IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005233

An Efficient Routing Protocol and Neural Network Approach for Detection and Prevention of Wormhole Attack in Wireless Sensor Networks

Shivgopal Pragee[1], Prof. Rajdeep Shrivastava[2]

Research Scholar, Dept. of ECE, Lakshmi Narain College of Technology Excellence, Bhopal, India[1]

Assistant Professor, Dept. of ECE, Lakshmi Narain College of Technology Excellence, Bhopal, India[2]

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 network (WSN). Wormhole 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, MAC, CAN.

I. INTRODUCTION

Wireless Sensor Networks are independent and decentralized remote frameworks. Wireless sensor network consist of nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. vehicle phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These hubs can arrange themselves and due to their self-design capacity, they can be conveyed critically without the need of any foundation. Internet Engineering Task Force (IETF) has WSN working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for WSNS, i.e. AODV, OLSR, DSR etc.

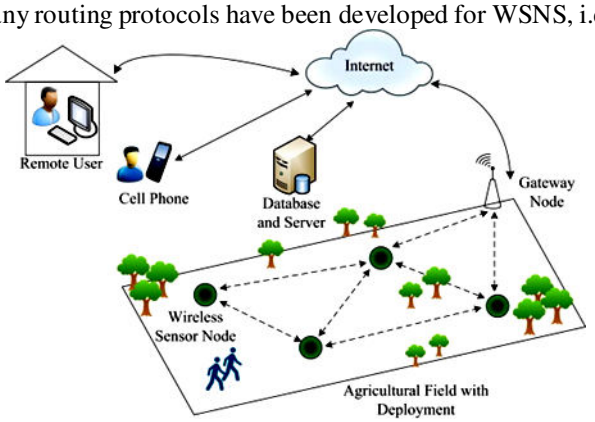

Figure 1: WSN representation

The most important concern for the essential usefulness of the organization is security in the wireless sensor Organization. The nature of organization access, classification and information protection can be refined by guaranteeing security issues have been addressed. WSNs likewise experience the ill effects of safety attacks because of their highlights like open medium, powerfully evolving geography, absence of focal control and the board, agreeable calculations and no particular insurance component. These elements changed the circumstance on the front line for the WSNs against the dangers to safeguard.

The WSNs work without an incorporated administration where the hubs communicate on shared trust. That component makes WSNs more powerless against being mishandled inside the organization by an interloper. Wireless

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005233

connections regularly make the WSNs more helpless against attacks, making it simpler for the attacker to arrive at the organization and access the progressing correspondence. Hubs present inside the scope of wireless connections can catch and even partake in the organization. WSNs should have a protected method of transmission and correspondence and this is an exceptionally troublesome and basic issue on the grounds that there are that dangers of attack on the networks.

Security is the call of the day. Vehicle hubs present in the wireless correspondence reach can catch and even take part. To guarantee safe correspondence and transmission, the designers need to comprehend various sorts of attacks and their effect on the WSNs. Wormhole attack, Dark hole attack, Sybil attack, flood attack, steering table flood attack, Disavowal of Administration (DoS), egotistical hub making trouble, pantomime attack are sorts of attacks that a WSN may experience the ill effects of. A WSN is more defenseless against these attacks as correspondence is centered around common certainty between hubs, there is no essential issue for network control, no authorization office, the geography is effectively developing and the assets are restricted.

Wireless sensor organization security is the greatest worry for the fundamental organization usefulness. The accessibility of organization access, classification and information trustworthiness can be refined by guaranteeing that security issues have been settled. WSN additionally experiences security attacks because of its highlights, for example, open media, dynamic difference in geography, absence of focal control, and no unmistakable protection component. These elements have changed the war zone circumstance for the WSN against the security dangers.

II. RELATED WORK

O. R. Ahutu, et al., presents a lightweight multi-hop directing convention for 802.15.4 WSN that expects to limit the energy utilization and furthermore to recognize the wormhole attacks. Recreation results demonstrate that our MAC Concentrated Directing Convention (MCRP) beats other existing comparative conventions. [1]

A. K. Goyal et al., proposed a protected and gainful WSN structure, a broad layout of traits, challenges, security attacks and necessities should be overseen. The excellent objective of this paper is to give a gathering of safety requirements, security ascribes and troubles. [2]

D. P. Choudhari et al., separating the parcel conveyance proportion (PDR) for the organization under Spying and DDoS attacks and after removal of these attacks the bundle conveyance proportion (PDR) is extended for the organization. The Bundle Conveyance Proportion for instance PDR is the amount of parcels got and the bundles made as recorded in follow archive [3]

R. Kolandaisamy, et al., proposed a novel arrangement attack area using vehicle mode examination in Exploratory Based Subterranean insect State Approach (EBACA) for WSN is proposed. The secret assumption that can't avoid being that a mode examination of vehicles decides faithful quality and interestingness of messages they drive. [4]

B. Luo, et al., propose a blockchain engaged trust-based zone security protection scheme in WSN. Specifically, by stalling the different requirements of the sales vehicle and the accommodating vehicle during the path toward building the obscure covering area, similarly as joining the credits of these two positions, we devise the trust the heads procedure reliant on Dirichlet conveyance.[5]

Y. Zeng et al., present a trouble based causative attack which centers at the stock organization of DL classifiers in the WSN. We first train a classifier using WSN replicated data which satisfies the rule accuracy for recognizing poisonous traffic in the WSN. By then, we develop the adequacy of our presented attack plot on this pre-arranged classifier. [6]

W. Li et al., proposes a Sybil hubs disclosure system subject to RSSI course of action and vehicle driving structure - RSDM. RSDM surveys the differentiation between the RSSI progression and the driving system by interesting detachment planning to recognize Sybil hubs. The test outcomes show that RSDM performs well with a higher recognizable proof rate and a lower botch rate. [7]

Y.Gao et al., proposed recognizable proof structure involves two basic portions: progressing network traffic collection module and organization traffic area module. To amass our proposed system, we go through Shimmer to speed data planning and use HDFS to store huge dubious attacks. [8]

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005233

J. R. et al., basically revolves around perceiving the harmful hub that declares to be a certified vehicle all through the meeting catching attack in WSNs and moreover analyzes on the throughput, delay at end centers, total checks of parcel created, traded and dropped using the Organization Test framework 2 (NS2) instrument and fitting acceptance gave. [9]

M. Poongodi et al., proposed regulator instrument thwarts the robotized attacks similarly like botnet zombies. The regulator is used to check and confine by far most of the robotized DDoS attacks. [10]

S. Kumar et al., proposed a bundle area figuring for the expectation of DoS attacks is proposed. This estimation will have the alternative to perceive the various threatening hubs in the organization which are sending superfluous bundles to stick the organization and that will in the end stop the organization to send the security messages. [11]

A. M. Alrehan et al., base on looking at the guideline attacks close by DDoS attack on WSN structure similarly as examining possible courses of action with an accentuation on man-made intelligence based responses for perceive such attacks at this moment. [12]

III. PROPOSED METHODOLOGY

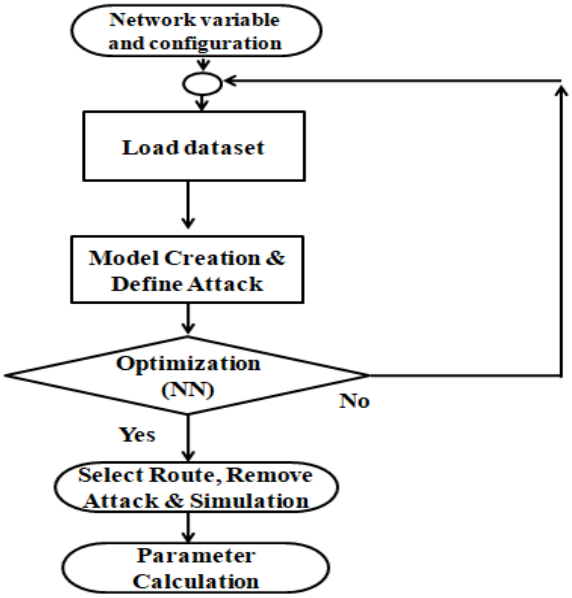

Figure 2: Flow Chart

Algorithm:

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 wormhole 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.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005233

IV. SIMULATION AND RESULT

The implementation of the proposed algorithm is done over MATLAB 9.4.0.813654 (R2018a). The wireless sensor 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.

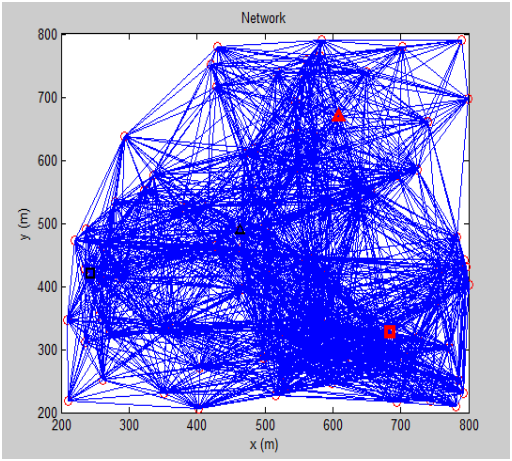

Figure 3: Network model creation and attack introduce

This figure shows the attack introduces, here node number 8 and node number 21 is assigned as a wormhole attack node.

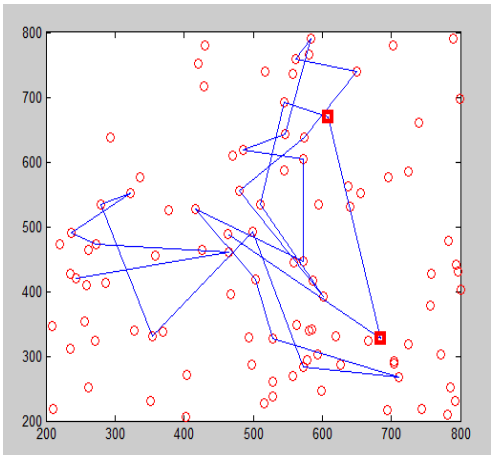

Figure 4: Network model simulation-I

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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005233

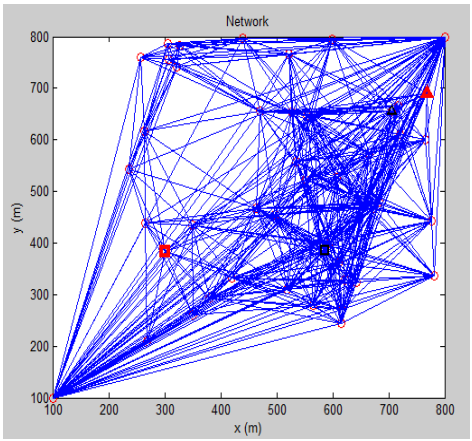

Figure 5: Attack node optimization-I

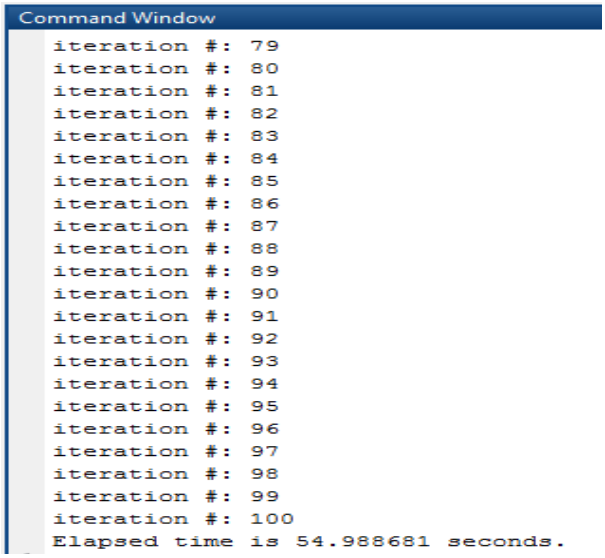

Figure 6: Iteration

This figure shows the optimization of attack, after 100 iterations such attack node identified.

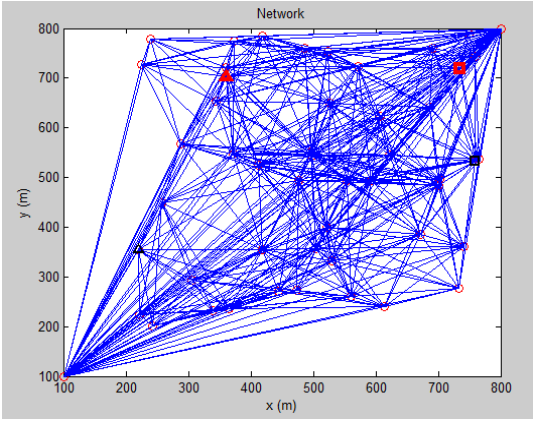

Figure 7: Attack node optimized

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005233

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

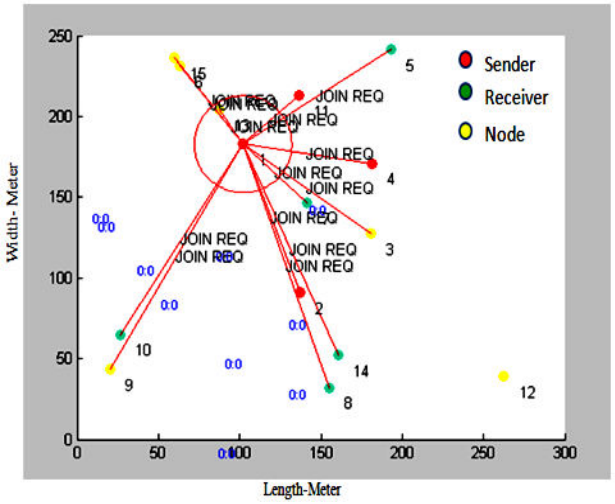

Figure 8: Simulation of WSN using ODMRP

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 9.4
2	Simulation area	Upto 8000m X 800m
3	Methodology	NN and ODMRP
4	Simulation time (Sec)	83
5	Packet size (B)	1024
6	Source and Destination average node	20
7	Total packets sent	196
8	Total packets rcvd	3666
9	Total bytes sent	46048
10	Total bytes rcvd	944464
11	End to End Delay (Sec)	0.01
12	Throughput (Kbps)	6800
13	Packet Delivery ratio	6.2%

V. CONCLUSION

This paper presents wormhole attack protected On-Demand Routing Protocol with authentication algorithm for WSN. 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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005233

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] O. R. Ahutu and H. El-Ocla, "Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks," in IEEE Access, vol. 8, pp. 63270-63282, 2020, doi: 10.1109/ACCESS.2020.2983438.

[2] A. K. Goyal, A. Kumar Tripathi and G. Agarwal, "Security Attacks, Requirements and Authentication Schemes in WSN," 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), GHAZIABAD, India, 2019, pp. 1-5.

[3] D. P. Choudhari and S. S. Dorle, "Maximization of packet delivery ratio for DADCQ protocol after removal of Eavesdropping and DDoS attacks in WSN," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-8.

[4] R. Kolandaisamy, R. M. Noor, M. R. Zaba, I. Ahmedy and I. Kolandaisamy, "Markov Chain Based Ant Colony Approach for Mitigating DDoS Attacks Using Integrated WSN Mode Analysis in WSN," 2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP), Chennai, India, 2019, pp. 1-5.

[5] B. Luo, X. Li, J. Weng, J. Guo and J. Ma, "Blockchain Enabled Trust-based Location Privacy Protection Scheme in WSN," in IEEE Transactions on Wireless Technology.

[6] Y. Zeng, M. Qiu, J. Niu, Y. Long, J. Xiong and M. Liu, "V-PSC: A Perturbation-Based Causative Attack Against DL Classifiers' Supply Chain in WSN," 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, NY, USA, 2019, pp. 86-91.

[7] W. Li and D. Zhang, "RSSI Sequence and WSN Driving Matrix Based Sybil Nodes Detection in WSN," 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN), Chongqing, China, 2019, pp. 763-767.

[8] Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo and X. Zeng, "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Wireless Ad Hoc Network," in IEEE Access, vol. 7, pp. 154560-154571, 2019.

[9] J. R. and N. S. Bhuvaneswari, "Malicious node detection in WSN Session Hijacking Attack," 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2019, pp. 1-6.

[10] M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi and M. Ma, "Intrusion Prevention System for DDoS Attack on WSN With reCAPTCHA Controller Using Information Based Metrics," in IEEE Access, vol. 7, pp. 158481-158491, 2019.

[11] S. Kumar and K. S. Mann, "Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in WSNs," 2019 International Conference on Automation, Computational and Technology Management (ICACTM), London, United Kingdom, 2019, pp. 89-94.

[12] A. M. Alrehan and F. A. Alhaidari, "Machine Learning Techniques to Detect DDoS Attacks on WSN System: A Survey," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6.

[13] R. N. Nabwene, "Review on Intelligent Internal Attacks Detection in WSN," 2018 4th Annual International Conference on Network and Information Systems for Computers (ICNISC), Wuhan, China, 2018, pp. 1-6.

[14] T. Zaidi and Syed.Faisal, "An Overview: Various Attacks in WSN," 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 2018, pp. 1-6.

[15] S. Hamdan, A. Hudaib and A. Awajan, "Hybrid Algorithm to Detect the Sybil Attacks in WSN," 2018 Fifth International Symposium on Innovation in Information and Communication Technology (ISIICT), Amman, 2018, pp. 1-6.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details