Research Result

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

Jyoti Rathore[1], Prof. Prakash Saxena[2], Prof. Seema Kirar[3]

[1]*Research Scholar, Department of ECE, Bansal Institute of Science and Technology, Bhopal*
[2]*Assistant Professor & HoD, Department of ECE, Bansal Institute of Science and Technology, Bhopal*
[3]*Assistant Professor Department of ECE, Bansal Institute of Science and Technology, Bhopal*

Received: 10 March 2022; Revised: 20 April 2022; Accepted: 23 April 2022;

ABSTRACT

Wireless networks are gaining popularity today, as users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the wireless sensor network (WSN). A wormhole attack is one of the security threats in which the traffic has redirected this type of node that honestly does no longer exist inside the network. This paper is proposed a neural network (NN) for optimization and a 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

1. INTRODUCTION

Wireless Sensor Networks are autonomous and decentralized distant structures. Remote sensor networks comprise hubs that are free in moving done in the organization. Hubs are the frameworks or gadgets, for example, vehicle telephones, PC, individual advanced help, MP3 player and PC that are taking an interest in the organization and are versatile. These hubs can go about as host/switch or both simultaneously. They can frame inconsistent geographies relying upon their availability with one another in the organization. These centres can organize themselves, and because of their self-plan limit, they can be conveyed basically without the need for any establishment. Web Designing Team (IETF) has a WSN working gathering (WG) committed to creating IP directing conventions. Steering conventions are one of the problematic and intriguing examination regions. Many directing conventions have been created for WSNS, such as AODV, OLSR, DSR, etc.

The main worry for the fundamental convenience of the association is security in the remote sensor Association. The idea of association access, characterization and data insurance can be refined by ensuring security issues have been tended to. WSNs, in like manner, experience the evil impacts of security assaults because of their features like open medium, effectively advancing topography, nonattendance of central control and the board, pleasing estimations and no specific protection part. These components changed the situation on the bleeding edge for the WSNs against the threats to protect.

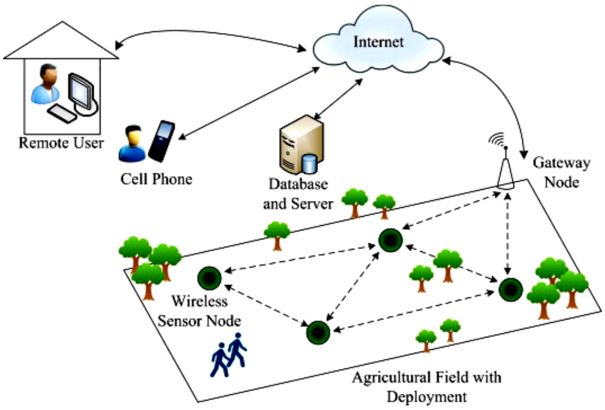


Figure 1: WSN representation

The WSNs work without a joined organization where the centre points convey shared trust. That part makes WSNs more feeble against being misused inside the association by a gatecrasher. Remote associations routinely make the WSNs more powerless against assaults, simplifying it for the assailant to show up at the association and access the advancing correspondence. Center points present the extent to of remote associations can get and even participate in the association. WSNs ought to have a safeguarded strategy for transmission and correspondence, and this is an especially irksome and essential issue because there are that risks of assault on the organizations.

Security is the call of the day. Vehicle centre points present in the remote correspondence reach can get and even participate. To ensure safe correspondence and transmission, the architects need to appreciate different kinds of assaults and their impact on the WSNs. Wormhole assault, Dull opening assault, Sybil assault, flood assault, controlling table flood assault, Repudiation of Organization (DoS), self-absorbed centre point raising hell, emulate assault are kinds of assaults that a WSN might encounter the evil impacts of. A WSN is all the more unprotected against these assaults as correspondence is revolved around normal sureness between centres, there is no fundamental issue for network control, no approval office, the geology is successfully created, and the resources are confined.

Remote sensor association security is the best concern for the essential association handiness. The availability of association access, order, and data reliability can be refined by ensuring that settled security issues. WSN encounters security assaults in light of its features, such as open media, dynamic contrast in geology, nonappearance of central control, and no undeniable assurance. These components have changed the disaster area situation for the WSN against the security risks.

2. BACKGROUND

O. R. Ahutu, et al.,[1] presents a lightweight multi-jump coordinating show for 802.15.4 WSN that hopes to restrict the energy usage and besides to perceive the wormhole assaults. Diversion results show that our Macintosh Concentrated Coordinating Show (MCRP) beats other existing similar shows. [1]

A. K. Goyal et al., proposed a safeguarded and beneficial WSN structure, an expansive format of qualities, challenges, security assaults and necessities ought to be administered. The great goal of this paper is to give a social occasion of well-being necessities, security attributes and inconveniences. [2]

D. P. Choudhari et al., isolating the package movement extent (PDR) for the association under Spying and DDoS assaults, and after the expulsion of these assaults, the group transport extent (PDR) is reached out for the association. The Group Transport Extent for example, PDR is how much packages got and the packs made as kept in follow chronicle [3]

R. Kolandaisamy et al., proposed an original game plan assault region involving vehicle mode assessment in Exploratory Based Underground bug State Approach (EBACA) for WSN is proposed. The mysterious suspicion that can't try not to be that a mode assessment of vehicles concludes steadfast quality and intriguing quality of messages they drive. [4]

B. Luo, et al., propose a blockchain drew in trust-based zone security insurance conspire in WSN. In particular, by slowing down the various prerequisites of the deals vehicle and the obliging vehicle during the way toward building the dark covering region, also as joining the credits of these two positions, we devise the trust the heads technique dependent on Dirichlet conveyance.[5]

Y. Zeng et al., present a difficulty based causative assault which focuses at the stock association of DL classifiers in the WSN. We first train a classifier involving WSN imitated information which fulfils the standard exactness for perceiving noxious traffic in the WSN. By then, at that point, we foster the ampleness of our introduced assault plot on this set-up classifier. [6]

W. Li et al., proposes a Sybil center points divulgence framework subject to RSSI strategy and vehicle driving design - RSDM. RSDM studies the separation between the RSSI movement and the driving framework by fascinating separation intending to perceive Sybil center points. The test results show that RSDM performs well with a higher conspicuous evidence rate and a lower bungle rate. [7]

Y. Gao et al. proposed an unmistakable confirmation structure that includes two essential segments: the advancing organization traffic assortment module and the associated traffic region module. To accumulate our proposed framework, we go through Gleam to speed information arranging and use HDFS to store immense questionable assaults. [8]

J. R. et al., essentially spins around seeing the hurtful center point that pronounces to be an ensured vehicle all through the gathering getting assault in WSNs and also investigates on the throughput, delay at end focuses, absolute checks of package made, exchanged and dropped utilizing the Association Test structure 2 (NS2) instrument and fitting acknowledgment gave. [9]

M. Poongodi et al., proposed reCAPTCHA controller instrument upsets the robotized goes after likewise like botnet zombies. The reCAPTCHA controller is utilized to check and keep the vast majority of the robotized DDoS assaults by a wide margin. [10]

S. Kumar et al., proposed a group region figuring for the assumption for DoS assaults is proposed. This assessment will have the choice to see the different compromising centre points in the association, which are sending unnecessary groups to stick to the association and that will, in the end, stop the association from sending the security messages. [11]

A. M. Alrehan et al., base on taking a gander at the rule goes after nearby DDoS assault on WSN structure in basically the same manner as looking at potential game-plans with a highlight on man-made insight based reactions for see such goes after right now. [12]

3. PROPOSED METHODOLOGY

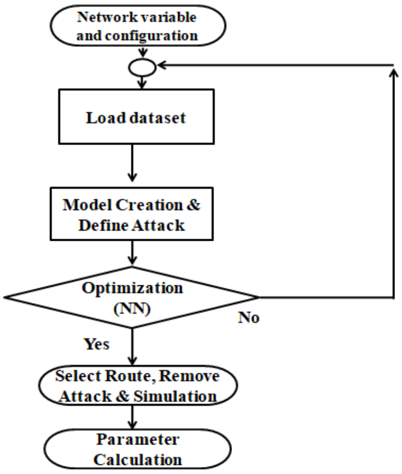

Network variable and configuration
Load dataset
Model Creation & Define Attack
Optimization (NN)
No
Yes
Select Route, Remove Attack & Simulation
Parameter Calculation

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

4. 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.

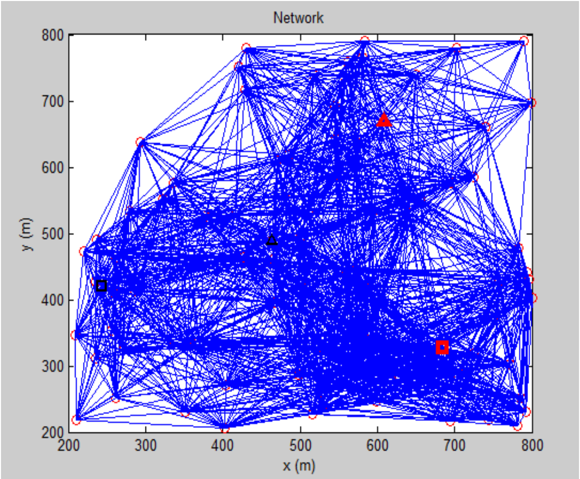


Figure 3: Network model creation and attack introduce

This figure 3 shows the attack introduces, here node number 8 and node number 21 is assigned as a wormhole attack node.

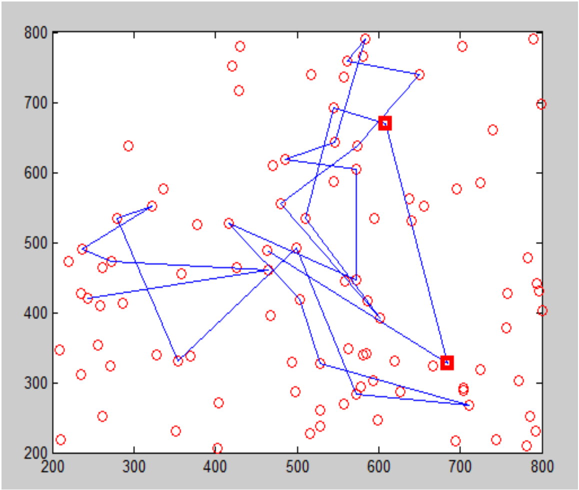


Figure 4: Network model simulation-I

This figure 4 shows the simulation of various nodes with attack nodes. But attack node start identifying.

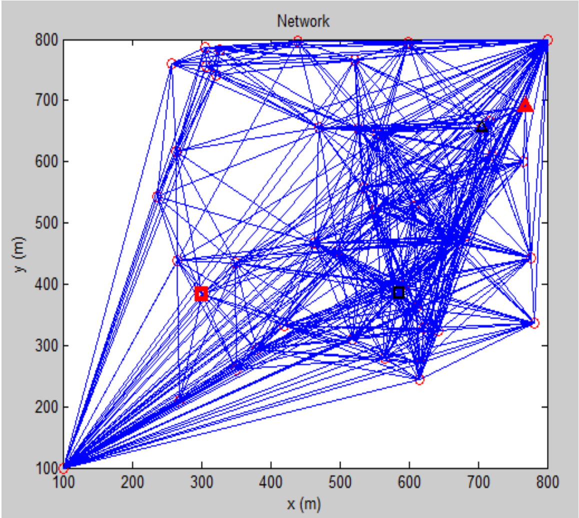
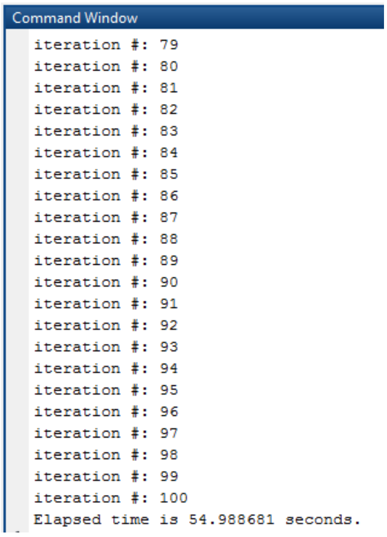


Figure 5: Attack node optimization-I



```
iteration #: 79
iteration #: 80
iteration #: 81
iteration #: 82
iteration #: 83
iteration #: 84
iteration #: 85
iteration #: 86
iteration #: 87
iteration #: 88
iteration #: 89
iteration #: 90
iteration #: 91
iteration #: 92
iteration #: 93
iteration #: 94
iteration #: 95
iteration #: 96
iteration #: 97
iteration #: 98
iteration #: 99
iteration #: 100
Elapsed time is 54.988681 seconds.
```

Figure 6: Iteration

This figure 6 shows the optimization of attack, after 100 iteration such attack node identified.

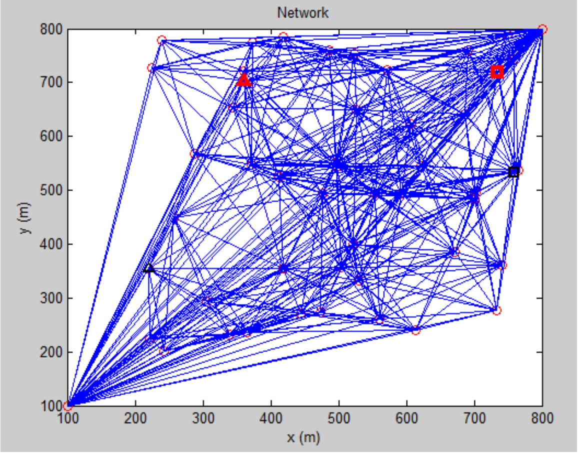


Figure 7: Attack node optimized

This figure 7 shows the optimization of attack. After 100 iterations such attack node identified.

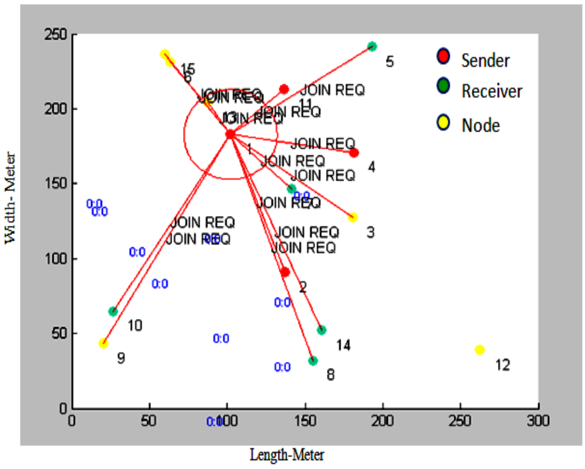


Figure 8: Simulation of WSN using ODMRP

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%

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.

5. 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 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.