Particle Swam Optimization Based Technique for Node Capture Attack in Wireless Sensor Network

Ruby Bhatt[1], Priti Maheshwary[2], Piyush Shukla[3]
[1]Choithram College of Professional Studies, Indore (M.P.) India.
[2]Department of CSE, AISECT, University, Bhopal (M.P.) India.
[3]Department of CSE, UIT, Bhopal (M.P.) India.

ABSTRACT
To improve the attacking efficiency of node capture attack, we designed a Node Capture Attack Algorithm based on Particle Swarm Optimization (NCPSO). NCPSO takes multiple objectives into consideration, that are: Maximum Node Participation, Maximum Key Participation and Minimum Resource Expenditure to find a set of optimal nodes using PSO that satisfies all the objectives, destroys maximum portion of the network and provides higher attacking efficiency at least attacking cost. The simulation results manifest that NCPSO can provide reduced attacking cost (resource expenditure) than Matrix Algorithm (MA) so the attacking efficiency of NCPSO is considerably improved

Keywords: Attacking Cost, Attacking Efficiency, Node Capture Attack, Particle Swarm Optimization, Wireless Sensor Network.

I INTRODUCTION

It has been observed that Node capture attack [1] is one of the hazardous attacks in the wireless sensor network (WSN) [2], and cannot be avoided in normal circumstances. In this attack, an adversary gains complete control over a sensor node by a direct physical access, and then the adversary can easily extract cryptographic information stored on the memory chip of the captured node using an antithesis engineering process to get to eavesdrop on the transmission of messages between the sensor nodes to destruction of the entire WSN [3]. Investigating the way of mounting an attack to break the security of the wireless sensor network provides deep insights for developing the countermeasures against the node capture attack.

II PROBLEM DEFINITION & PROPOSED WORK

As the node capture attack [4] suffers from the low attacking efficiency [5] and high resource expenditure, to overcome these problems, various vulnerability evaluation techniques have been developed, and also so many are under process. The aim of the node capture attack is to capture [9] a number of nodes to compromise the different routes of the network. To compromise distinctive routes of the sensor network, all the paths belonging to that route must be compromised. So, the attacker's aim is to compromise maximum possible routes of the network by capturing a set of nodes that satisfy multiple objectives that are maximum node participation in the network through which maximum packets transmitted in the network can be captured by minimum resource expenditure [10] and maximum keys.

III MODELS AND DEFINITIONS

This section includes the proposed models and various definitions related to our work Table 1 summarizes the related symbols and their definitions.

Table 1
A summary of related symbols and their Definitions

Symbols	Description
N	Set of sensor nodes in the network
Ni	ith sensor node
K	Set of total keys in the key pool
Ki	Set of keys acquired by node ni
L	Set of links between nodes
l (i, j)	Link between node ni and nj
S, D	Set of source and destination nodes
SR	Set of routes in the network
rs,d	A Route from source node s and destination node d
Wi	Capturing cost of Node ni
Cn	Set of Compromised Nodes
P(Ri)	Total number of paths of route Ri
Pk (i, j)	Number of paths in which node nj participates in route Ri
Fi	Objective function for node ni

IV PARTICLE SWARM OPTIMIZATION

Particle swarm optimization is a population-based computational technique. It learns from the scenario and uses it to find a potential solution for an optimization problem. PSO is initiated with a group of random particles and looks for an optimum value by updating generations.

In each round, each particle is updated by tracking two best values: first, one is the pbest (personal best) value. This is the value of the fitness function it has achieved so far. Another one is called the gbest (global best). This value is the best value obtained so far by any particle in the population and tracked by the particle swarm optimizer. After finding pbest and gbest, the particles update its velocity and position with the following equations:

v [ ] = v [ ]+ c1*rand( )*(pbest[ ] – p[ ]) + c2* rand ( )* (gbest[ ] – p[ ])

p [ ] = p[ ] + v[ ]

Where, v [ ] represents the particle velocity, p [ ] is the current position of the particle, rand is the random number between 0 to 1 and c1, c2 are learning factors.

The basic procedure of the PSO algorithm is as follows:

Step 1: Initialize the position and velocity of all particles.

Step 2: Evaluate the fitness of each particle according to the desired optimization. So the optimal value of individuals (pbest) and optimal value of swarm (gbest) can be obtained.

Step 3: Update the velocity and position of the particles.

Step 4: Determining whether the condition meets ends, if not, goto step 2 [20].

V NODE CAPTURE ATTACK ALGORITHM BASED ON PSO (NCPSO) & SIMULATION PARAMETERS

The projected algorithm estimates the optimal nodes for the node capture attack using PSO such as only a limited number of nodes capturing compromises the whole network by providing maximum benefits to an attacker.

To analyze the participation of sensor nodes in the network, we can calculate the Route Node Participation Matrix, which represents the participation of each sensor node in each route through the network at fig. 1, Simulation parameters are tabulated at Table 2

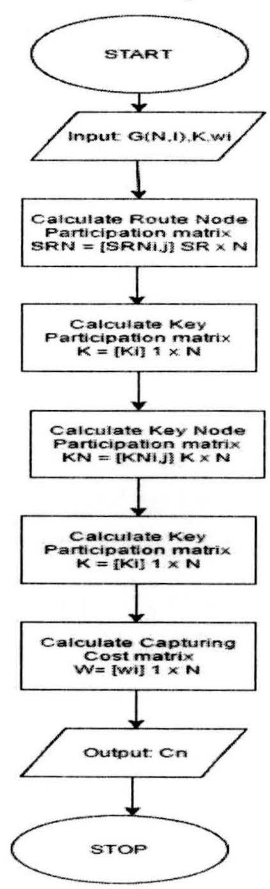

Fig. 1: Node Capture Attack Algorithm: NCPSO

Table 2
Simulation Parameters

S.No	Parameter	Value	Meaning
1.	N	200	The number of sensor nodes
2.	S	5	Number of source nodes
3.	D	3	Number of destination nodes
4.	Region Size	100*100	Region Size of the Sensor network
5.	Sensing Range	20	Maximum Transmission range of the senor network
6.	Key pool Size	20	The Key pool Size of the sensor nodes

VI SIMULATION BASED RESULTS & ANALYSIS

To analyze the performance of multiple objectives based node capture attack algorithm, we performed the following simulation. The experimental parameters are shown in the table 2. In the simulation work, 200 nodes are deployed throughout the sensor network. From the total deployed nodes, 5 source sensor nodes and 3 destination nodes are randomly selected. Random key pre-distribution scheme is used to assign keys to different nodes in the sensor network. Keys are assigned randomly from a key pool to each sensor node, when the network is deployed. Key distribution probability is 0.5 that show that number of keys assigned to each sensor node should be less than 50 % of the total keys in the key pool.

(a) Attacking Cost (Resource Expenditure)
In this experiment, we evaluate attacking cost or resource expenditure of each algorithm in compromising the network. If the adversary captures more nodes, the more will be resource expenditure due to utilization of the higher number of resources.

$$\textbf{Attacking Cost (Resource Expenditure)} = \sum_{i=0}^{n} wi$$

(b) Single Path Routing:

Table 3
Attacking Cost Vs. Number of Nodes Captured for Single Path Routing

Number of Nodes Captured	Attacking Cost	
	NCPSO	MA
2	0.8925	1.7261
4	1.5972	3.608
6	1.9417	4.9223
8	2.99	6.984
10	4.9633	8.62

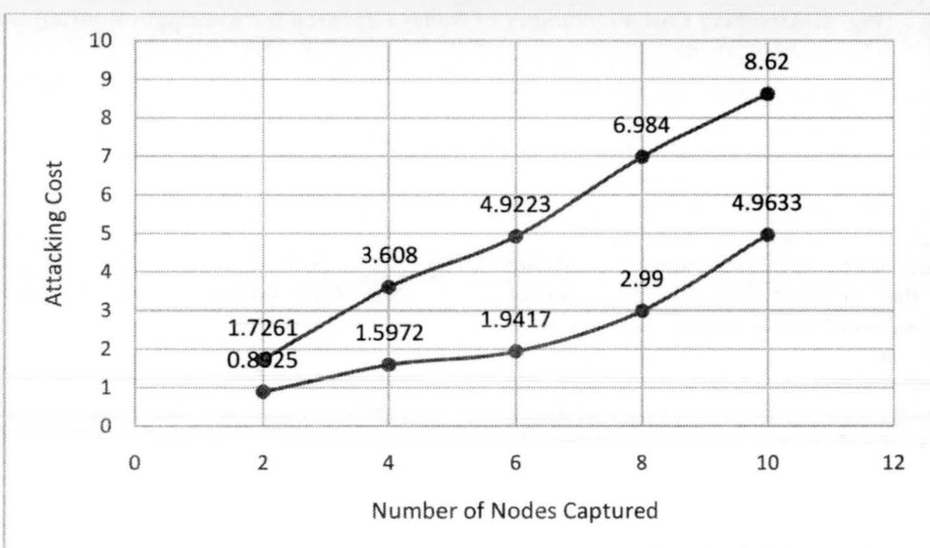

Fig. 1: Attacking Cost Vs Number of Nodes Captured for Single Path Routing

Figure 2 illustrates the comparison of NCPSO with MA in case of single path routing as the number of nodes captured varies from 0 to 10. At 4 captured nodes in the simulation, the Attacking Cost or Resource Expenditure for NCPSO is 1.5972 whereas the MA has been attacking cost 3.608. Our approach consumes less resource expenditure than MA. It manifest that attacking cost of NCPSO based technique is lowest. This is due to capture of the minimum number of nodes to compromise the network. Other Algorithms like MA takes comparatively more attacking cost due to the higher number of attacking rounds to compromise the network.

(c) Multipath Routing:

Table 5

Attacking Cost Vs. Number of Nodes Captured for Multipath Routing

Number of Nodes Captured	Attacking Cost	
	NCPSO	MA
2	1.2284	1.8517
4	1.9330	3.6301
6	3.5223	5.1599
8	5.2977	6.5614
10	6.4789	8.8501

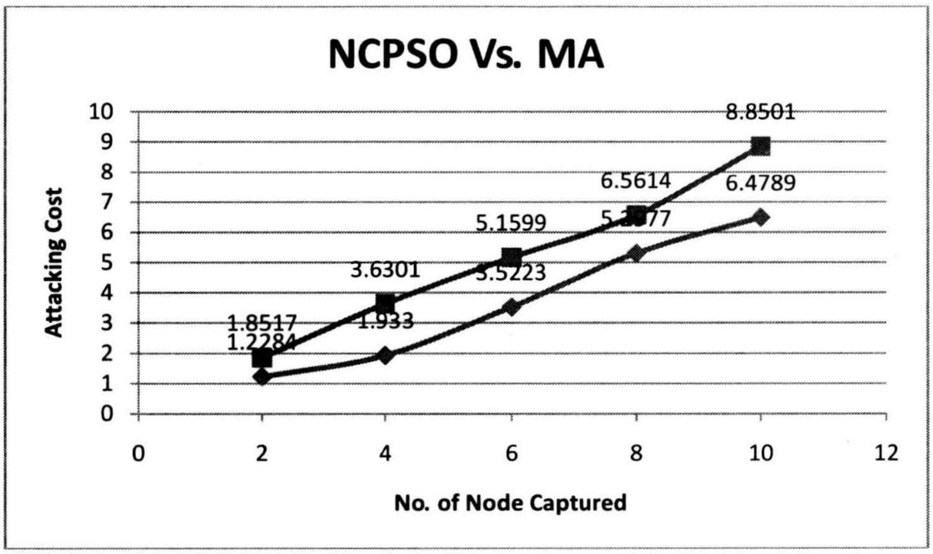

Fig. 2: Attacking Cost Vs. Number of Nodes Captured for Multipath Routing

Figure 3 shows the comparison of NCPSO with MA in case of multipath routing as the number of nodes captured varies from 0 to 10. When 4 nodes are captured in the simulation, the Attacking Cost or Resource Expenditure for NCPSO is 1.9330 whereas the MA has been attacking cost 3.6301. Our approach consumes less resource expenditure than MA that manifest that attacking cost of NCPSO based technique is lowest. This is due to capture of the minimum number of nodes to compromise the network. Other Algorithms like MA takes comparatively more attacking cost due to the higher number of attacking rounds to compromise the network.

VII CONCLUSION

Here to enhance the attacking efficiency of the node capture attack in the sensor network, a technique have been proposed based on multiple objective's node capture attack algorithms

(NCPSO) it has been designed for random key pre-distribution in the wireless sensor network.

NCPSO takes three objectives into consideration to capture a node that are maximum node participation, maximum key participation and minimum resource expenditure. NCPSO provides higher attacking efficiency than MA by capturing a limited number of nodes that compromise whole network.

REFERENCES

[1] Tague, P. & Poovendran, R. "Modeling adaptive node capture attacks in multi-hop wireless net-works", Ad Hoc Network, vol.5, No. 6, 2007, pp. 801–814.

[2] Tague P, Poovendran R, "Modeling node capture attacks in wireless sensor networks", In: Proc 46th annual Allerton conference on communication, control, and computing, 2008, pp. 1221–1224.

[3] Tague P, Slater D, Rogers J, Poovendran R, "Vulnerability of network traffic under node capture attacks using circuit theoretic analysis", In: Proc IEEE 28th international conference on computer communications, 2009, pp. 161–165.

[4] Wu, G., Chen, X., Obaidat, M.S., Lin, C., "A high efficient node capture attack algorithm in wireless sensor network based on route minimum key set", In Security And Communication Network, vol. 6, 2012, pp. 230-238.

[5] Chi Lin, GW, Enhancing the attacking efficiency of the node capture attack in wsn: a matrix approach, J Supercomput, 2013.

[6] Chi Lin, Guowei Wu, Feng Xia, Lin Yao, Enhancing Efficiency of Node Compromise Attacks in Vehicular Ad-hoc Networks Using Connected Dominating Set, Mobile Networks and Applications, vol. 18, No.6, 2013, pp. 908-922.

[7] Milan Simek, Patrik Moravek and Jorge sa Silva," Wireless Sensor Networking in Matlab:Step-by-Step", 2010.

[8] Chen X, Makki K, Yen K, Pissinou N, "Node compromise modeling and its applications in sensor networks", In: 12th IEEE symposium on computers and communications, 2007, pp. 575–582.

[9] Chan K, Fekri F, "Node compromise attacks and network connectivity", In Proc SPIE 6578, 2007, pp. 1–12.

[10] Bonaci T, Bushnell L, Poovendran R, "Probabilistic analysis of covering and compromise in node capture attacks", 2010. http://www.ee.washington.edu/research/nsl/papers/techReport_tamara_NodeCap.pdf.

[11] Piyush Kumar Shukla, Sachin Goyal, Rajesh Wadhvani, M. A. Rizvi, Poonam Sharma, and Neeraj Tantubay, "Finding Robust Assailant Using Optimization Functions (FiRAO-PG) in Wireless Sensor Network, " Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2015, Article ID 594345, 7 pages, http://dx.doi.org/10.1155/2015/594345.