
Shivgopal Pragee¹, Prof. Rajdeep Shrivastava²
Research Scholar, Dept. of ECE, Lakshmi Narain College of Technology Excellence, Bhopal, India¹
Assistant Professor, Dept. of ECE, Lakshmi Narain College of Technology Excellence, Bhopal, India²

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
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]
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

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.

Figure 2: Flow Chart
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.
This figure shows the optimization of attack, after 100 iterations such attack node identified.
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

<table>
<thead>
<tr>
<th>Sr No.</th>
<th>Parameters</th>
<th>Proposed Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Software</td>
<td>MATLAB 9.4</td>
</tr>
<tr>
<td>2</td>
<td>Simulation area</td>
<td>Upto 8000m X 800m</td>
</tr>
<tr>
<td>3</td>
<td>Methodology</td>
<td>NN and ODMRP</td>
</tr>
<tr>
<td>4</td>
<td>Simulation time (Sec)</td>
<td>83</td>
</tr>
<tr>
<td>5</td>
<td>Packet size (B)</td>
<td>1024</td>
</tr>
<tr>
<td>6</td>
<td>Source and Destination average node</td>
<td>20</td>
</tr>
<tr>
<td>7</td>
<td>Total packets sent</td>
<td>196</td>
</tr>
<tr>
<td>8</td>
<td>Total packets rcvd</td>
<td>3666</td>
</tr>
<tr>
<td>9</td>
<td>Total bytes sent</td>
<td>46048</td>
</tr>
<tr>
<td>10</td>
<td>Total bytes rcvd</td>
<td>944464</td>
</tr>
<tr>
<td>11</td>
<td>End to End Delay (Sec)</td>
<td>0.01</td>
</tr>
<tr>
<td>12</td>
<td>Throughput (Kbps)</td>
<td>6800</td>
</tr>
<tr>
<td>13</td>
<td>Packet Delivery ratio</td>
<td>6.2%</td>
</tr>
</tbody>
</table>

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 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


INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH
IN SCIENCE | ENGINEERING | TECHNOLOGY

Impact Factor: 7.512

9940 572 462  6381 907 438  ijirset@gmail.com

www.ijirset.com