International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 13, Issue 01, January 2024)

Blackhole Attack Detection based on Modified On-Demand Multicast Routing Protocol with Neural Network Algorithm

Hemant Dhoot[1], Prof. Suresh S. Gawande[2]

[1]*Research Scholar,* [2]*Head of Department, Dept. of Electronics & Communication Eng., Bhabha Engineering Reasearch Institute, Bhopal, India*

***Abstract*—Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Wireless Sensor Networks (WSNs). Black hole attack is one of the security threat in which the traffic is redirected this type of node that honestly does no longer exist inside the network. This paper is proposed neural network (NN) for optimization and multicast routing protocol approach for attack detection and prevention. The measurements were taken in terms of throughput, end-to-end delay and network load.**

***Keywords*— Attack, NN, Routing, WSN, DOS, DDOS.**

I. INTRODUCTION

In recent years, wireless ad-hoc networks have become increasingly prevalent in various applications, ranging from military communications and disaster management to sensor networks and smart cities. However, the open and dynamic nature of these networks makes them susceptible to various security threats, with one of the most challenging being the Blackhole attack. A Blackhole attack involves a malicious node, known as the Blackhole node, which falsely advertises itself as having the optimal path to a destination, leading to the diversion and dropping of data packets.

To mitigate the risks associated with Blackhole attacks in ad-hoc networks, researchers have been actively exploring innovative solutions. One such solution involves the integration of a Modified On-Demand Multicast Routing Protocol (MODMRP) with a Neural Network (NN) algorithm for efficient and accurate Blackhole attack detection.

Ad-hoc networks are decentralized, self-organizing networks where nodes communicate with each other without relying on a centralized infrastructure. This flexibility makes them suitable for dynamic and temporary communication environments. Blackhole attacks in ad-hoc networks disrupt the normal flow of communication by attracting and dropping data packets, leading to potential information leakage, service denial, or degradation of network performance. Traditional routing protocols like AODV (Ad-hoc On-Demand Distance Vector) are vulnerable to Blackhole attacks due to their reliance on the shortest path without considering the trustworthiness of the nodes.

MODMRP is an enhancement to traditional on-demand multicast routing protocols. It integrates mechanisms for monitoring and evaluating the trustworthiness of nodes in the network, dynamically adjusting the multicast routes to avoid malicious nodes.

Neural Networks are computational models inspired by the human brain's structure, capable of learning complex patterns and making intelligent decisions. In the context of Blackhole attack detection, a Neural Network is trained to recognize patterns indicative of malicious behavior based on historical data. The integration of MODMRP with the Neural Network algorithm is expected to significantly enhance the security of ad-hoc networks by effectively detecting and mitigating Blackhole attacks. The combination of the Modified On-Demand Multicast Routing Protocol with a Neural Network algorithm offers a promising approach to strengthen the security of wireless ad-hoc networks against Blackhole attacks. This innovative solution aims to provide a robust defense mechanism by dynamically adapting to the evolving nature of network threats and ensuring the integrity and reliability of communication in challenging and dynamic environments.

II. PROPOSED METHODOLOGY

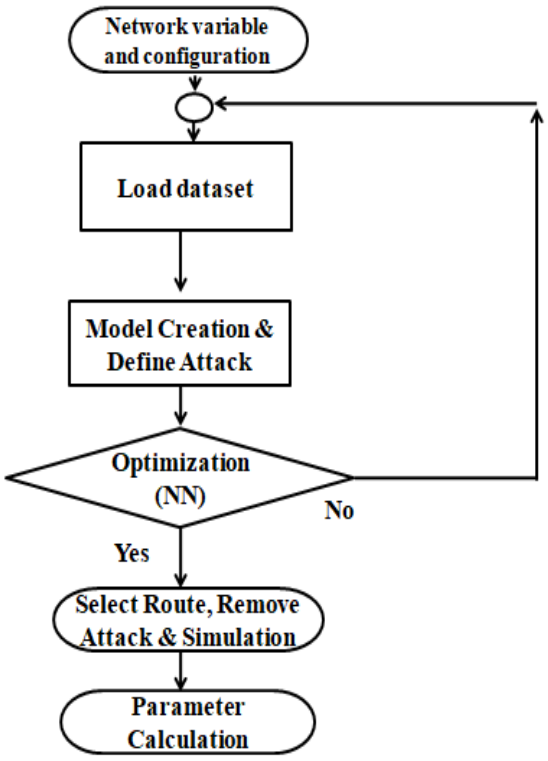

Figure 1: Flow Chart

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 13, Issue 01, January 2024)

Step-1: Reading configuration, runtime variables total packets generated in the simulation

Step-2: Load data set, MAC protocol, Agents used in this simulation

Step-3: Creation of network model and introduce 2 black-hole attack nodes

Step-4: Optimization of attack node using neural network methodology. Then due to high security such attacking node is identified and removed or stop.

Step-5: Select route using ODMRP protocol then update topology matrix, and update plot graph and simulation of nodes in environment.

Step-6: Various simulation parameters calculation

III. Simulation And Result

The usage of the proposed calculation is done over MATLAB. The ad-hoc network and communication commands and function such us to utilize the capacities accessible in MATLAB Library for different techniques like moving, scaling and so forth.

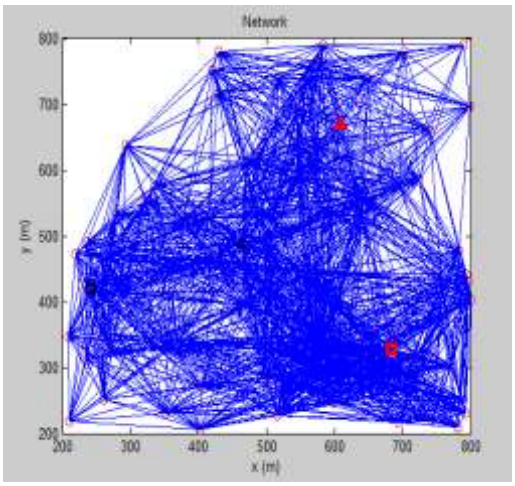

Figure 2: Network model creation and attack introduce

This figure shows the attack introduce, here node number 8 and node number 21 is assigned as a black hole attack node.

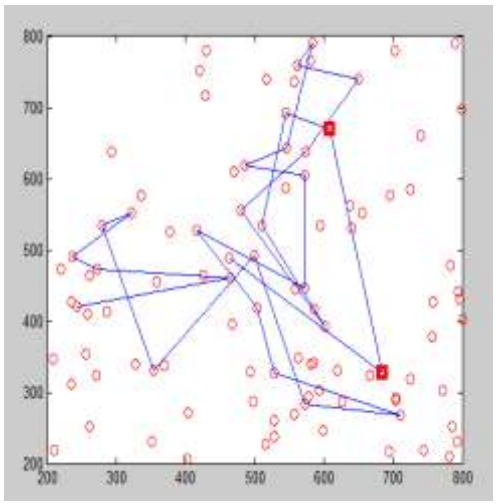

Figure 3: Network model simulation-I

This figure shows the simulation of various nodes with attack nodes. But attack node start identifying.

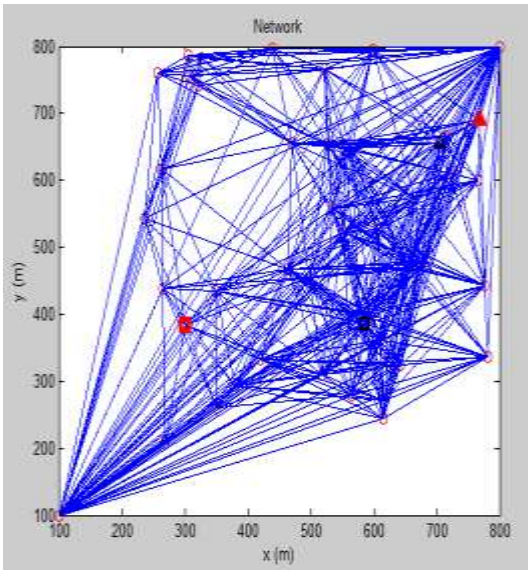

Figure 4: Attack node optimization-I

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 13, Issue 01, January 2024)

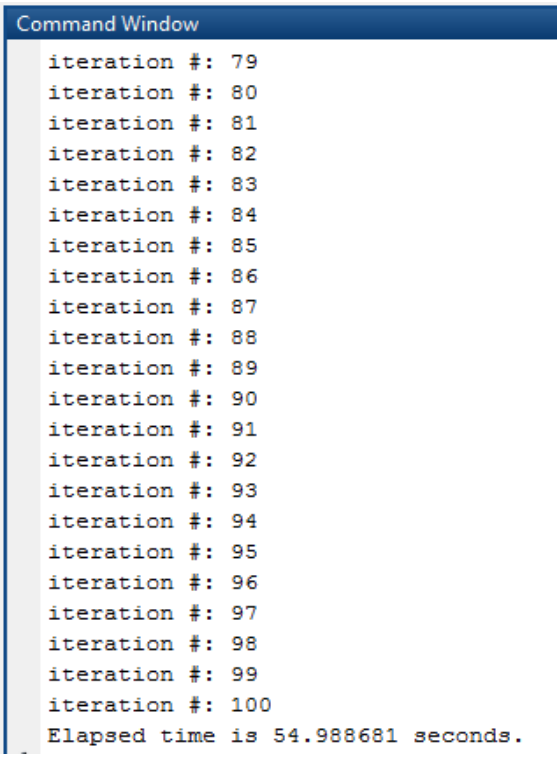

Figure 5: Iteration

This figure shows the optimization of attack. After 100 iteration such attack node identified.

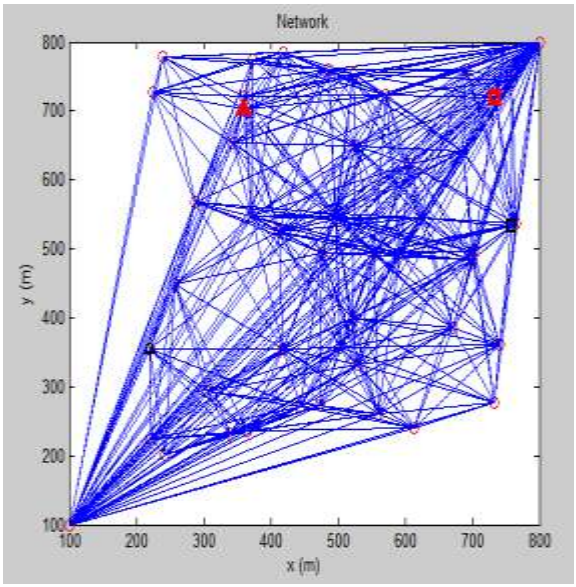

Figure 6: Attack node optimized

This figure shows the optimization of attack. After 100 iteration such attack node identified.

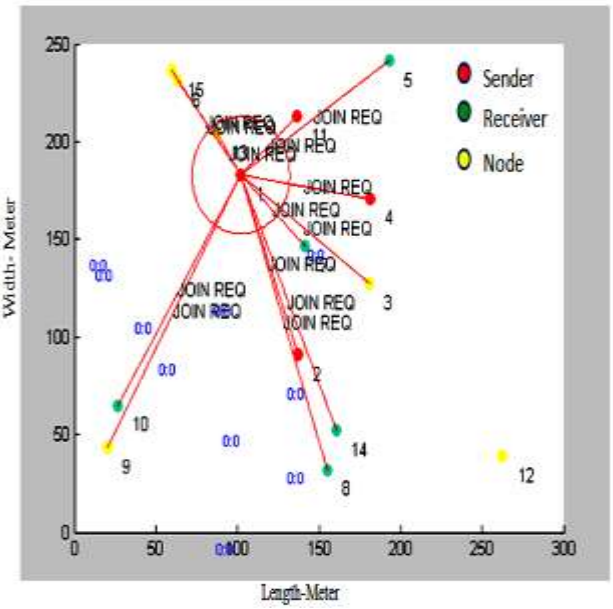

Figure 7: Simulation of VANET using ODMRP

In simulation graph there are three state of node. First is the node which only behave as a node, it showing by yellow color. Second type of node which behave as a sender node, it is showing by red color. Third type of node which behave as a receiver node, it is showing by green color.

Table 1:
Simulation parameter

Sr No.	Parameters	Proposed Work
1	Software	MATLAB
2	Simulation area	Upto 8000m X 800m
3	Methodology	NN and ODMRP
4	MAC Protocol	802.11
5	Number of nodes	Upto 100
6	speed (m/s)	25
7	Simulation time (Sec)	83
8	Packet size (B)	1024
9	Source and Destination average node	20
10	Total packets sent	196
11	Total packets rcvd	3666
12	Total bytes sent	46048
13	Total bytes rcvd	944464
14	End to End Delay (Sec)	0.01
15	Throughput (Kbps)	6800
16	Packet Delivery ratio	6.2%

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 13, Issue 01, January 2024)

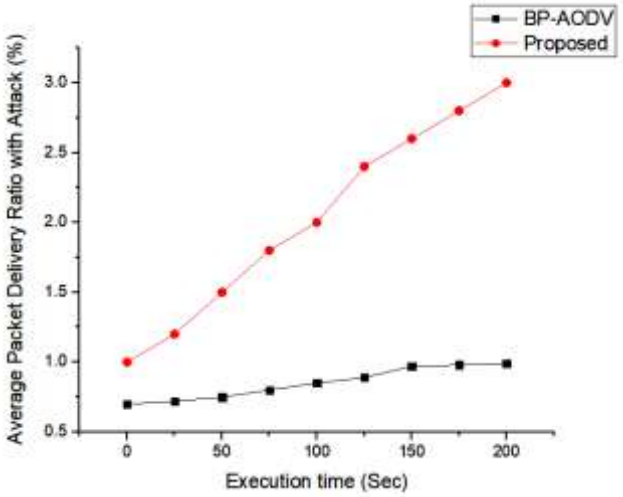

Figure 8: Packet Delivery ratio with attack

This figure shows packet delivery ratio with attack condition. Previous PDR is 0.9% while in proposed work it achieve upto 3%.

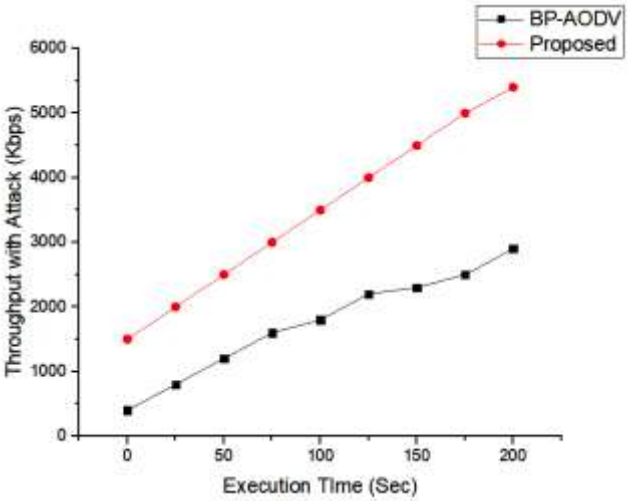

Figure 10: Throughput with attack

This figure shows throughput with attack condition. Proposed algorithm achieves upto 5400Kbps while previous it achieves upto 2600Kbps.

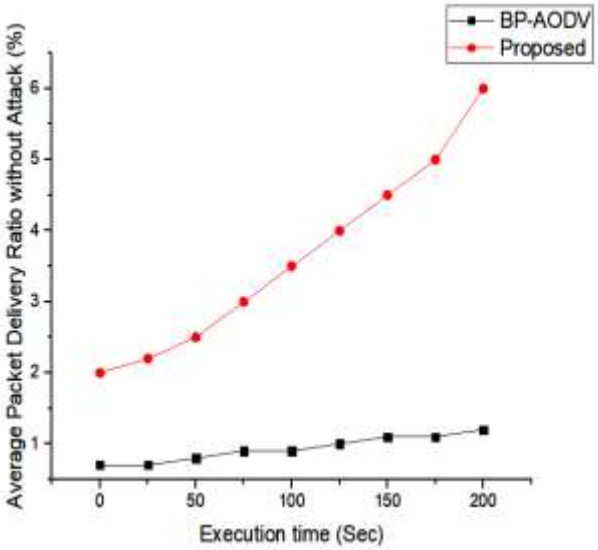

Figure 9: Packet Delivery ratio without attack

This figure shows packet delivery ratio without attack condition. Previous PDR is 1% while in proposed work it achieves upto 6.2%.

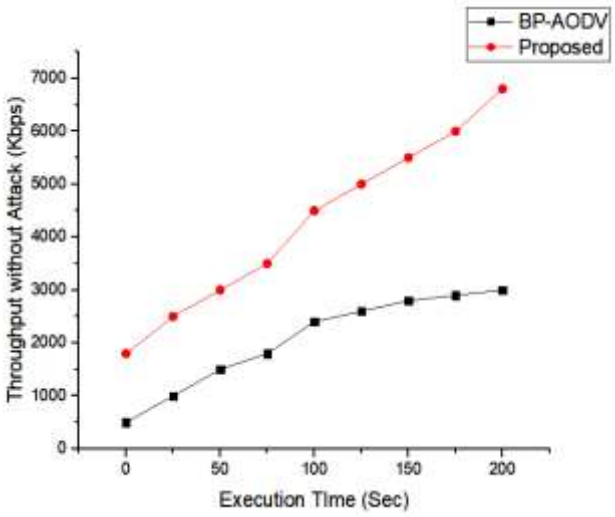

Figure 11: Throughput without attack

This figure shows throughput without attack condition. Proposed algorithm achieves upto 6800Kbps while previous it achieves upto 2800Kbps.

IV. CONCLUSION

This paper presents blackhole attack protected On-Demand Routing Protocol with authentication algorithm for VANIT. This research work consider total number of nodes upto 100, where some of source node and some of destination node. Proposed method based on demand protocol and NN for optimization while previous work based on AODV protocol. The overall simulation time is reduced by proposed approach. There are two scenarios to calculate performance parameters. First is when consider black hole attack another is when consider without attack. Proposed algorithm achieved significant better result than previous approach. Therefore proposed approach gives better result in terms of packet delivery ratio, end to end delay and throughput both case of attack for attack and without attack.

REFERENCES

[1] A. Revathi and S. G. Santhi, "Blackhole attack Detection based on Trust Calculation Mechanism in Wireless Sensor Networks," 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2022, pp. 1-4, doi: 10.1109/ICAECT54875.2022.9807980.

[2] E. Lema, E. G. -M. Desalegn, B. Tiwari and V. Tiwari, "Trust Embedded AODV for securing and Analyzing Blackhole attack in MANET," 2022 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Naya Raipur, India, 2022, pp. 362-367, doi: 10.1109/WIECON-ECE57977.2022.10150765.

[3] A. V. Jatti and V. J. K. Kishor Sonti, "Performance Improvements of Routing Protocol by Blackhole Detection using Trust Based Scheme," 2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Amman, Jordan, 2022, pp. 159-164, doi: 10.1109/MENACOMM57252.2022.9998237.

[4] W. Choukri, H. Lamaazi and N. Benamar, "A Novel Deep Learning-based Framework for Blackhole Attack Detection in Unsecured RPL Networks," 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakheer, Bahrain, 2022, pp. 457-462, doi: 10.1109/3ICT56508.2022.9990664.

[5] P. P. Ioulianou, V. G. Vassilakis and S. F. Shahandashti, "ML-based Detection of Rank and Blackhole Attacks in RPL Networks," 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Porto, Portugal, 2022, pp. 338-343, doi: 10.1109/CSNDSP54353.2022.9908049.

[6] S. Barai and P. Bhaumik, "Detection and Mitigation of Blackhole Attack Effect in Opportunistic Networks," 2021 19th OITS International Conference on Information Technology (OCIT), Bhubaneswar, India, 2021, pp. 155-160, doi: 10.1109/OCIT53463.2021.00040.

[7] A. U. Khan, R. Puree, B. K. Mohanta and S. Chedup, "Detection and Prevention of Blackhole Attack in AODV of MANET," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 2021, pp. 1-7, doi: 10.1109/IEMTRONICS52119.2021.9422643.

[8] T. Terai, M. Yoshida, A. G. Ramonet and T. Noguchi, "Blackhole Attack Cooperative Prevention Method in MANETs," 2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW), Naha, Japan, 2020, pp. 60-66, doi: 10.1109/CANDARW51189.2020.00024.

[9] R. Saputra, J. Andika and M. Alaydrus, "Detection of Blackhole Attack in Wireless Sensor Network Using Enhanced Check Agent," 2020 Fifth International Conference on Informatics and Computing (ICIC), Gorontalo, Indonesia, 2020, pp. 1-4, doi: 10.1109/ICIC50835.2020.9288571.

[10] F. Taranum, A. Sarvat, N. Ali and S. Siddiqui, "Detection and Prevention of Blackhole node," 2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), Kolkata, India, 2020, pp. 1-7, doi: 10.1109/IEMENTech51367.2020.9270072.