Abstract-- Wireless Sensor Network (WSN) is an emblematic particular type of wireless network use to solve many real time tribulations. The node participates in this cluster help in collecting the information from various usable entities and delivers it for the productive purpose. WSN use hop-to-hop, end-to-end proclamation to distribute the right information proficiently. It helps in handing out useful information using the safe and sound, routing techniques. Intermediate node chipping in always makes it enable to provide high end rescue. A chipping in of malevolent node degrades the network performance due to lacking in peer-to-peer announcement. Malevolent node association make more energy dilapidation from the given other contributor nodes. In such circumstances the detection and prevention of the suspicious nodes in the network is important. In this work a method comprises with various algorithms have been explained and have been used to identify the suspicious node in WSN.

I. INTRODUCTION

The term WSN (Wireless Sensor Network) [1] is employed for amalgamation of sensor nodes for sensing, dispensation and transmitting the data, nodes here connected by wireless links in a standalone trend in a outsized network. Nodes will Connect, /disconnect and reconnect with each passing moment and through the entire duration the network [2] connections will operate between the nodes that are part of it. In a assemblage of node services single/multiple nodes uses unusual topology [3] and technique to deliver data from source to intention with aim to provide time & energy efficient, a lesser amount of delay in network [4], high packet delivery ratio in its parameter.

For the period of recent years, there is a rapid development in the network technologies and wireless communications [5]. Numerous wireless services and devices like cell phones, PDA’s, laptop, etc. have been used widely all around the world. Wireless Sensor Network (WSN) [6] is turning into reality due to remarkable advancements in the wireless technology.

II. LITERATURE REVIEW

WSN keep a extraordinary network which deals to haul out the information using its sensor node and applications [7]. The sensor information such as temperature, humidity, pressure etc. can be extracted using such network. This set of connections is also applicable in area where the security and secure data packet transmission is required. Wireless is the media using which an applicability of packet transmission [8] can occur over the remote locations and thus information can be gathered. Selfish nodes [9] extract the knowledge information from it and enable the transmission by acquiring the properties of data or maneuver it for the misuse. Thus an application and research behind it to categorize the selfish entity and process them as detection and prevention purpose [10]. In these papers [1, 2], a survey over the different selfish node such as hiding the properties from self Participation. Working with the identification over the wireless sensor network has been discussed. A dynamic routing and finding a selfish node among them is need to be improved. In [3, 4], they presented the cluster based approach for the selfish node detection. The paper explained about the cluster generation, cluster finding technique and then optimizing the routing path to agree on the working nodes. Further the dissemination of selfish node [5, 6] presented. This paper [7, 8] mainly discussed all the clustering mining approaches working with the selfish node mining and separating them from the normal node using the clustering solution. Thus selfish node detection can get performed using the proposed solutions given by different authors. In these paper [9, 10], the author presented a fault tolerance method for detection of selfish node and prevention from such node network. The conversation made which gives how the node energy dissemination can be saved. The communication protocol with fault tolerance mechanism is presented to find selfish node over the WSN. In [1, 2, 3], have given the fault tolerance and discussion mechanism using the cluster head from the network node availability.
III. Assumptions & Notations

We have uses some proposition for implementing the proposed approach named as ARP-PET will verify the genuine node by providing an Honesty Stamp to each valid node by checking its previous history.

Information about each and every node has been already stored in TSU. Every Node will calculate the approximate distance of each neighbor node by within the range.

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Symbols</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GNT</td>
<td>Genuine Neighbor Table</td>
</tr>
<tr>
<td>2</td>
<td>SN</td>
<td>Speed of Node</td>
</tr>
<tr>
<td>3</td>
<td>TD</td>
<td>Time Duration</td>
</tr>
<tr>
<td>4</td>
<td>LP</td>
<td>Last position</td>
</tr>
<tr>
<td>5</td>
<td>RT</td>
<td>Reliable Trust</td>
</tr>
<tr>
<td>6</td>
<td>AP</td>
<td>Actual Position</td>
</tr>
<tr>
<td>7</td>
<td>IT</td>
<td>Indirect Trust</td>
</tr>
<tr>
<td>8</td>
<td>DT</td>
<td>Direct Trust</td>
</tr>
<tr>
<td>9</td>
<td>EP</td>
<td>Estimated Position</td>
</tr>
<tr>
<td>10</td>
<td>PTV</td>
<td>Preliminary Trust Value</td>
</tr>
<tr>
<td>11</td>
<td>MNT</td>
<td>Malevolent Node Table</td>
</tr>
<tr>
<td>12</td>
<td>CV</td>
<td>Credit Value</td>
</tr>
</tbody>
</table>
IV. PROBLEM FORMULATIONS

Majority rule could actually be harmful as some nodes can collude to perform an attack, and not provide an honest judgment about other nodes. The selection of acceptability is a trade-off between obtaining more accurate trustworthiness value and the convergence time required to obtain it. Less packet transmission and high delay while dealing with multiple computations Recommendation based trust model ARP-PET-WSN utilizes clustering technique to dynamically filter out attacks related to dishonest recommendations between certain time based on number of interactions, compatibility of information and closeness between the nodes.

The recommending node is chosen based on three factors to check its honesty:

- Number of interactions with the evaluated node. Unity of view with the evaluating node for solving the problem of the scarcity of knowledge. Closeness to the evaluating node. Recommendations are accumulated over a period of time to ensure the consistency of recommendations provided by the recommending node regarding the evaluated node.

V. ATTACKS RESILIENT AND PROFICIENT PROTOCOL FOR EFFICIENT & TRUSTED (ARP-PET) WSN COMMUNICATIONS

When node gets information, then it calculates the approximate value of each neighbor node. After that it decides from whom it wants to communicate further, on the basis of following cases:

- If last info station of neighbor node is not same with itself and they not have “Authentication Certificate Computed by Random Trust” then receiving node can refuses to receive its information and mark it as suspicious selfish node.
- If last info station of neighbor node is same but its location is not in the range of “last actual position” and “Approximate position”, then that node is marked as suspicious selfish node.

5.1 Algorithm 1: Approximate Position Estimation

- At every TD (Time Duration i.e Say TD=5 Seconds) Neighbor table will be updates itself and will delete its previously stored data to save the energy.
- Step 1: Send Hello Packets to the Near Nodes
- Step 2: Receive replies in format from each node in (PTV, LP, SN, IT, DT, AP)
- Step 3: Calculate Estimated Position (EP) = (SN*TD) + LP
- If EP=AP Set Credit Value (CV) =0 else Increase Credit Value +1
- Step 4: Put values in Genuine Neighbor Table (GNT)
- Step 5: End

Algorithm 2: Reliable Trust (RT) Calculation

- Step 1: Receive “Hello Packets”
- Step 2: if TRUST >= PTV goto Step 4
- Step 3: Else discard packet from that Node & declare as malicious node.
- Step 4: Compute (RT, IT, DT, SN, AP) step 6
- Step 5: Else Delete previous data.
- Step 6: Put new Flag to that Node & update the new trust value in RT.
- Step 7: End

5.2 Algorithm 2: Reliable Trust (RT) Calculation

Algorithm 2: Reliable Trust (RT) Calculation

- Step 1: Receive “Hello Packets”
- Step 2: if TRUST >= PTV goto Step 4
- Step 3: Else discard packet from that Node & declare as malicious node.
- Step 4: Compute RT (DT, IT, SN, AP) step 6
- Step 5: Else Delete previous data.
- Step 6: Put new Flag to that Node & update the new trust value in RT.
- Step 7: End

5.3 Algorithm 3: Discarding Malevolent Nodes

- After receiving packet from any node at receiving end following action necessary to be perform
- Step 1: Receive Packet
- Step 2: If TRUST<= RT & >=PTV [in TD=5 Seconds] go to Step 7 (Check Trust with Malicious Node Table (MNT))
- Step 3: Perform Calculations Using (IT, DT, ITV);
- RT= (CV+IT+DT) & go to Step 9
- Step 4: If (RT<=PTV) & (AP<=EP) goto Step 6
- Step 5: Else Discard data
Step 6: Put Node ID in MNT & goto Step 8
Step 7: Accept Packet From That Node

VI. RESULT & ANALYSIS

In order to evaluate the efficiency of our work, we have setup a simulation on a Machine Red Hat Linux, where we have installed and configured correctly all the patches of NS-2 which is a simulator for the network scenario and protocol.

We further configured Ubuntu with NS-2 and performed simulation and result evaluation between existing and proposed protocol.

To analyze the performance of the proposed ARP-PET for WSN, we have performed the simulation using Network Simulator-2. The performance of our proposed work is measured in terms of Average Throughput, Packet Delivery Ratio, and Average End to End Delay.

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Parameters for Simulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No. of Nodes</td>
</tr>
<tr>
<td>2</td>
<td>No. of Source</td>
</tr>
<tr>
<td>3</td>
<td>Area</td>
</tr>
<tr>
<td>4</td>
<td>Mobility model</td>
</tr>
<tr>
<td>5</td>
<td>Bandwidth</td>
</tr>
<tr>
<td>6</td>
<td>Speed</td>
</tr>
<tr>
<td>7</td>
<td>Pause time</td>
</tr>
<tr>
<td>8</td>
<td>Buffer Size</td>
</tr>
<tr>
<td>9</td>
<td>Transmission range</td>
</tr>
<tr>
<td>10</td>
<td>Sensing range</td>
</tr>
<tr>
<td>11</td>
<td>Packet size</td>
</tr>
<tr>
<td>12</td>
<td>Traffic source</td>
</tr>
<tr>
<td></td>
<td>MAC protocols</td>
</tr>
</tbody>
</table>
6.2 Evaluation Parameter: Normalized routing load, PDR (Packet Delivery Ratio), Throughput, End-to-End Delay and Energy are used to calculate performance of technique [6].

(i) Throughput: It is the measure of whole performance of the approach in terms of number of packet transmitted per seconds.

(ii) PDR (Packet Delivery Ratio): It is the ratio of, no. of packet accurately delivered to the destination with the number of packet transmitted at transmitter ends.

6.2.1 Throughput Vs Fraudulent Recommendation

Performance of our approach is measured on the basis of throughput vs. Fraudulent Nodes compared with existing approach.

In fig. 6.1 shows, the percentage of throughput, by graph we are observe on two different graph lines Existent and proposed work and hare No Defense is common scenario for both approaches. In the graph x-axis showing the Dishonest Node Recommendation and y-axis is showing throughput of three different lines and using proposed approach we improved throughput of the network.

6.4. Packet Loss Vs Attackers

Performance of our approach is measured on the basis of Packet Loss vs. dishonest recommendation. We are comparing between Existent A recommendation based trust model in dishonest nodes and Proposed approach Creating Trust Environment by Remove Time and Location Attack (CTE & RLT) hare No Defense is common scenario for both approach.
In fig. 6.2, in graph it can be observed that on two different graph lines existent and proposed work and here no Defense is common scenario for both approaches. In the graph x-axis showing the attacker % and y-axis is showing Packet Loss in all three methods through different lines and it is very clear that using proposed approach significant reduction in the packet loss of the network has been observed.

VII. CONCLUSION & FUTURE WORK

7.1 Conclusion

To detect efficiently misbehaviors and malevolent Sensor nodes in WSN, Here one Method ARP-PET has been proposed in Wireless Sensor Network This method have been designed to identify and cut off the nodes showing abnormal behavior as well as decreasing the network performance. ARP-PET-WSN Nodes the selection of verifier nodes which perform the work of monitoring node’s behavior. ARP-PET improves the pre-existing work which selects all the nodes as verifiers which have distrust value less than the node to be monitored. It has been optimized by proposed method taking into consideration with different parameters. The simulation results indicate that ARP-PET-WSN performs better.

7.2 Future Work

Different Machine Learning Algorithm can be used to identify the malevolent nodes in WSN environment. Few optimization techniques can be experienced to select the verifiers with the proposed methodologies. Complex traffic and mobility modeling can be considered in our simulation framework and can be evaluated in different scenarios. The proposed work can be in mitigated with a preclusion technique for the suspicious nodes nodes. The proposed method with all its algorithms can be deployed in real time to test and investigate its presentation under realistic conditions.

REFERENCES


