International Journal of Engineering &Technology, 8 (3) (2019) 142-145

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Instigating Fruit Fly Optimization for Node Capture Attack in calculating Energy Cost for Single Path Routing in Wireless Sensor Network

Ruby Bhatt [1] *, Priti Maheshwary [2], Piyush Shukla [3]

[1] *Resaerch Scholar, Department of CSE, Rabindranath Tagore University, Bhopal*
[2] *Associate Professor, Department of CSE, Rabindranath Tagore University, Bhopal*
[3] *Assistant Professor, Department of CSE, UIT, Bhopal 462023, India*
**Corresponding author E-mail: ruby_15@rediffmail.com*

Abstract

Wireless sensor network (WSN) [1]is susceptible to different types of physical attacks. It is collection of tiny sized sensor nodes. The reason behind that is its limited resource capacity. It is screened to external atmosphere for circulating data. Node capture attack is supposed to be severe attacks 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 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 [4]. The simulation result illustrates that FFOA obtains a maximum fraction of compromised traffic, lower attacking rounds, and lower energy cost as compared with matrix algorithm (MA) [5] and other node capture attack algorithms.

Keywords: *Vertex; Seizure; Fruit Fly; Optimization; Capturing; Vulnerable.*

1. Introduction

Sensor technology has evolved several applications, like, catastrophic, health and defense monitoring. Sensor networks are highly susceptible to node capture attack because of vulnerable nature. It is a practically imitative and inclusive attack in which opponent physically seizures the node by excerpting cryptographic keys [1] and confidential information. Node seizure [1] is the most incommodious problem that ventures the discretion, consistency, and protection of sensor nodes.

In these technologies, the intruders arbitrarily confine the node to cooperation in the communication of WSN. However, susceptibility assessment theory has been dignified whereby an intruder can choose a node smartly to cooperate the network using susceptibility metric [28].

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].

2. Literature review

Several researchers have described numerous modelling node capture techniques using vulnerability evaluation, epidemic theory and probabilistic analysis. The intruder 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 key set [16]. Itwas calculated by the maximum flow of the network. The overlapping value was allocated to each node on the foundation of route minimum key set. The node with maximum overlapping value was captured in every round of attack. Results of simulation reveled 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] is developed. Itis a heuristic method. It is used to minimize energy cost along with maximum destructiveness for node capture attack.

Copyright © 2019 Ruby Bhatt et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

3. Models used

3.1. Network model

Wireless sensor network model is represented by directed network graph G = (N, L), where N is the nodes number and L is the links number.

3.2. Key Predistribution model

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

3.3. 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.

3.4. Adversary model

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

4. FFOA[13] based multi objective node capture attack algorithm [4]

Pacificationof 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

KR=$\left[KR_{a,b}\right]_{K\times R}$, where:

$$KR_{a,b} = \begin{cases} 1 & If\ \ K_a\ \ can\ \ Cooperate\ \ P_b \\ 0 & Otherwise \end{cases} \tag{1}$$

4.2. Vertex (sensor node)-key matrix

$$VK_{b,a} = \begin{cases} 1 & If\ \ K_a \in N_b \\ 0 & Otherwise \end{cases} \tag{2}$$

4.3. Key-number matrix

$$KN_b = \begin{cases} \sum_{a=1}^{K} VK_{b,a} & If\ few\ keys\ belongs\ to\ node\ N_b \\ 0 & Otherwise \end{cases} \tag{3}$$

4.4. Vertex (sensor node) - route matrix

Where VR = VK * KR (4)

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

MM= β×VR+(1 −β)×VLR (5)

Where β is a parameter decided from (0, 1):

$$MM_b = \begin{cases} \sum_{a=1}^{R} MM_{b,a} & Parfticipation\ of\ \ Node\ \ N_b \\ 0 & \end{cases} \tag{6}$$

4.5. Cost seizing matrix

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

$$CS_{b,a} = \frac{MM_{b,a}}{W_b} \tag{7}$$

Where, W_b is the seizing cost of compromising N_b .

$$CS_b = \begin{cases} \sum_{a=1}^{R} CS_{b,a} & Seizing\ Cost\ of\ \ Node\ N_b \\ 0 \end{cases} \tag{8}$$

CS_b shows the resource expenses for vertex N_b .

4.6. Multi objective function

The multi objective function is denoted as follows:

$$F_b = \sum_{b=1}^{N} \sum_{a=1}^{R} \left\{ \frac{1}{MM_b} + \frac{1}{KN_b} + CS_b \right\} \tag{9}$$

4.7. Fruit fly optimization algorithm (FFOA)

After estimating multi objective function, FFOA 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 [14].
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 generate optimal value of individual and population.
Fitness = Function (Smell)
Step3. Update position and best index of each vertex.
Step4. Find optimal solution, if not, repeat step2.
If found the optimal solution gives nodes ID`s.
End

5. Results and analysis

The performance of FFOA is analyzed om the basis of based multi objectives node capture attack algorithm is analyzed under following parameters listed in table 3.

Table 1: Experimental Specifications

Bounds	Standards
Vertices (Sensor Nodes)[1] Number	200
Region Size	100 * 100
Source Vertices Numbers	10
Range of Sensing	20
Destination Vertices Digits	3
Group of Keys	200
Allotted Keys to a Vertex	20
Sender and Receiver Vertices	R
Population Size	50
Number of Rounds (Iterations)	200

During simulation, 200 vertices (sensor nodes)[1] are distributed in the WSN[1]. 10nodes as source and 3 destination vertices are arbitrarily selected. Single path routing protocol issued 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 fraction of compromised traffic, energy cost, attacking rounds and execution time and compare the results with an MA (matrix algorithm) and other node capture attack algorithms like Random Attack (RA) [42], Maximum Key Attack (MKA)[14], Maximum Traffic Attack (MTA)[14], Maximum Link Attack (MLA)[14], Greedy Node capture Approximation using Vulnerability Evaluation (GNAVE) [14].

5.1. Energy cost

In this simulation, the energy consumption is analyzed. The energy cost of node capturing is distributed inU(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.

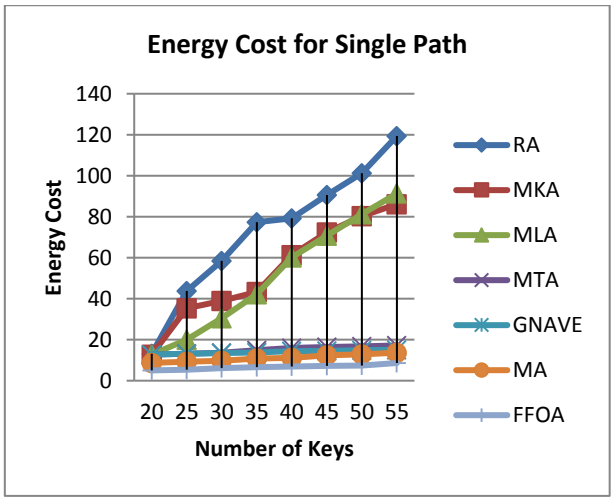


Fig. 1: Energy Cost for Single Pathrouting Protocol.

6. 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. These nodes form the best combination of the objectives and create extreme harmfulness. The simulation result illustrates that FFOA obtains a maximum fraction of compromised traffic, lower attacking rounds, and lower energy cost compared with a matrix algorithm (MA) [4] and other node capture attack algorithms. Therefore, FFOA gives maximum attacking efficiency than MA and other algorithms by capturing minimum nodes that compromise the whole network.

References

[1] Amandeep Kaur and Sandeep Singh Kang, "Attacks in Wireless Sensor Network- A Review", International Journal of Computer Sciences and Engineering, IJCSE, Vol. 6, Issue 4, pp-157-162, 2016.
[2] BhavanaButani, Piyush Kumar Shukla, and Sanjay Silakari, "An Exhaustive Survey on Physical Node Capture Attack in WSN",International Journal of Computer Applications, IJCA, Volume 95, No.3, pp-32-39, 2014. https://doi.org/10.5120/16577-6265.
[3] Bhoopathy V. and R.M.S. Parvathi, "Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks", International Journal of Engineering Research and Applications, IJERA, Vol. 2, Issue 2, pp-466-474, 2012.
[4] Chi Lin andGuoweiWu, "Enhancing the attacking efficiency of the node captureattack in WSN: a matrix approach", J Supercomput, Springer Science &Business Media, pp-1-19, 2013.
[5] Chi Lin, Guowei Wu, Chang Wu Yu, and Lin Yao, "Maximizing destructiveness of node capture attack in wireless sensor networks", J Supercomput, Springer Science & Business Media, Vol. 71, pp-3181–3212, 2015. https://doi.org/10.1007/s11227-015-1435-7.
[6] Chi Lin, Tie Qiu, Mohammad S. Obaidat, Chang Wu Yu, Lin Yao and Guowei Wu, "MREA: a minimum resource expenditure node capture attack in wireless sensor networks", Security and Communication Networks, Wiley Online Library, Vol. 9, pp-5502–5517, 2016. https://doi.org/10.1002/sec.1713.
[7] Chuiwei Lu, and Defa Hu, "A Fault-Tolerant Routing Algorithm for Wireless SensorNetworks Based on the Structured Directional de Bruijn Graph", Cybernetics and Information Technologies, Bulgarian Academy Of Sciences, Volume 16, No 2, pp-46-59, 2016. https://doi.org/10.1515/cait-2016-0019.
[8] Daehee Kim, Dongwan Kim, and Sunshin An, "Source Authentication for Code Dissemination Supporting Dynamic Packet Size in Wireless Sensor Networks", Sensors, MDPI, Vol. 16, pp-1 -22, 2016. https://doi.org/10.3390/s16071063.
[9] Daehee Kim, Dongwan Kim and SunshinAn, "Communication Pattern Based Key Establishment Scheme in Heterogeneous Wireless Sensor Networks", KSII Transactions on Internet and Information Systems, Vol. 10, No. 3, pp-1249-1272, 2016. https://doi.org/10.3837/tiis.2016.03.017.
[10] Harpreet Kaur, "Node Replication attack detection using Dydog in Clustered sensor network", Computer Science and Engineering Department, Thapar University Patiala, pp-1-71, 2017.
[11] I. QasemzadehKolagar, H. Haj SeyyedJavadi, and M. Anzani, "Hypercube Bivariate-Based Key Management for Wireless Sensor Networks", Journal of Sciences, Islamic Republic of Iran, University of Tehran, Vol. 28, No. 3, pp-273 – 285, 2017.
[12] R. Vijayarajeswari, A. Rajivkannan and J. Santosh, "Survey Of Malicious Node Detection In Wireless Sensor Networks", International Journal of Emerging Technology and Innovative Engineering, Volume 2, Issue 6, pp-335-338, 2016.
[13] Ze Wang, Chang Zhou, and Yiran Liu, "Efficient Hybrid Detection of Node ReplicationAttacks in Mobile Sensor Networks", Hindawi, Mobile Information Systems, pp-1-14, 2017. https://doi.org/10.1155/2017/8636379.
[14] Xiao C., Hao K., Ding Y., "An Improved Fruit Fly Optimization Algorithm Inspired from Cell Communication Mechanism", Hindawi Corporation, 2017.
[15] Tague P., "Identifying, modeling, and mitigating attacks in wireless adhoc and sensor networks".
[16] W. Guowei, C. Xiaojie, S. Mohammad and L. Chi, "A high efficient node capture attack algorithm in wireless sensor network based on route minimum key set".