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 3, March 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 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003008

An Efficient Routing Protocol and Neural Network Approach for Detecting and Preventing Wormhole Attacks in Wireless Sensor Networks

Poonam[1], Prof. Nitesh Kumar[2]

M.Tech Scholar, Dept. of ECE., Sagar Institute of Research Technology & Science, Bhopal, India[1]

Assistant Professor, Dept. of ECE., Sagar Institute of Research Technology & Science, 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.

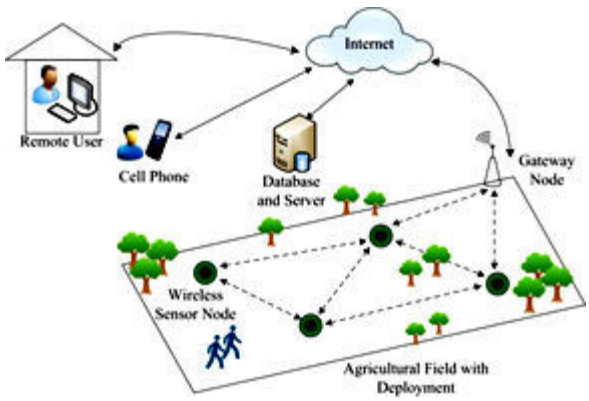

Figure 1: WSN representation

The most important concern for the basic functionality of the network is security in the wireless sensor Network. The quality of network access, confidentiality and data privacy can be accomplished by ensuring security issues have been addressed. WSNs also suffer from security attacks due to their features such as open medium, dynamically changing

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

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003008

topology, lack of central control and management, cooperative algorithms and no specific protection mechanism. These factors changed the situation on the battlefield for the WSNs against the threats to defense.

The WSNs operate without a centralized administration where the nodes interact on mutual trust. That feature makes WSNs more vulnerable to being abused within the network by an intruder. Wireless links often make the WSNs more vulnerable to attacks, making it easier for the attacker to reach the network and access the ongoing communication. Nodes present within the range of wireless links can overhear and even participate in the network. WSNs must have a safe way of transmission and communication and this is a very difficult and critical problem because there are that threats of attack on the networks.

Security is the cry of the day. Vehicle nodes present in the wireless communication range can overhear and even participate. To ensure safe communication and transmission, the engineers have to understand different types of attacks and their impact on the WSNs. Wormhole attack, Black hole attack, Sybil attack, flood attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kinds of attacks that a WSN may suffer from. A WSN is more vulnerable to these attacks as communication is focused on mutual confidence between nodes, there is no central point for network control, no authorization facility, the topology is actively evolving and the resources are limited.

Wireless sensor network (WSN) security is the biggest concern for the basic network functionality. The availability of network access, confidentiality and data integrity can be accomplished by ensuring that security problems have been resolved. WSN also suffers from security attacks due to its features such as open media, dynamic change of topology, lack of central control, and no clear defense mechanism. These factors have changed the battle field situation for the WSN against the security threats.

II. BACKGROUND

O. R. Ahutu, et al.,[1] presents a lightweight multi-hop routing protocol for 802.15.4 WSN that aims to minimize the energy consumption and also to detect the wormhole attacks. Simulation results prove that our MAC Centralized Routing Protocol (MCRP) outperforms other existing similar protocols. [1]

A. K. Goyal et al., proposed a safe and productive WSN framework, a broad outline of attributes, challenges, security attacks and necessities must be managed. The prime goal of this paper is to give a grouping of security prerequisites, security attributes and difficulties. [2]

D. P. Choudhari et al., breaking down the packet delivery ratio (PDR) for the network under Spying and DDoS attacks and after expulsion of these attacks the packet delivery ratio (PDR) is expanded for the network. The Packet Delivery Ratio for example PDR is the quantity of packets got and the packets created as recorded in follow document [3]

R. Kolandaisamy, et al., proposed a novel plan attack location utilizing vehicle mode investigation in Exploratory Based Ant Colony Approach (EBACA) for WSN is proposed. The hidden supposition that will be that a mode investigation of vehicles determines unwavering quality and trickiness of messages they drive. [4]

B. Luo, et al., propose a blockchain empowered trust-based area security insurance conspire in WSN. In particular, by breaking down the various prerequisites of the solicitation vehicle and the helpful vehicle during the way toward building the unknown shrouding locale, just as joining the attributes of these two jobs, we devise the trust the executives technique dependent on Dirichlet conveyance.[5]

Y. Zeng et al., present a bother based causative attack which focuses at the inventory network of DL classifiers in the WSN. We first train a classifier utilizing WSN reproduced information which fulfills the guideline precision for distinguishing pernicious traffic in the WSN. At that point, we expand on the adequacy of our introduced attack plot on this pre-prepared classifier. [6]

W. Li et al., proposes a Sybil nodes discovery strategy dependent on RSSI arrangement and vehicle driving framework - RSDM. RSDM assesses the distinction between the RSSI succession and the driving framework by unique separation coordinating to distinguish Sybil nodes. The test results show that RSDM performs well with a higher identification rate and a lower mistake rate. [7]

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

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003008

Y. Gao et al., proposed identification framework comprises of two fundamental segments: ongoing network traffic assortment module and network traffic location module. To assemble our proposed framework, we go through Sparkle to speed information preparing and use HDFS to store enormous suspicious attacks. [8]

J. R. et al., essentially centers around recognizing the malignant node that professes to be a genuine vehicle all through the session capturing attack in WSNs and furthermore examines on the throughput, delay at end focuses, complete checks of packet produced, traded and dropped utilizing the Network Test system 2 (NS2) instrument and fitting induction gave. [9]

M. Poongodi et al., proposed reCAPTCHA controller instrument forestalls the robotized attacks comparatively like botnet zombies. The reCAPTCHA controller is utilized to check and restrict the vast majority of the robotized DDoS attacks. For actualizing this system, the data hypothesis based measurement is utilized to examine the deviation in clients demand regarding entropy. [10]

S. Kumar et al., proposed a packet location calculation for the anticipation of DoS attacks is proposed. This calculation will have the option to recognize the numerous malignant nodes in the network which are sending irrelevant packets to stick the network and that will in the end stop the network to send the security messages. [11]

A. M. Alrehan et al., center around examining the principle attacks alongside DDoS attack on WSN framework just as investigating potential arrangements with an emphasis on AI based answers for recognize such attacks right now. [12]

R. N. Nabwene et al., Trust foundation in WSN helps manage insider attacks, albeit the vast majority of the current arrangements accept the attacker will consistently show a stable deceptive conduct after some time, which isn't the situation with clever insider attackers, they display insightful practices to evade identification. [13]

T. Zaidi et al., Right now, it is being seen that numerous security challenges are there where research need to step-up forward for making WSN progressively secure. A basic examination is talked about broadly concerning WSN parts, security issues and difficulties, attacks and its answers. [14]

III. PROPOSED METHODOLOGY

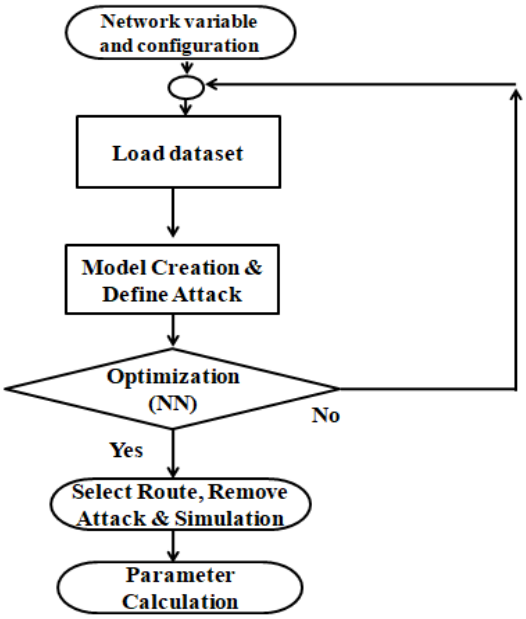

Figure 2: Flow Chart

Algorithm:

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

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

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003008

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

IV. SIMULATION RESULTS

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.

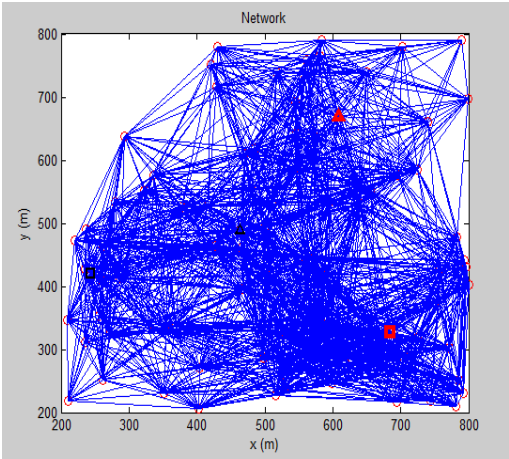

Figure 3: Network model creation and attack introduce

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

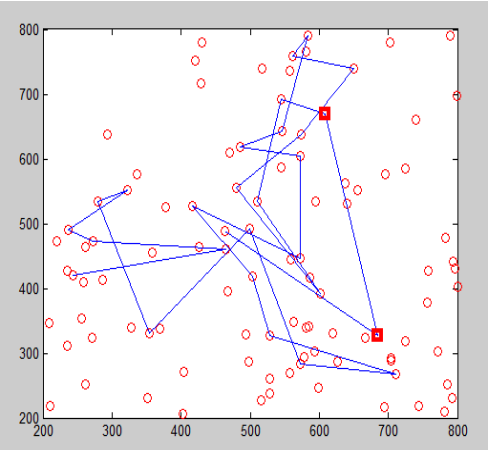

Figure 4: Network model simulation-I

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

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003008

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

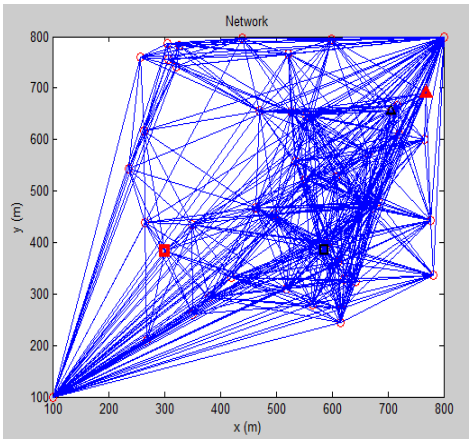

Figure 5: Attack node optimization-I

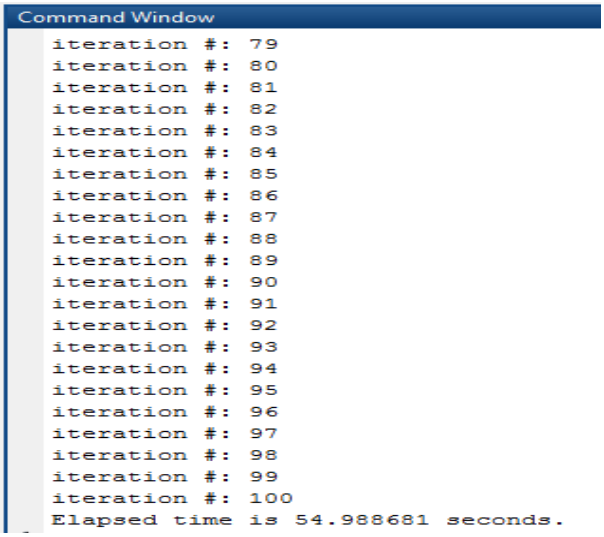

Figure 6: Iteration

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

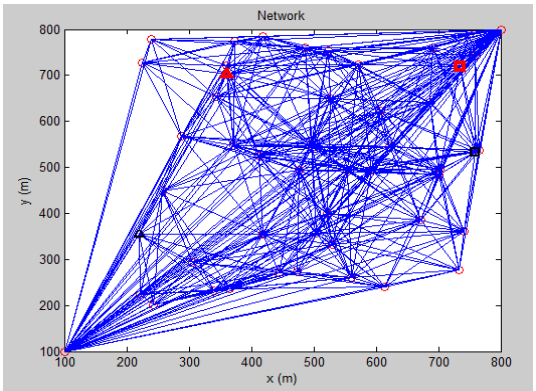

Figure 7: Attack node optimized

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

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003008

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

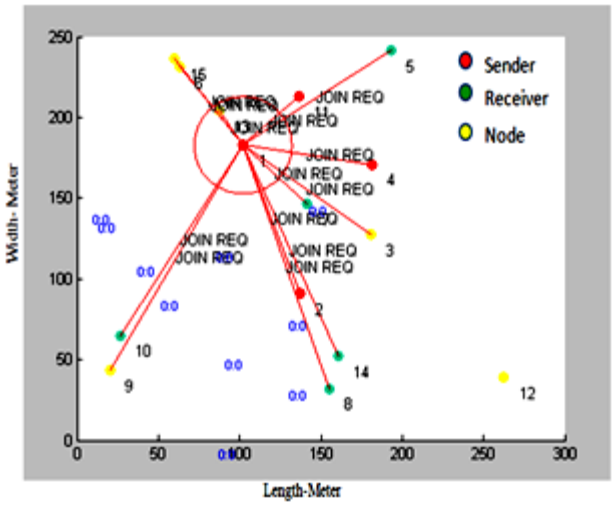

Figure 8: Simulation of WSN using ODMRP

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 parameters. First is when consider black hole attack another is when consider without attack. Proposed algorithm

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

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003008

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