Simulating Fruit Fly Optimization Algorithm in Calculation of Energy Cost with respect to Multipath Routing for Node Capture Attack in WSN

Ruby Bhatt, Priti Maheshwary, Piyush Shukla

Abstract: The concept of ‘Smart’ has made sensors very much prominent in one’s life. In this smart world, Wireless sensor network (WSN) [1] is another area of interest. There are good side and bad side of coin when dealt with WSN. Good side of WSN has made its presence felt in various areas but bad side has made it susceptible to different types of physical attacks. It is collection of tiny sized sensor nodes. And the tiny sensor nodes have limited resource capacity. It is screened to external atmosphere for circulating data. But, due to its mobile nature, nodes are susceptible for many types of attacks. Node capture attack is supposed to be severe attack in WSN [2]. In this type, the node is substantially captured by an assailant and eradicates the secret information from the node’s storage. This paper proposes a Fruit Fly Optimization Algorithm (FFOA) [13]. It is based on multiple objectives [4] node capture attack algorithm. Proposed algorithm serves these objectives: maximum node contribution [4], maximum key contribution [4], and least resource expenses. Routing can be single path or it may be multipath. The simulation result illustrates that FFOA obtains a lower energy cost and lower attacking rounds as compared with matrix algorithm (MA) [5] and other node capture attack algorithms for multipath routing.

Keywords: Vertex, Seizure, Fruit Fly, Optimization, Capture, Vulnerable.

I. INTRODUCTION

Sensor technology has ascertained expedient in several applications, like, catastrophic, health and defense monitoring. But, sensor networks are highly prone to node capture attack because of its exposed nature. It is a practically imitative and inclusive attack in which opponent physically seizes the node by excerpting cryptographic keys [5] and confidential information. Node seizure [5] is the most incommodeous problem that ventures the discretion, consistency, and protection of sensor nodes.

In this technology, the intruder arbitrarily compromises the node to create destruction in the communication of nodes in WSN. In susceptibility assessment theory, an intruder used to choose anode smartly to cooperate the whole network using susceptibility metric [6]. To surmount the difficulties of susceptibility based approaches the node capture attack approach is developed by combining multiple objectives like large amount of node contribution, highest key contribution, and least resource expenses to discover an optimal node using Fruit Fly Optimization Algorithm (FFOA) [13]. Using this algorithm, the attacker makes the attack more powerful. It works so efficiently that cost of attack also considerably reduced.

II. LITERATURE REVIEW

Several researchers have described numerous modelling node capture techniques using vulnerability evaluation [4], epidemic theory and probabilistic analysis [4]. The intruders smartly captures sensor nodes and removes the keys from their storage to devastate the protection, consistency and secrecy of the WSN. Matrix Algorithm (MA) [4] which is matrix-based node capture attack is projected to stipulate nodes and paths correlation along with maximum destructiveness and least resource expenditure. The results represent that the MA [5] can decrease the rounds used for confronting and time required for accomplishment with the increase in the confronting competence and energy cost [4]. Greedy node captured based on route minimum key set (GNRMK) [16] was designed to find the route minimum set. It was calculated by the maximum flow of the network. The overlapping value was allocated to each node on the foundation of route minimum key set. Thenode with maximum overlapping value was captured in every round of attack. Results of simulation revealed that, compared with other node capture attack schemes, GNRMK [16] could conceal the network. Because of the pseudo random key pre-distribution scheme and convoluted network design, Minimum Resource Expenditure node capture Attack (MREA) [6] was developed. It was a heuristic method. It was used to minimize energy cost along with maximum destructiveness for node capture attacks.

III. MODELS

The whole process is completed by applying the four models. These models define the pathway to describe the whole implementation part.

1.1. Network Model

Wireless sensor network is created using this network model. This model [4] is represented by directed network graph $G = (N, L)$, where $N$ is the nodes number and $L$ is the links number.
1.2. Key Predistribution Model

In WSN, the cryptographic keys [4] represent a key group set K and every sensor node \( N_a \) belongs to N is randomly assigned a subset of keys \( K_a \) is subset from K from a key group set. Two nodes \( N_a \) and \( N_b \), which share a set of keys \( K_{a,b} = K_a \cap K_b \).

1.3. Link Model

In WSN, several links are controlled by the paths and routes. A link \( L_{a,b} \) is a consistent and protected if it is encoded by key.

1.4. Adversary Model

This model is described from the view of an attacker’s [4] and it is supposed that the intruder has latent to spy on the information transmitting through the WSN [2].


Pacification of the whole network comes in the major task. Different routes, which contain multiple paths, are therefore confined for compromising the complete network. The following matrices are calculated:

4.1. Key-Route Matrix

This matrix gives the relationship between the keys that are attached with every sensor node and the different routes that connect source node to the destination node.

\[
KR = \left[ K_{KR_{a,b}} \right]_{N \times R} \text{, where:}
\]

\[
K_{KR_{a,b}} = \begin{cases} 
1, & \text{if } K_a \text{ cooperate } N_b \\
0, & \text{otherwise}
\end{cases} 
\]  

(1)

4.2. Vertex (Sensor Node)-Key Matrix

This matrix gives the relationship between the keys that are attached with every sensor node. Each node can have any number of associated keys. It can start from 2 keys to 3 keys or to any ‘n’ number of keys.

\[
VK = \left[ VK_{a,b} \right] \text{, where:}
\]

\[
VK_{a,b} = \begin{cases} 
1, & \text{if } K_a \in N_b \\
0, & \text{otherwise}
\end{cases} 
\]  

(2)

4.3. Key-Number Matrix

This matrix gives the relationship between the keys that are attached with every sensor node. The keys number matrix is exclusive system to take care of various key combinations in the whole network.

\[
KN = \left[ KN_{b} \right] = \sum_{a=1}^{x} VK_{a,b}, \text{ if few nodes } \in N_b \\
0, \text{ otherwise}
\]  

(3)

4.4. Vertex (Sensor Node)-Route Matrix

This matrix gives the relationship between the sensor node and the different routes that connect source node to the destination node. This is very interesting matrix as it caters for two conditions:

(i) Single Path Routing
(ii) Multi Path Routing

Where \( VR = VK \ast KR \), is considered for single path routing.

To evaluate on the partially cooperation relationship between nodes [12] and the routes, in case of Multi path routing, we calculate another matrix,

\[
VLR = \left[ VLR_{b,a} \right]_{N \times R} \]  

(4)

We combine the values of these two matrices into a single matrix \( MM = \left[ MM_{b,a} \right]_{N \times R} \) as:

\[
MM = \beta \times VR + (1 - \beta) \times VLR 
\]  

(5)

Where \( \beta \) is a parameter decided from (0, 1);

\[
MM_{b,a} = \sum_{a=1}^{N} MM_{b,a}, \text{ Participation of Node } N_b \\
0, \text{ Otherwise} 
\]  

(6)

4.5. Cost Seizing Matrix

The Cost seizing matrix \( CS = \left[ CS_{b,a} \right]_{N \times R} \) is denoted as follows:

\[
CS_{b,a} = \frac{MM_{b,a}}{W_b} 
\]  

(7)

Where, \( W_b \) is the seizing cost of compromising

\[
CS_{b,a} = \sum_{a=1}^{N} CS_{b,a}, \text{ Seizing Cost of Node } N_b \\
0, \text{ Otherwise} 
\]  

(8)

\( CS_{b,a} \) shows the resource expenses for vertex \( N_b \).

4.6. Multi Objective Function

The multi objective function is denoted as follows:

\[
F = \sum_{b=1}^{N} \sum_{a=1}^{R} \left[ \frac{1}{MM_{b,a}} + \frac{1}{KN_{b}} + CS_{b,a} \right] 
\]  

(9)

4.7. Fruit Fly Optimization Algorithm (FFOA)

After estimating multi objective function, FFOA [4] is instigated. It discover optimal vertex (sensor nodes) [1] from the existing vertex, which minimize the objective function [4] to generate the best results. In order to discover the optimal nodes [4], that causes extreme ferocity in WSN [1] using FFOA [13].

**Start**

Step1. Initialize population, generation, function, position and smell of each vertex (sensor node).

Step2. Compute the fitness of each vertex based on distance and smell and geographic coordinates.

Step3. Update position and best index of each vertex.
Step 4. Find optimal solution, if not, repeat step 2. If found the optimal solution gives nodes ID’s.

End

V. RESULT AND ANALYSIS

The performance of FFOA is analyzed on the basis of based multi objectives node capture attack algorithm is analyzed under following parameters listed in table 1.

Table 1: Experimental Specifications

<table>
<thead>
<tr>
<th>Bounds</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes Number</td>
<td>200</td>
</tr>
<tr>
<td>Size</td>
<td>100 * 100</td>
</tr>
<tr>
<td>Source Nodes</td>
<td>10</td>
</tr>
<tr>
<td>Range of Sensing</td>
<td>20</td>
</tr>
<tr>
<td>Destination Nodes</td>
<td>3</td>
</tr>
<tr>
<td>Keys Group</td>
<td>200</td>
</tr>
<tr>
<td>Allotted Keys to a Vertex</td>
<td>20</td>
</tr>
<tr>
<td>Population Size</td>
<td>50</td>
</tr>
<tr>
<td>Number of Rounds (Iterations)</td>
<td>200</td>
</tr>
</tbody>
</table>

During simulation, 200 vertices (sensor nodes) [1] are distributed in the WSN [1]. 10 nodes as source and 3 destination vertices are arbitrarily selected. Multi path routing protocol is used for communication between sensor vertices in the range of 20m. The proposed algorithm is analyzed for single path and run over 200 repetitions. We evaluate the recital of the FFOA in terms of energy cost and attacking rounds and then the results compared with an MA (matrix algorithm) and other node capture attack algorithms like Random Attack (RA) [4], Maximum Key Attack (MKA) [4], Maximum Traffic Attack (MTA) [4], Maximum Link Attack (MLA) [4], Greedy Node capture Approximation using Vulnerability Evaluation (GNAVE) [4].

5.1. Energy Cost

In this simulation, the energy consumption is analyzed. The energy cost of node capturing is distributed in $U(0, 1)$. Capturing cost of network is enhanced by enhancing the number of capturing nodes. It is therefore very obvious that MA [4] and other algorithms have higher energy cost than FFOA [13]. MA and other node capture attack algorithms uses greater number of nodes to compromise the whole network.

5.2. Attacking Rounds [4]

In this simulation [4], we calculate the number of rounds [4] (i.e. the number of vertex the intruders desires to capture [28] to conciliation the whole network) the intruders attack [16]. Fig. 2 illustrate the results in which x-coordinate shows the number of keys [4] for each node and the y-coordinate indicates the number of attacking rounds [4] of FFOA, MA [4] and other node capture attack [3] desires to attack to cooperation the network. Attacking rounds are directly dependent on the fraction of the compromised traffic so FFOA has lower attacking rounds than MA [4] and other node capture attack algorithms like Random Attack (RA) [4], Maximum Key Attack (MKA) [4], Maximum Traffic Attack (MTA) [4], Maximum Link Attack (MLA) [4], Greedy Node capture Approximation using Vulnerability Evaluation (GNAVE) [4]. Therefore, FFOA gives maximum attacking efficiency than MA and other algorithms by capturing minimum nodes that compromise the whole network.

VI. CONCLUSION

The proposed algorithm - Fruit Fly Optimization Algorithm (FFOA) [13] is initiated to increase the efficiency of attack using multi objective node capture attack in WSN [2]. FFOA describes three objectives: (1) maximum key contribution (2) least resource expenses, and (3) maximum node contribution to discover optimal nodes for overall devastation of network [4]. These nodes form the best combination of the objectives and create extreme harmfulness. The simulation result illustrates that FFOA obtains a lower attacking rounds, and lower energy cost as compared with a matrix algorithm (MA) [4] and other node capture attack algorithms like Random Attack (RA) [4], Maximum Key Attack (MKA) [4], Maximum Traffic Attack (MTA) [4], Maximum Link Attack (MLA) [4], Greedy Node capture Approximation using Vulnerability Evaluation (GNAVE) [4]. Therefore, FFOA gives maximum attacking efficiency than MA and other algorithms by capturing minimum nodes that compromise the whole network.
Simulating Fruit Fly Optimization Algorithm in Calculation of Energy Cost with respect to Multipath Routing for Node Capture Attack in WSN

REFERENCES


Piyush Kumar Shukla received his Bachelor’s degree in Electronics & Communication Engineering, LNCT, Bhopal in 2001, M. Tech (Computer Science & Engineering) in 2005 from SATI, Vidisha and Ph.D. (Computer Science & Engineering) in 2013 from RGPV, Bhopal. M.P. India. He is Member of ISTE (Life Member), IEEE, ACM, IACSIT, IAENG. Currently he is working as an Assistant Professor (Grade 8,000/-) in Department of Computer Science & Engineering, UIT-RGPV Bhopal. He is also IJC of PG Program (Dual Degree Integrated PG-Programs) in DoCSCE, UIT, RGPV, Bhopal, Madhya Pradesh. He has published more than 60 Research Papers in various International & National Journals & Conferences, including 04 papers in SCIJE Journals & more than 10 papers in Scopus Journals. He has also published an Indian patent. He is guiding 04 students in PhD Program and also has been awarded 02 candidates in PhD under his guidance.

Priti Maheshwary is an Associate Professor in Computer Science and Engineering department and Director, Centre of Excellence for IoT & Advanced Computing (CIoTAC) at Rabindranath Tagore University (Formerly known as AISECT University), Bhopal. She had her Doctorate from MANIT, Bhopal in Remote Sensing Image Retrieval. She has completed research project on Climate Change detection and monitoring funded by SAC and Environment Monitoring using Sensor devices funded by AISECT University. Ongoing Project is on Crop Monitoring sponsored by SAC. She is the author of more than 20 publications in different journals of repute out of which two journal papers and two conference papers on IoT. She is the author of book chapter on Software Copyright. Her interests include Internet of Things, Cyber Physical Systems, Mobile Networks, WSN, Adhoc Networks, Data mining, and Image Processing. Her work experience includes 20 years in teaching computer science and engineering. She is guiding PhD in the field of image processing, IoT and Networks.

Ruby Bhatti is a Research Scholar in Computer Science and Engineering Department at Rabindranath Tagore University (RNTU) (formerly known as Aisect University), Bhopal. She has completed her M. Phil. in Computer Science from Vikram University, Ujjain and M. Sc. in Computer Science from Rani Durgawati University, Jabalpur. She has mastered many programming languages, like C / C++, Java, HTML / CSS, JavaScript and high-performance language for technical calculation - MATLAB. Her area of interest includes Wireless Sensor Networks, Security Issues in Sensor Networks, Artificial Intelligence and Data Mining. She has been working on Fruit Fly Optimization Algorithm. She has attended many National and International Conferences and also has Research Paper Publication to her credit. She has authored two journal papers and two conference papers on Security Issues in Wireless Sensor Network and Optimization Techniques. She is a committed professional and her academic experience has a long journey of fifteen years in different colleges of Central India.