Prevention of Gray Hole Attack Using ABC and Fuzzy Logic

Lokeshwar Singh
Student M Tech, Computer Science of
Computer Engineering, BIMT,
Shimla, Himachal Pradesh, India

Ashish Sharma
Assistant Professor Department of
Computer Engineering, BIMT,
Shimla, Himachal Pradesh, India

DOI: 10.23956/ijarcsse/V7I8/0128

Abstract—There are many advantages and reasons for wireless sensor network to be popular. The key concern while establishing wireless sensor network (Mobile ad-hoc network) is the routing protocol to be applied. Routing process is the process of discovering the path that a data packet will follow to get it from the source node to the destination node. As the mobile ad-hoc network consists of mobile nodes with no controlling unit in which each and every step of communication is handled by the nodes within the network itself. The selection of routing protocol is one of the difficult tasks and the key challenge faced by the routing is the energy consumption issue apart from the others. In this research, the routing technique is developed with a basic focus on reduction of the energy consumption while improving the overall performance of the network. Presently, various efficient routing protocols have been estimated for wireless sensor network. In the presence of malicious nodes, the network becomes penetrable to different kind of attacks. In wireless sensor network, routing-attacks are relatively serious. It has number of potential-applications in completely un-predictable in dynamic environment. Routing protocol utilized here are in a form of reactive-routing protocol known as OLSR. This routing protocol route is based on demand. The proposed work has designed and implemented wireless sensor network in OLSR routing protocol. The gray hole attack is mitigated using Fuzzy Logic based on rule sets to have better routing process and ABC (Artificial Bee Colony) algorithm at superior rate for optimizing the route set at novel objective function. In this work, the performance analysis of the network with the scenarios consisting 50 nodes moving with the speed of the 5-10m/s within the area (1000X1000) m² has been done in regards to the parameters, namely, Throughput, End-to-End Delay, BER (bit error rate) and Energy consumption.

Keywords—WSN, ABC, OLSR, Fuzzy logic, MATLAB.

I. INTRODUCTION

Wireless Sensor Network (WSN) technology enables design and implementation of novel, intriguing applications that can be used to address numerous industrial, environmental, societal and economical challenges and thus, the importance and potential of WSNs are constantly growing.

A sensor node (as shown in the Fig. 1) is generally defined as a cheap and small piece of hardware, which consists of four main units:
• One or more sensors that detect physical phenomena. Common sensors monitor scalar values of temperature, pressure, humidity, light intensity, etc.
• The sensor is coupled with a data processing unit. The latter controls sensing, application logic and network transfer. It receives data from the sensors as well as it can filter (e.g. thresholding) compress or correlate data from a series of measurement. The network structure, the communication process and the power management of the node are also organized by the processing unit.
• The data’s wireless transmission is provided by a communication interface.
• For every operational electronic system an energy source is needed.

II. FUZZY LOGIC

Fuzzy Model is the generalized model of previous classic models. As the output is not limited to only 0 and 1, so the theory of fuzzy logic is introduced. It is also known as diffuse logic. Difference between fuzzy logic and classical model is introduced using membership functions. Consider a finite set:

\[ C = \{c_1, c_2, c_3, \ldots, c_n\} \]

It is the universal set. Now according to graphical representation, suppose fuzzy sets have only two elements c1 and c2. So the degree of fuzzification can be called as entropy. \( E = \frac{f_1}{f_2} \); Where \( f_1 \) and \( f_2 \) are the distances.

![Fig. 2 Fuzzy Logic Model](image)

III. ARTIFICIAL BEE COLONY

Artificial Bee Colony (ABC) is simple as Particle Swarm Optimization (PSO) and Differential Evolution (DE) algorithms, and uses only common control parameters such as colony size and maximum cycle number. ABC as an optimization tool provides a population-based search procedure in which individuals called foods positions are modified by the artificial bees with time and the bee’s aim is to discover the places of food sources with high nectar amount and finally the one with the highest nectar. In ABC system, artificial bees fly around in a multidimensional search space and some choose food sources depending on the experience of themselves and their nest mates, and adjust their positions.

Two techniques have been developed for the process of carrying out the collection of honey bees nectar

- Recruitment
- Abandonment

The essential ABC algorithm can be divided into three stages:

i. Employed bee phase
ii. Onlooker bee phase
iii. Scout bee phase

![Fig. 3 Foraging behaviour of honey bees](image)

IV. OBJECTIVES

Aims and objectives of the work are summarized as follow:

a) To study and analyse the various existing work on detection of gray hole attack using OLSR protocol in WSN.

b) To design a WSN simulator over MATLAB 2010a with various parameters like no. of nodes, length and width of network.

c) To design and implement Intrusion Detection system based on Computational method like fuzzy logic with ABC algorithm to detect gray-hole attack in network.

d) To define a novel objective function for ABC algorithm with the rule sets for fuzzy logic to minimize the drawback of existing work.

e) To compare the proposed result with existing techniques, QOS parameters of the proposed work will be calculated.
S. P. Dongare and R. S. Mangrulkar, 2015 [5], proposed an efficient and trust based protocol for achieving energy efficiency in WSN for gray hole and black hole attacks. The proposed technique has been prevented and detected the attacker within the network. All the simulations have been carried out in NS-2 software and the performance in term of packet delivery ratio, throughput, less end-to-end delay have been compared with the LEACH protocol and find that the proposed algorithms perform better.

V. Kumar et al., 2014 [31], has proposed some of the security goal for Wireless Sensor Network. Further, as security being vital to the acceptance and use of sensor networks for many applications; author have made an in depth threat analysis of Wireless Sensor Network. Lastly it proposed some security mechanisms against these threats in Wireless Sensor Network.

Deepali et al., 2014 [21], proposed that the security of a wireless sensor network was compromised because of the random deployment of sensor nodes in open environment, memory limitations, power limitations and unattended nature. This paper focused on various attacks that manifest in the network and provides a tabular representation of the attacks, their effects and severity. The paper presented a comparison of attacks basis packet loss and packet corruption. Also, the paper discussed the known defense mechanisms and countermeasures against the attacks.

Marigowald et al., 2013 [30], has provided comprehensive information on types of attacks WSN was exposed to and possible methods of countering such attacks effectively. The motto of the paper was to help novice researchers with objective to work on security challenges in Wireless Sensor Network environment.

Saoucene Mahfoudh et al., 2003 [7], have shown how the standardized OLSR routing protocol can be extended to make it energy efficient. By considering residual node energy, three novel selection algorithms of multipoint relays, dependent on minimum residual energy has been executed and the best one was chosen. This OLSR extension selected the path lessening the energy being consumed in the end-to-end transmission of flow packet and avoids nodes having less residual energy. The author has compared this extension with two-path source routing strategy. The evaluation has shown that this energy efficient extension maximize network lifetime as well as user data delivered.

Tiago Camilo et al. 2006 [16], proposed the Energy Efficient Ant Based Routing Algorithm for WSNs (EEABR), taking into account and ACO Meta heuristic, was another proposed burrowing little creature based calculation to expand the lifetime of WSNs. The calculation utilized a decent technique considering vitality levels of the hubs and the lengths of the steered ways.

Zhang et al., 2004 [15] proposed burrowing little creature based calculations for WSNs; their study incorporates three steering calculations named Sensor-driven and Cost-aware ant routing (SC), Flooded Forward ant (FF), and Flooded piggybacked ant routing (FP). The calculations are fruitful with starting pheromone settings to have a decent framework start-up; however the SC and FF calculations are not exactly powerful in dormancy, while giving better vitality proficiency. Plus, the FP calculation, while giving high achievement rates of information conveyance, devours much higher vitality than the FC and FF calculations.

Raja Wassem et al., 2014 [9], presented that security is a fundamental requirement for these networks. In this research, the centre of attention was on physical attacks and issues in wireless sensor networks. The purpose of this research was to identify the attackers. Further, well-known approaches of security detection against physical attacks have been discussed.

VI. PROBLEM STATEMENT

Security is an essential service in wireless sensor network. WSN brings new challenges to the security of the network. Due to their unique characteristics, they are prone to various types of attacks. Securing network protocol requires detailed analysis of the network protocol. WSN is the challenging area from number of years for its network security problem. However, this feature provides various challenges as well as opportunities in achieving security goals. In the proposed work, we will discuss gray hole attack on the widely used OLSR routing protocol. Routing protocols are necessary to communicate with each other, so this work will utilise OLSR protocol. It has noticed from literature survey that computational methods are good for provision of accuracy; therefore, usage of fuzzy logic along with ABC method will be done with the comparison of with Fuzzy+ABC and without Fuzzy+ABC. The work will be evaluated using number of network parameters as defined below;

- **Throughput**

Throughput is defined as the total number of packets transmitted n the whole simulation time. Mathematically, it is defined as:

\[
\text{Throughput} = \frac{\sum \text{Packet sent}}{\text{Total data packets}}
\]

- **End to end delay**

The average time taken by data packet to reach the destination and includes all delays caused by buffering during route discovery latency, queuing at the interface queue. Mathematically, it can be defined as:

\[
\text{Avg. EED} = \frac{S}{N}
\]

S is the amount of the time spent to bring packet for each destination, and N is the number of packets received by the all destination nodes.

- **Bit error rate**

Bit Error rate (BER) is defined as the number of bits per unit time. It is the division of bit errors by the total number of transferred bits during time interval. It is often defined in the form of percentage and it is a measure of unit less performance.
• **Energy consumption**

Energy consumption is defined as the energy consumed by the whole routing process at different instants of time. It is obtained by energy consumed summation in every operation mode during simulation time. It is defined mathematically as below:

\[
\text{Energy Consumption} = \sum_{i=0}^{n-1} (\text{Energy consumed by node}(i))
\]

### VII. METHODOLOGY USED

**Step 1**: Start

**Step 2**: Initialize The Network With Various No. Of Nodes.

**Step 3**: Enter Width And Length Of Network To Implement Network.

**Step 4**: Calculation Of X And Y Location Of Nodes

**Step 5**: Deployment Of Sensor Nodes In Network

**Step 6**: Plotting Of Source And Destination

**Step 7**: Find Coverage Set, And Then Find Distance Between Nodes.

**Step 8**: Define Rule Sets For Fuzzy Logic To Find Out The Routs.

**Step 9**: Optimize The Rule Sets Using ABC Optimizer To Find Attackers Based On The Analysis Of QOS Parameters.

**Step 10**: If Attackers Are Founded Then Call The ABC To Discover The Route Which Provides The Best Optimal Results.

**Step 11**: Calculate The QOS Performance Metrics Like Throughput, Delay Rate, Bit Error Rate And Energy Consumption.

**Step 12**: End
RESULT AND DISCUSSION

Table I Network Requirements

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>50-100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>1000-1000 meters</td>
</tr>
<tr>
<td>Simulation Tool</td>
<td>MATLAB</td>
</tr>
<tr>
<td>Evaluation Parameter</td>
<td>Throughput, Delay, BER, Energy Consumption</td>
</tr>
</tbody>
</table>

The network area of the existing work in wireless sensor network consists of area 1000× 1000 having 50 numbers of nodes to run the network. The network is run for five times that means five iterations have been applied so that best results can be obtained.

As it is depicted in the above figure that the black colour line indicates the throughput values obtained from the wireless sensor network without optimization i.e. when LEACH protocol is used to find the route to reach the packet at the destination node. Whereas the blue line indicates the throughput values obtained for the wireless sensor network with optimization i.e. ABC and fuzzy logic is used to find the accurate path and the packet has to reach at exact destination. The process is repeated five times so that we can get accurate results. Thus, the maximum throughput values obtained for the network without optimization is 83202.4885 whereas the throughput values obtained for network with ABC and Fuzzy is 86348.1575.

Table II Comparison of throughput for existing and proposed work

<table>
<thead>
<tr>
<th>Number of rounds</th>
<th>Existing work LEACH (without optimization)</th>
<th>Proposed work (ABC+FUZZY with optimization)</th>
<th>OLSR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4.8</td>
<td>5.2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4.7</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>8.3</td>
<td>8.6</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>5.8</td>
<td>6.2</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>7.8</td>
<td>8.2</td>
<td></td>
</tr>
</tbody>
</table>

The network area of the existing work

![Fig. 5 Network area of the existing work](image)

![Fig. 6 Throughput for existing and proposed work](image)
Table III comparison of delay for existing work with proposed

<table>
<thead>
<tr>
<th>Number of rounds</th>
<th>Existing work LEACH (without optimization)</th>
<th>Proposed work OLSR (ABC+FUZZY with optimization)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>-8</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>-10</td>
</tr>
<tr>
<td>3</td>
<td>20</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>1</td>
</tr>
</tbody>
</table>

Fig. 7 Delay for existing and proposed work

The average values obtained for the existing work without ABC-Fuzzy and for proposed work with ABC-FUZZY are 19.892 and 7.3896 respectively. When we compare these values with the proposed work the average value obtained with LEACH protocol is 20.2353 and with optimization it gets reduced and we obtained average delay of 0.70394, which is very much less than the existing work.

Table IV comparison of BER for existing work and proposed work

<table>
<thead>
<tr>
<th>Number of rounds</th>
<th>Existing work LEACH (without optimization)</th>
<th>Proposed work OLSR (ABC+FUZZY with optimization)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>16.1</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>15.9</td>
<td>15.8</td>
</tr>
<tr>
<td>3</td>
<td>16.2</td>
<td>16.1</td>
</tr>
<tr>
<td>4</td>
<td>14.8</td>
<td>14.8</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Fig. 8 BER for existing and proposed work
The average value of bit error rate (BER) obtained for the existing work with LEACH protocol is 16.2101 and with OLSR (ABC-Fuzzy) the average value gets decreased and become 16.1861. It get decreased because with the OLSR protocol the BER obtained get optimized by using ABC optimization algorithm and for classification Fuzzy logic is used. Whereas, the average value obtained for the proposed work for with and without optimization algorithm are 16.7424 and 11.5814 respectively.

Table V Comparison of Energy Consumption for existing and Proposed work

<table>
<thead>
<tr>
<th>Number of rounds</th>
<th>Existing work LEACH (without optimization)</th>
<th>Proposed work OLSR (ABC+FUZZY with optimization)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>16.1</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>15.9</td>
<td>15.8</td>
</tr>
<tr>
<td>3</td>
<td>16.2</td>
<td>16.1</td>
</tr>
<tr>
<td>4</td>
<td>14.8</td>
<td>14.8</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Form the above graph, it is concluded that more energy is consumed without ABC+Fuzzy algorithm that is for the previous work than the ABC + fuzzy algorithm being applied to the network as we have proposed. Without optimization, the energy consumption is 121.168 whereas; with optimization the energy consumption is 109.2157 which is less as compared to without optimization.

IX. CONCLUSION

Wireless Sensor Network is quiet unsafe as well as susceptible to numerous attacks so it is required, a dependable, proficient as well as a protected protocol which can be able to quickly organized and also utilizes dynamic routing technique. OLSR is prone to countless attacks similar to alteration in the sequence quantities or hop counts, source route channelling, spoofing in addition to construction in the error messages. Gray hole attack is an actual threat in contradiction of OLSR protocol in wireless sensor network. Gray hole attack knows how to be certainly launched even in network grids that is available confidentiality in addition to authenticity. The malicious nodes generally target the routing controller messages interrelated to routing data.

In this research, we have analysed the effect of Gray Hole in the network. For this purpose, we have used an OLSR routing protocol. For analysing, fuzzy set and ABC are used as a classifier. It works on the basis of rule sets which can help to find whether the attack is present or not. Through fuzzy logic technique, the rules are being set as per OLSR routing protocol. The simulation has been executed using the MATLAB. The simulation results has shown that when the gray hole node exists in the network, the performance of the network is being affected and decreased and can be optimized by using ABC algorithm with fuzzy rule sets. In the proposed work, throughput value (99018.1835), delay (7.38 msec), BER (16.18) and energy consumption (89.9357) are obtained when optimization is being used.

REFERENCES


Singh et al., International Journal of Advanced Research in Computer Science and Software Engineering 7(8) ISSN(E): 2277-128X, ISSN(P): 2277-6451, DOI: 10.23956/ijarcsse/V7I8/0128, pp. 1-9


