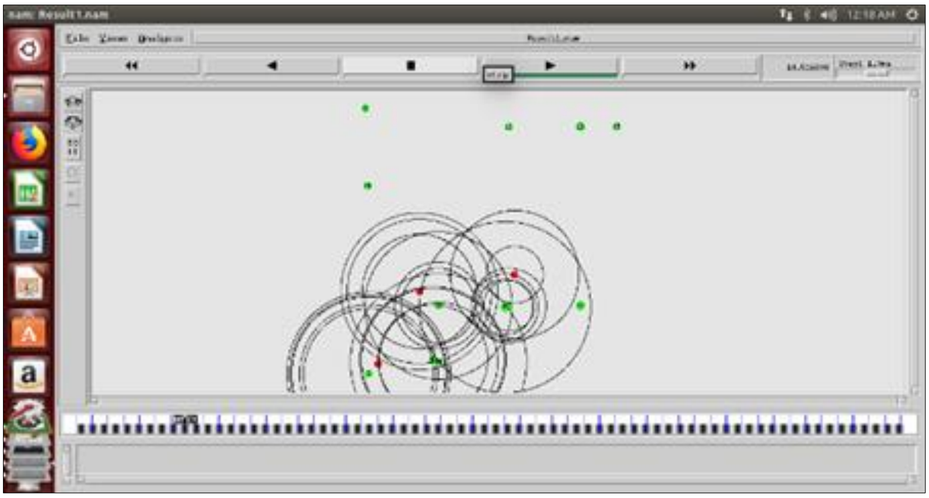


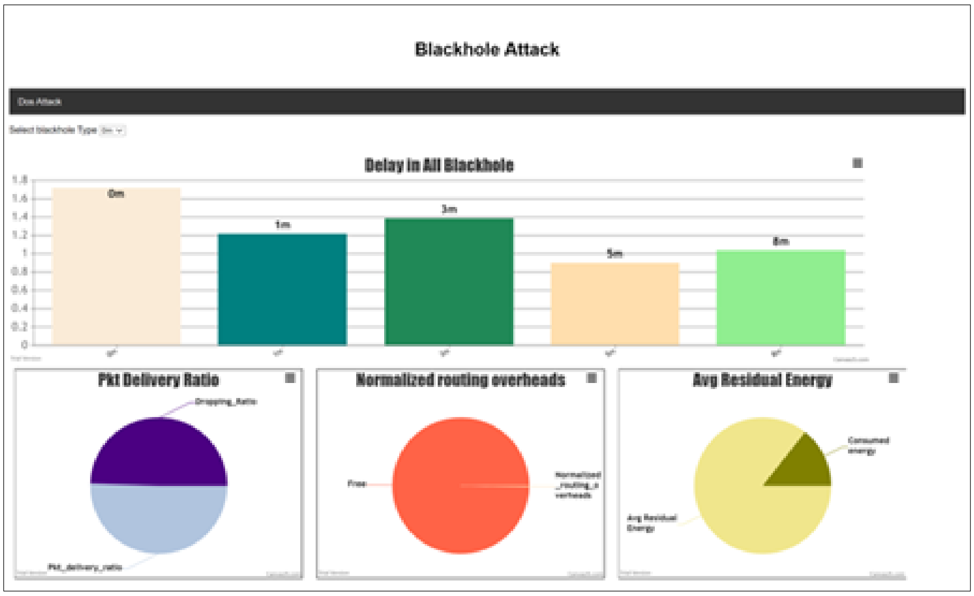
Figure 7 Three malicious nodes disrupting the network by the extra volume of the sent

4. Results and analysis

The HKI-Reader is a graphical user interface (GUI) tool designed to facilitate the analysis and interpretation of simulation outcomes related to network attacks, such as Black Hole and Denial of Service (DoS) attacks. Moreover, it provides a clear visualization of the simulation results, allowing users to quickly understand and interpret the behavior of the network during these attacks. The HKI-Reader enhances the efficiency of analyzing simulation data, enabling researchers to gain valuable insights into the impact and characteristics of various network attacks.

The ***HKI-Reader*** has to part the upper part to show the delays for all malicious, and the bottom part shows the PDF, routing overheads, and the average residual energy for each number of malicious selected from the down menu.

The coming figures depict the analysis results for transitioning from a non-malicious to an attack involving eight malicious nodes forming a black hole. Figure 8 illustrates no malicious node in the black-hole simulation. In the context of a black-hole simulation, the term "No malicious node" refers to a scenario where no node within the network is identified as malicious. When the HKI-Reader indicates "No malicious node," it means that during the simulation, none of the nodes in the network exhibited behavior indicative of participating in a black-hole attack. Where the dropping and PKT delivery ratio is equal.

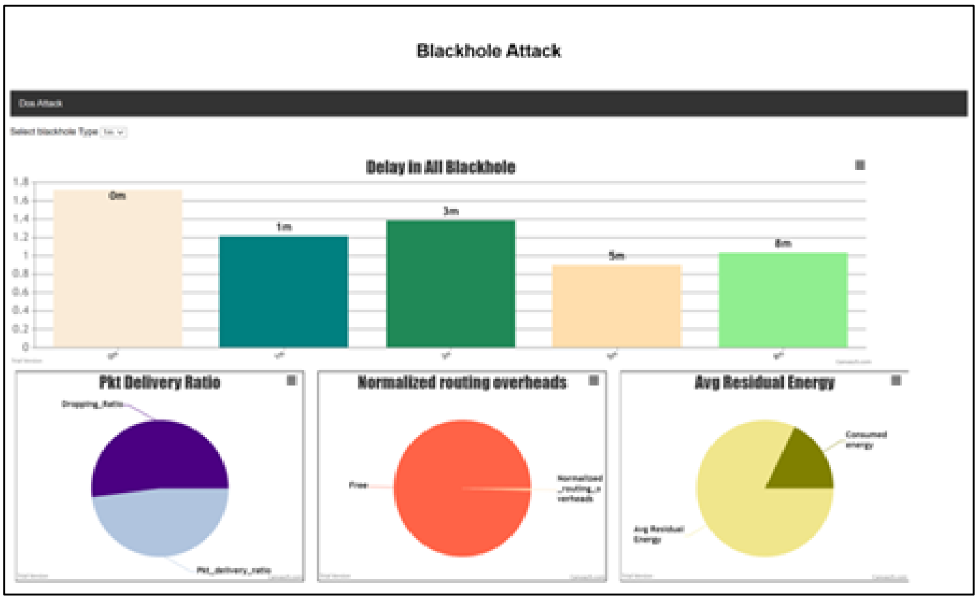

Blackhole Attack

Dos Attack

Select blackhole Type 0m

Figure 8 No malicious node in the black-hole simulation

Figure 9 identifies a single node within the network as malicious. When the HKI-Reader indicates "one malicious node," it means that during the simulation, one specific node in the network exhibited behavior consistent with participating in a black-hole attack. The dropping ratio slightly increased compared with the PKT. A decrease in the PKT delivery ratio may indicate the impact of these attacks on the network's performance, resulting in packet loss or disruption of communication between nodes.


Blackhole Attack

Dos Attack

Select blackhole Type 1m

Figure 9 One malicious node in the black-hole simulation

The scenario of the three malicious nodes refers to where three nodes within the network are identified as malicious, as shown in Figure 10. Furthermore, when it indicates "three malicious nodes," three nodes within the network were identified as exhibiting behavior characteristic of malicious activity associated with a black-hole attack—a quarter of the overall PKT delivery ratio.

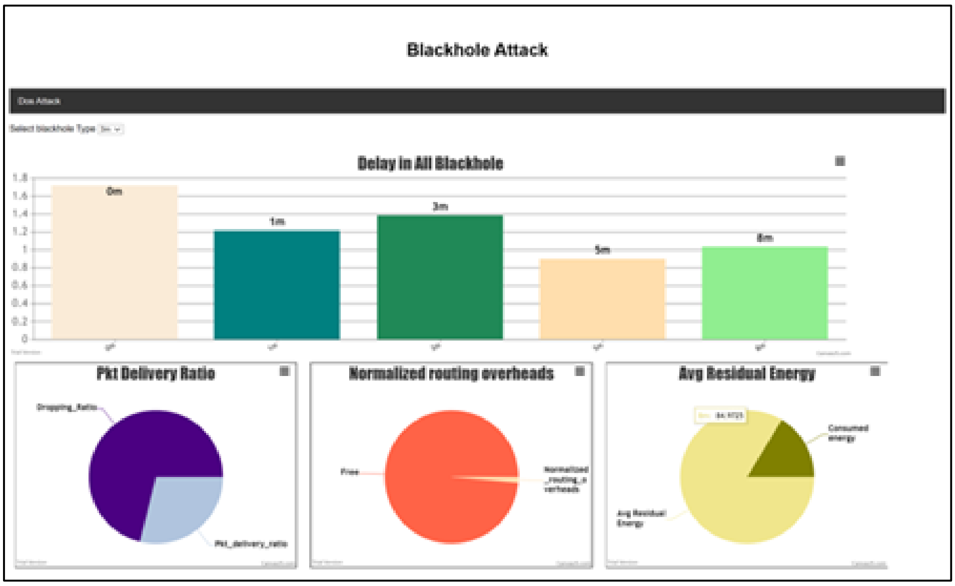


Figure 10 Three malicious nodes in black-hole simulation

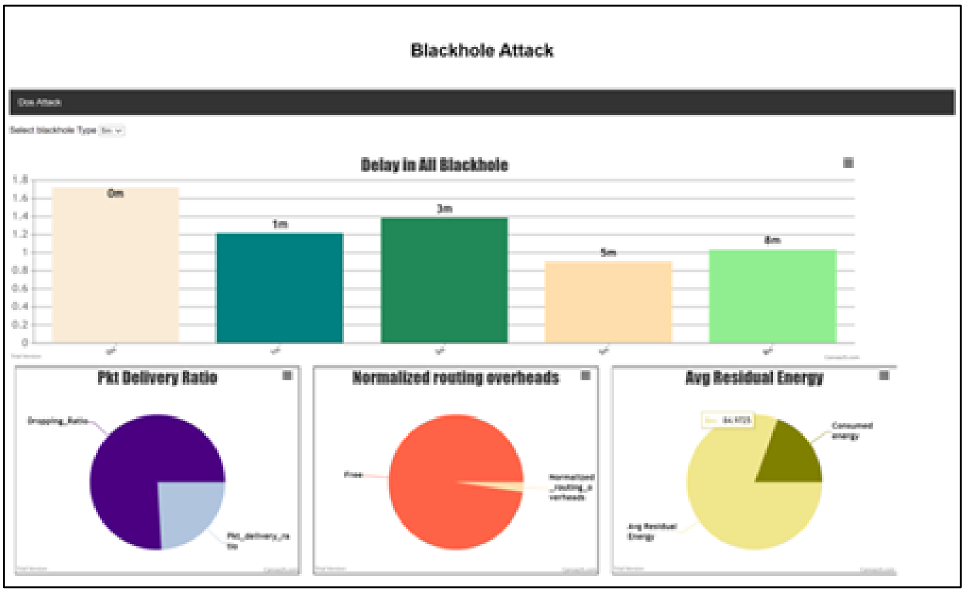


Figure 11 Five malicious nodes in black-hole simulation

The presence of "five malicious nodes" indicates that five nodes within the network displayed behavior consistent with a black hole attack. Less than a quarter illustrates the PKT delivery ratio.

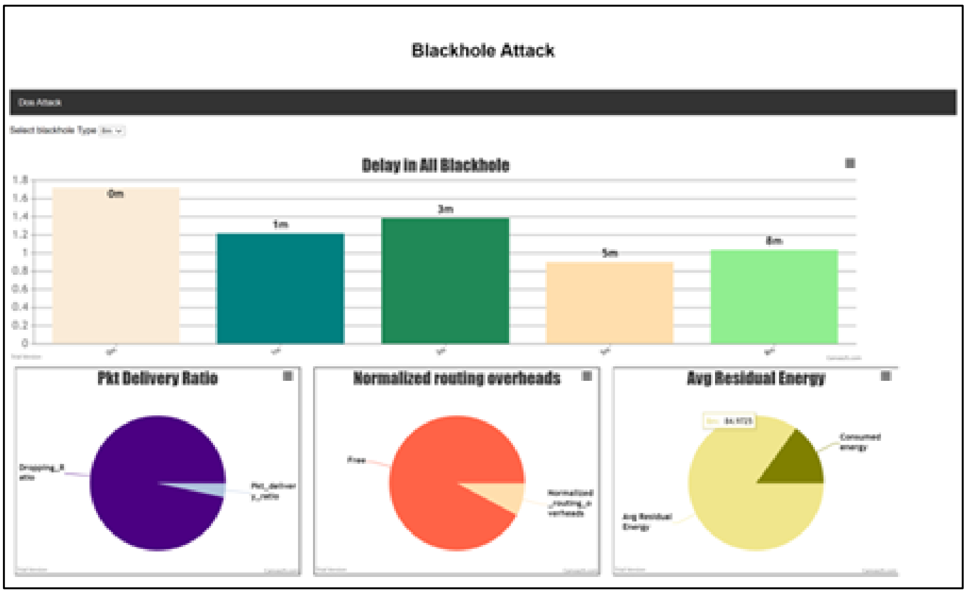


Figure 12 Eight malicious nodes in black-hole simulation

The following figures depict the analysis result for DoS attacks from zero to 8 malicious DoS node attacks.

In the DoS simulation with zero malicious nodes, the HKI-Reader provides insights into the network behavior without deliberate attacks. Figure 13 illustrates zero malicious nodes in the DoS simulation. The drop in PKT delivery ratio appears to decrease sharply and remains similar to other scenarios.

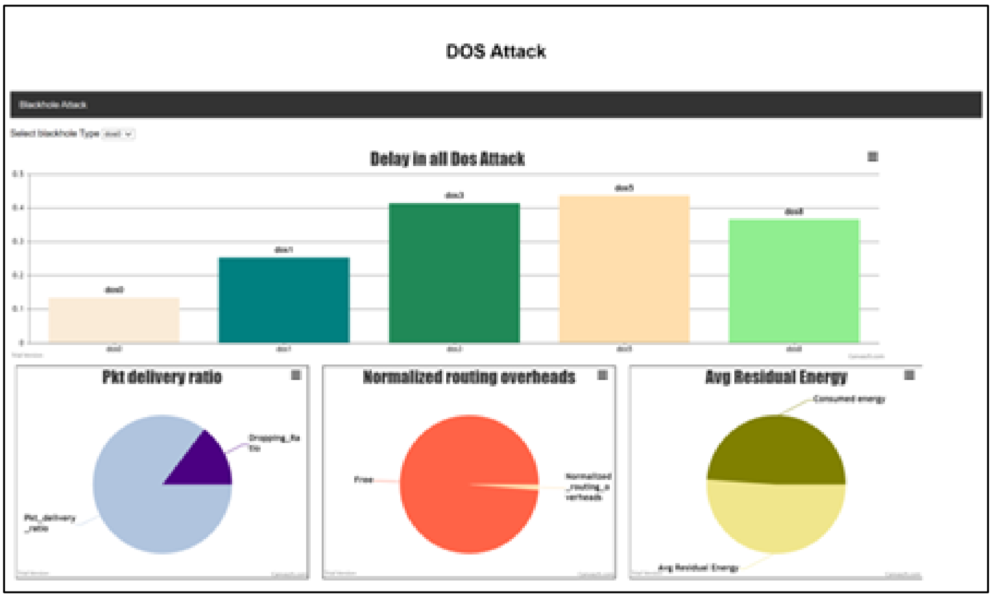


Figure 13 Zero malicious nodes in DoS simulation

In the DoS simulation with one malicious node, the HKI-Reader analyzes various parameters, including packet delivery ratio (PKT delivery ratio) and other network performance metrics, by monitoring the impact of a single malicious node on packet delivery and network behavior Figure 14.

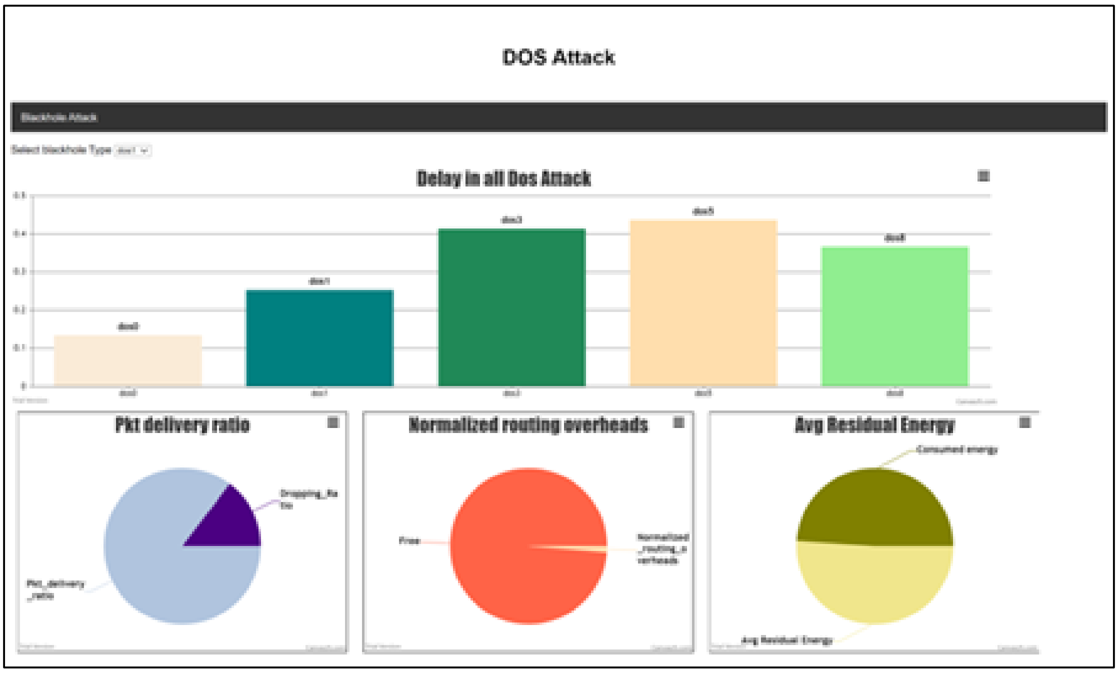


Figure 14 One malicious node in the DoS simulation

Similarly to Figure 15, the presence of three malicious nodes introduces a higher level of disruption and congestion to the network compared to scenarios with fewer malicious nodes.

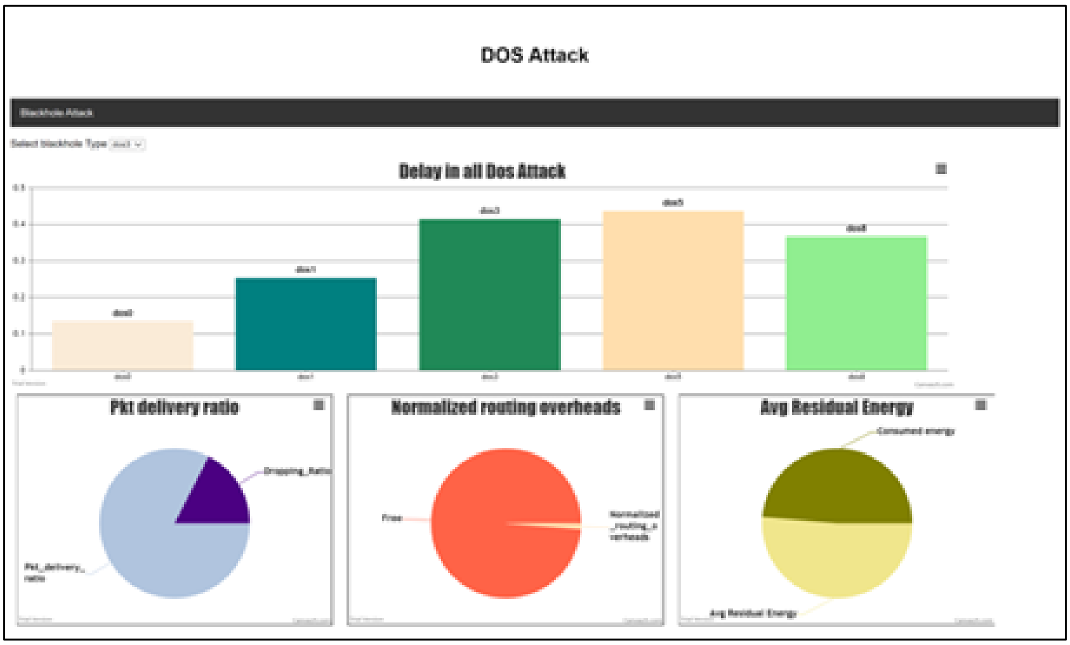


Figure 15 Three malicious nodes in the DoS simulation

In the DoS simulation analyzed using the HKI-Reader, the presence of five malicious nodes exacerbates network congestion and degradation, significantly impacting network performance. Additionally, the dropping ratio remains consistently low, indicating sustained network resilience against the heightened malicious activity, as illustrated in Figure 16.

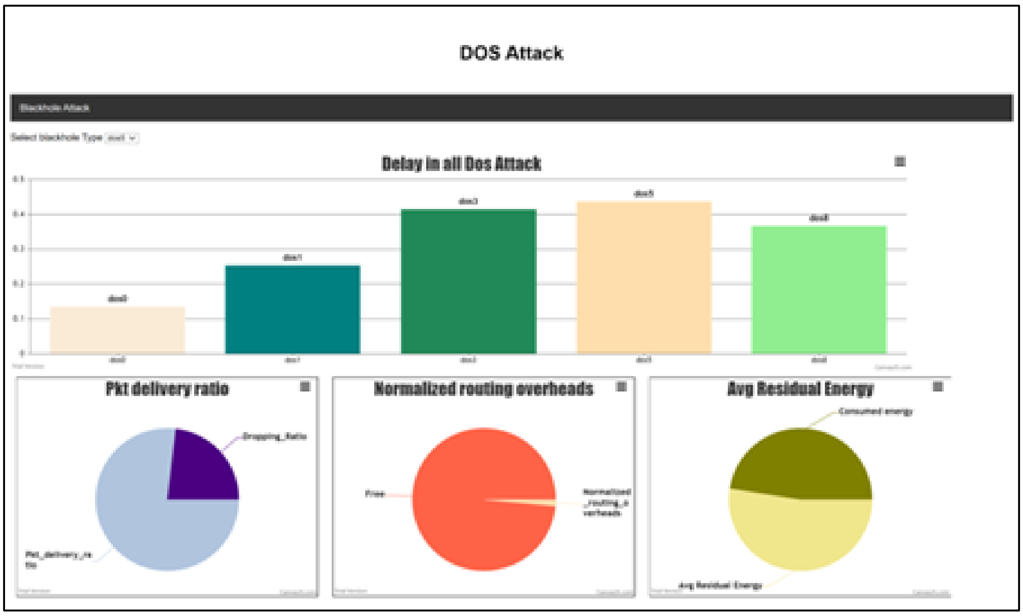


Figure 16 five malicious nodes in the DoS simulation

Finally, in Figure 17, despite the heightened malicious activity, the dropping ratio is consistently low, indicative of sustained network resilience against the increased onslaught of malicious nodes.

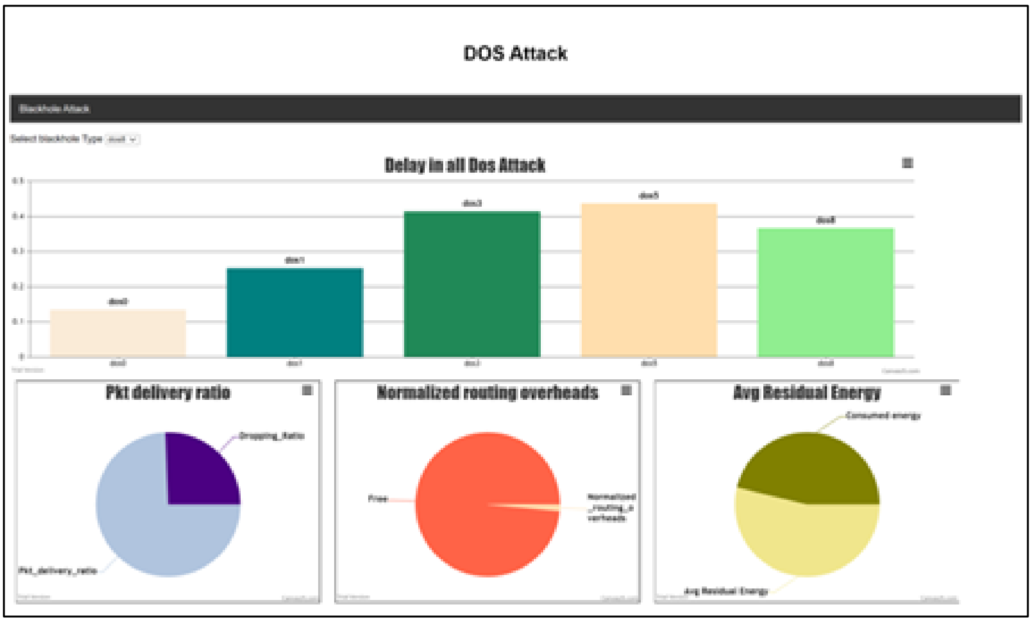


Figure 17 Eight malicious nodes in the DoS simulation

From the results figures mentioned, it's visually possible to determine the affection of the malicious nodes in each equivalent number of malicious in both attacks. As a result, a black-hole attack causes more disruption than Dos because it drops all the packets once the malicious node has received them. The black-hole attack causes more disruption than DoS because it drops all received packets, leading to a complete communication breakdown. Unlike DoS, which may target specific resources, the black-hole attack indiscriminately intercepts and discards all incoming packets, resulting in widespread service disruption and potential data loss. Its indiscriminate nature makes it challenging to detect and mitigate effectively, prolonging its impact and severity.

It's worth noting that the delay time in a black-whole attack is opposite from the expected because all the nodes involved in the network –passing the traffic – and after isolating the malicious nodes, the number of total nodes in the network decreased; therefore, it will be faster to reach to the destination (less time), unlike the DoS simulation where all nodes don't need to be involved in passing the traffic. In addition, the simulation couldn't isolate the malicious nodes due to the network size limitation in the eight malicious node simulations in black hole attacks.

5. Conclusion

In summary, the black-hole attack damages more frequently affect the network in this simulation even after the isolation of the malicious node because that malicious node drops all packets from the beginning once it attracts the source node as the shortest path until it is detected and isolated. In contrast, in a DoS attack, the nodes typically transfer the data until the malicious nodes send many packets that the network can no longer handle, forcing the network to shut down. Moreover, once it starts sending extra packets, it will also be detected and isolated. So, the stability and availability of the network in case of a DoS attack depends on the network strength and hardness. Meanwhile, the current configuration of the malicious node in the simulation has been set to a medium level of disruption, which means that the network can resist and handle a sufficient number of packets until it loses or drops them.

Some mitigation actions can be taken in case of a black-hole attack, like collecting multiple RREP messages (from more than two nodes) and thus hoping for numerous redundant paths to the destination node and then buffering the packets until a safe route is found and maintaining a table in each node with the previous sequence number in increasing order. Each node before forwarding packets increases the sequence number. The sender node broadcasts RREQ to its neighbors, and once this RREQ reaches the destination, it replies with an RREP with the last packet sequence number. If the intermediate node finds that RREP contains a wrong sequence number, it understands that somewhere, something went wrong. While in a Dos attack, one of the mitigation techniques is to turn off the IP and block a particular attacker node, another approach is by a technique that uses cryptographic puzzles in combination with game theory to force possible malicious nodes to execute many computations before they get access to the resources of another node.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Munas, Mohamed, and Kuruvikulam Chandrasekaran Arun. "Performance Evaluation of Distance Vector (RIP) and Link-State (OSPF) Routing Protocols." 2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS). IEEE, 2023.

[2] G.Vijaya Kumar, Y.Vasudeva Reddyr, Dr.M.Nagendr, "Current Research Work on Routing Protocols for MANET, 2010.

[3] Teeb H. Hadi, "MANET and WSN: WHAT MAKES THEM DIFFERENT?", 2017.

[4] Vivarekar, Jay, S. T. Sonnis, and D. A. Roy. "Time-Triggered Distance Vector Routing Protocol For Mobile Ad-hoc Networks." 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2021.

[5] Aniruddha Bhattacharyya, Arnab Banerjee and Dipayan Bose, "Different types of attacks in Mobile ADHOC Network Prevention and mitigation techniques", 2016

[6] L. A. Hassnawi, R.B Ahmad, Abid Yahya, S. A. Aljunid and M. Elshaikh, "Performance Analysis of Various Routing Protocols for Motorway Surveillance System Cameras Network", 2012.

[7] Sundari, K., and A. Senthil Thilak. "Impact of realistic mobility models on the performance of VANET routing protocols." 2023 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT). IEEE, 2023.

[8] Raghavendra, C. Sai, and N. Deepa. "An Intelligent Traffic Management System in Vehicle-to-NH Road (V2N) using Dynamic Optimal Random Access (DORA) protocol in Comparison with Dynamic Source Routing (DSRP) Protocol to Improve Packet Delivery Ratio." 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT). IEEE, 2023.

[9] Dr Umadevi Chezhiyan, "Measurement Based Analysis of Reactive Protocols in MANET", 2013

[10] Sharma, Manjita, and Varsha Agarwal. "Maximization Network Throughput by Efficient Geographic Routing Protocol for IoT based Sensor Network." 2023 IEEE 4th Annual Flagship India Council International Subsections Conference (INDISCON). IEEE, 2023.

[11] Er. Inakshi Garg and Er. Meenakshi Sharma, “DOS Attack Mitigation In MANET”, 2016.

[12] Antonis Michalas, Nikos Komninos and Neeli R. Prasad, “Mitigate DoS and DDoS attack in mobile ad hoc networks”, 2011.

[13] Wei Wei-Houbing Song-Huihui Wang-Xiumei Fan,” Research and Simulation of Queue Management Algorithms in Ad Hoc Networks Under DDoS Attack” IEEE Access, 13 March 2017.

[14] Bhavin Joshi - Nikhil Kumar Singh” Mitigating dynamic DoS attacks in mobile ad hoc network” IEEE Xplore, 19 September 2016.

[15] Changwang Zhang, Jianping Yin, Zhiping Cai, and Weifeng Chen "RRED: Robust RED Algorithm to Counter Low-Rate Denial-of-Service Attacks" IEEE COMMUNICATIONS LETTERS, MAY 2010.

[16] M Poongothai-M Sathyakala "Simulation and analysis of DDoS attacks"IEEE Xplore, 06 May 2013

[17] Mehta, Deepak, and Sharad Saxena. "A comparative analysis of energy-efficient hierarchical routing protocols for wireless sensor networks." 2018 4th International Conference on Computing Sciences (ICCS). IEEE, 2018.

[18] Pantazis, Nikolaos A., Stefanos A. Nikolidakis, and Dimitrios D. Vergados. "Energy-efficient routing protocols in wireless sensor networks: A survey." IEEE Communications surveys & tutorials 15.2 (2012): 551-591.

[19] NS Simulator for Beginners | By Eitan Altman, Tania Jiménez | [practical]

[20] ROUTING ISSUES IN MANETs | By B. V. V. S. PRASAD | Educreation Publishing, Jul 5, 2016

[21] Computer Network Simulation in Ns2: Basic Concepts and Protocols Implementation | By Neeraj Bhargava, Pramod Singh Rathore, Dr Ritu Bhargava , Abhishek Kumar | BPB Publications, Dec 24, 2019

[22] Treplan, Gergely, et al. "Reliable and energy aware routing protocols for wireless sensor networks." SoftCOM 2009-17th International Conference on Software, Telecommunications & Computer Networks. IEEE, 2009.

[23] Aggarwal, Nikhil, Neha Sharma, and Yogiraj Bhale. "Performance Analysis of Power Efficient Routing Protocols for Wireless Sensor Networks: A Survey." 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE, 2022.

[24] Purohit, Rajshree, and Navjot Sidhu. "Wireless sensor network: Routing protocols and attacks-a survey." 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2015.

[25] Sathish, M., et al. "Detection of single and collaborative black hole attack in MANET." 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). IEEE, 2016.