Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 594345, 7 pages
http://dx.doi.org/10.1155/2015/594345

Research Article

Finding Robust Assailant Using Optimization Functions (FiRAO-PG) in Wireless Sensor Network

Piyush Kumar Shukla,[1] Sachin Goyal,[2] Rajesh Wadhvani,[3] M. A. Rizvi,[4] Poonam Sharma,[5] and Neeraj Tantubay[2]

[1]*Department of Computer Science and Engineering, UIT, RGPV, Bhopal, India*
[2]*Department of Information Technology, UIT, RGPV, Bhopal, India*
[3]*Department of Information Technology, MANIT, Bhopal, India*
[4]*Department of Computer Engineering and Applications, NITTTR, Bhopal, India*
[5]*Department of Computer Science & Information Technology, MITS, Gwalior, India*

Correspondence should be addressed to Piyush Kumar Shukla; pphdwss@gmail.com

Received 24 September 2014; Accepted 23 December 2014

Academic Editor: Gerhard-Wilhelm Weber

Wireless sensor network consists of hundreds or thousands of low cost, low power, and self-organizing tiny sensor nodes that are deployed within the sensor network. Sensor network is susceptible to physical attacks due to deprived power and restricted resource capability and is exposed to external environment for transmitting and receiving data. Node capture attack is one of the most menacing attack in the wireless sensor network and may be physically captured by an adversary for extracting confidential information regarding cryptographic keys, node's unique id, and so forth, from its memory to eliminate the confidentiality and integrity of the wireless links. Node capture attack suffers from severe security breach and tremendous network cost. We propose an empirically designed multiple objectives node capture attack algorithm based on optimization functions as an effective solution against the attacking efficiency of node capture attack. Finding robust assailant optimization-particle swarm optimization and genetic algorithm (FiRAO-PG) consists of multiple objectives: maximum node participation, maximum key participation, and minimum resource expenditure to find optimal nodes using PSO and GA. It will leverage a comprehensive tool to destroy maximum portion of the network realizing cost-effectiveness and higher attacking efficiency. The simulation results manifest that FiRAO-PG can provide higher fraction of compromised traffic than matrix algorithm (MA) so the attacking efficiency of FiRAO-PG is higher.

1. Introduction

With the advent of wireless communication technology, sensor network has become a user-perceived network for many applications in the recent years. WSN inheres apportioned low power, low-cost, and self-organizing sensor nodes to get secret information and plays a decisive role to preserve confidentiality and integrity of the radio links in applications like military surveillance, environment monitoring, and many more scenarios. However, due to unattended nature of sensor network, it is highly vulnerable to physical node capture attack [1]. It is an empirically derived comprehensive attack where the adversary physically tampers the sensor node by extracting cryptographic keys and other top-secret information. By leveraging the extracted confidential information, an attacker gathers secret information from the network by eavesdropping communication among the sensor nodes. Node capture is the most vexing problem that jeopardizes the confidentiality, reliability, and security of sensor nodes.

Analyzing the way of mounting the node capture attack can provide threatening models for developing defending techniques against it. Development of effective threatening techniques keeps greater importance because the performance of defending technique directly depends on it. The former node capture attack algorithms proposed suffered drawbacks like attacking modeling and low attacking efficiency. Modeling techniques of attack formalize the mechanism for analyzing the behavior of an adversary. After designing the modeling techniques, the adaptation of an adversary can be

intuitively expressed that exhibits the attacking target and attacking process. Therefore, the modeling of node capture attack can abet heuristic strategies for an adversary. To prototype node capture attack, attacking efficiency is an imperative characteristic that is used to delineate fraction of compromised traffic within the network. Higher attacking efficiency, which represents the network, will be compromised. Therefore, designing an enhanced and optimized way of node capture attack accreting improved attacking efficiency sanctifies its significance.

Multiform researchers have proposed techniques for modeling the node capture attack for its deeper analysis and design of a random key predistribution scheme [2] is applied for configuration of sensor network. Hypothetically, formalization of modeling techniques of the node capture attack can be categorized into an UML methods [1, 3], probabilistic analysis [3, 4], system theoretic approach [5], epidemic theory [6, 7], and vulnerability evaluation approach [8–12].

In certain modeling methods, the attacker randomly captures node to compromise in the communication of a whole sensor network. However, vulnerability evaluation approach has been formalized whereby an attacker can select a node intelligently to compromise the network using vulnerability metric. Vulnerability evaluation methods proposed so far in [8–12] suffer certain drawbacks.

(i) Vulnerability is distinguished as a real number, which cannot precisely outline the destructiveness within the network.

(ii) Attacking efficiency of node capture attack is low, which needs to capture a high number of nodes in the network.

(iii) Some vulnerability approach is restricted for deterministic key protocol, which is unsuitable for mobile network.

(iv) In few vulnerabilities based assailing approaches, node capture attack is modeled from the perspective of relationship among nodes and paths that not provide optimal solution to capture a node.

(v) To evaluate the vulnerability metric, some previous algorithms only provide a focus on the resource expenditure to capture a node, some provide focus on the maximum number of keys captured, and some take route vulnerability into the consideration. Until now, there is no approach designed that takes all the three objectives into the consideration.

To overcome the above problems of vulnerability based approaches and to enhance the attacking efficiency of the node capture attack, we model the node capture attack algorithm that works on the three objectives maximum node participation, maximum key participation, and minimum resource expenditure to find an optimal node using PSO that creates maximum destructiveness in the network and provides higher attacking efficiency at minimum resource expenditure.

2. Related Work

In the literature, various researchers have proposed modeling techniques based on the vulnerability evaluation. In this type of technique, an attacker can intelligently choose a node to attack with eavesdropping on the insecure messages transmitting in the network. In [10], the authors proposed a mathematical model for modeling of node capture attack on the different key establishment protocols within the heterogeneous wireless ad hoc and wireless mesh networks. Node capture attack is modeled using an integer-programming minimization problem which derives the NP-hard set cover problem in which attacks are evaluated with respect to the attacking cost and the benefit of an attack to the attacker. Node capture attack algorithm that receives the expected benefit at less cost for an attacker is mapped to the NP-hard minimization problem. The valuable solution for this problem is estimated with the help of known heuristics that are set coverage and subset coverage. This modeling technique of node capture attack is limited to probabilistic and deterministic key distribution schemes.

In [12], the authors examined the effect of physical node capture attack on the integrity and confidentiality of the network for which they present the node capture attack algorithm as a nonlinear integer programming problem. Because of NP-hardness of the minimization problem, the greedy node captured approximation using vulnerability evaluation protocol (GNAVE) is proposed. GNAVE is an elegant solution for approximating the minimum cost node capture attack. In the GNAVE algorithm, the compromise of the network traffic is mapped as flow of current, which is passed through an electronic circuit. In this algorithm, the route vulnerability metric is proposed, which depends on the routing and cryptographic protocols that can minimize resource expenditure to a certain level. At each step of the GNAVE algorithm, the attacker selects to capture the node with higher values per unit cost to improve the cost-effectiveness of the node capture attack. GNAVE provides increasing attacking efficiency for node capture attack by compromising fewer nodes with higher fraction of compromising traffic of the network. It does not include the execution time into the consideration for destroying the complete network [12].

In [8], Wu et al. proposed a greedy node capture attack algorithm based on the route minimum key set (GNRMK). In GNRMK, sensor network is mapped as flow network to acquire its route minimum key set that shows the vulnerability of the route within the network. The route minimum key set is used to destroy the network with less resource expenditure. It is achieved by evaluating the max-flow of the flow network by using the labeling and adjustment procedure which is based on the Ford-Fulkerson algorithm. Then, a node overlapping to values metric (NOV) is evaluated using the route minimum key sets. A node that has been maximum overlapping value is targeted as a node to be captured within the network. After capturing a node with highest overlapping values, the network topology is dynamically changed due to already compromised links or paths. GNRMK algorithm can only utilize within the static networks because it is exclusively

Table 1: A summary of related symbols and their definitions.

Symbols	Description
N	Set of sensor nodes in the network
N_i	ith sensor node
K	Set of total keys in the key pool
K_i	Set of keys acquired by node n_i
L	Set of links between nodes
$l(i, j)$	Link between node n_i and node n_j
S, D	Set of source and destination nodes
R	Set of routes in the network
W_i	Capturing cost of node n_i
C_n	Set of compromised nodes
$P(R_i)$	Total number of paths of route R_i
$Pk(i, j)$	Number of paths in which node n_j participates in route R_i
F_i	Objective function for node n_i

restricted to deterministic key protocol that is unsuitable for mobile networks.

3. Models and Definitions

The matrix algorithm (MA) is proposed in [9] to perform the node capture attack within the sensor network, when the network is configured with the random key predistribution scheme. In this algorithm, a compromising matrix is designed for evaluating a node that makes the network highly vulnerable by establishing a relationship between nodes and paths. Matrix algorithm takes less resource expenditure with larger destructiveness within the network. MA takes less number of attacking rounds, less execution time, high attacking efficiency, and less resource expenditure [9]. It is limited to the random key predistribution scheme, and it also provides less attention towards the relationship between the attacking efficiency of the node capture attack and attacking cost. It only provides the focus on resource expenditure to capture a specific node that means a node that has less resource expenditures compared to others, it is compromising enough paths in the network, and it will be captured. MA also considers those paths that are not influenced by capturing a particular node that increases computation overheads. 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.

3.1. Key Assignment Model. In WSN, the random key predistribution scheme is used to assign set of keys $K_i \in K$ to each sensor $n_i \in N$ that is randomly chooses from key pool. The set of keys shared between nodes n_i and n_j is represented by $K(i, j)$. Neighboring nodes can communicate with each other, when they are located within each other's transmission range r and they have at least one common sharing key $K(i, j)$. The more the number of keys in the set $K(i, j)$ will be, the higher the security of the link will be.

3.2. Network Model. In the network model, wireless sensor network consists of set of N sensor nodes and the network is represented by a directed network graph $G = (N, l)$. After the deployment of sensor nodes, the specific routing protocol is applied to construct multiple routes for transmitting packets from source to destination nodes. A packet from source node $s \in S$ to destination $d \in D$ will traverse one or more paths that depend on the routing protocol. Each of the paths of a particular route is constructed from a set of sequential links (i, j). The link topology of the network is presented by a $N \times N$ matrix (C) where a "c_{ij}" represents the link cost between the nodes, as shown in the following part.

The Connection Cost Matrix for 3 Nodes System. Consider

$$\begin{matrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{matrix} \quad (1)$$

Number link topology matrix is used by specific routing protocols to estimate the possible paths or routes in the network. Two kinds of routing protocols are implemented here that are single path and multipath routing protocols to evaluate the effect of node capture attack algorithm. The single path routing protocol establishes a single path from source to destination, whereas multipath protocol establishes more than one path to transmit packet from source to destination.

3.3. Adversary Model. The node capture attack algorithm is modeled from an attacker's point of view and it is assumed that the attacker has capability and network resources to eavesdrop on the messages passing through the network for capturing a node in the network and extracting cryptographic keys and other pieces of confidential information from nodes memory in polynomial time. It is also assumed that the attacker has knowledge of the key assignment model and routing protocols used in the network like key is represented as label key and adversary has knowledge of assignment of labels of the network keys, paths, and routes implemented by specific routing protocol. In the sensor network, destination nodes are usually implemented with higher security and protection mechanisms. So, it is considered that an attacker cannot intrude them.

The attacker's aim is to propose an efficient attack to compromise the whole network by achieving multiple objectives: minimum resource expenditure, maximum keys, and maximum capture of transmitting packets. To fulfill this goal, the particle swarm optimization technique is used to find network nodes that make sensor network more vulnerable. Therefore, the network is analyzed by an attacker to own the background information of the key assignment protocol and network parameter to model the attacking algorithm.

To compromise the sensor network, it is required for an attacker to extract the keys by capturing a node to break the security, confidentiality, and integrity of the network. To represent the compromise of a link, path, and route in the sensor network the following definitions are illustrated as follows.

Definition I. A link $l(i, j) \in l$ is compromised when the sharing key $K(i, j)$ belongs to the set of keys acquired by an attacker.

Definition II. A path $pi \in P$ is compromised when at least one link which belongs to that path is compromised.

In the single path routing protocol, a route consists of a single path only. So compromise of that single path is equivalent to compromise of a route. But in case of multipath routing, packets are segmented into pieces and then transmitted from separate paths. To compromise such routes the following definition is proposed.

Definition III. A route, $Rs, d \in R$ is compromised when all the paths which belong to that route are compromised.

Particle swarm optimization is a population based computational technique. It learns from the scenario and is used to find a potential solution to an optimization problem. In the context of PSO, a swarm refers to a number of potential solutions to the optimization problem, where each potential solution is referred to as a particle. PSO is initiated by 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 p_{best} (personal best) value. This is the value of the fitness function; it has been achieved so far. Another one is called the g_{best} (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 p_{best} and g_{best}, the particles update its velocity and position with the following equations:

$$\begin{aligned} V_i^{t+1} &= wV_i^t + c_1 \text{rand}\,() \left(P_i - X_i^t\right) \\ &\quad + c_2 \text{rand}\,() \left(P_g - X_i^t\right), \\ X_i^{t+1} &= X_i^t + V_i^{t+1}, \end{aligned} \tag{2}$$

where $i = 1, 2, \ldots, N$, N represents the individual number in the group; w is the inertia coefficient; t represents the iteration number; c_1 and c_2 are learning factors; rand() is uniformly distributed random variables in $[0, 1]$; P_i is particles best position till iteration t; X_i^t is particles current position in iteration t; and P_g represents globally best particle position in iteration t.

The basic procedure of the PSO algorithm is as follows.

(i) Assign initial values to the position and velocity of all particles.

(ii) Evaluate the fitness of each particle according to the desired optimization. So the optimal value of individuals (personal best) and optimal value of swarm (global best) can be obtained.

(iii) Update the position and velocity of the particles.

(iv) Determine whether the conditions meet ends, if not, go to Step 2.

4. Multiple Objectives Node Capture Attack Algorithm Based on PSO (FiRAO-PG)

The aim of the node capture attack algorithm is to capture a set of nodes to compromise the complete network. So, all the paths that belong to different routes should be captured for compromising the whole network. Therefore, the attacker's goal is to compromise maximum possible routes of the network by capturing a limited number of nodes that satisfy multiple objectives which are maximum participation of nodes within the network so that the maximum packets communicated within the network can be eavesdropped, and also maximum keys and minimum resource expenditure. The presented algorithm evaluates the optimal nodes for the node capture using PSO such that only a limited number of nodes capturing compromise the whole network by providing maximum benefit to an attacker.

To analyze the participation of sensor nodes in the network, we calculate the route node participation matrix, which represents the participation of each sensor node in each route of the network. Participation of a node in a specific route manifest that in how many path nodes participated to transfer packets to another node from all the paths belongs to that distinct route. In other words, it represents the participation ratio for each node in the network on the basis of number of paths in which that node belongs among all the paths available in that particular route. We denote the route node participation matrix as RN = $[\text{RN}(i, j)]R \times N$, where

$$\text{RN}\,(i, j) = \begin{cases} \dfrac{Pk\,(i, j)}{P\,(R_i)} & \text{If Node } n_j \text{ participates in Route } R_i \\ 0 & \text{Otherwise.} \end{cases} \tag{3}$$

$Pk(i, j)$ represents the number of paths of route R_i in which node n_j participates; $P(R_i)$ stands for total number of paths of route R_i.

To achieve another objective that is capturing a node that contains maximum keys together with maximum participation and minimum resource expenditure, we create another key node participation matrix that shows the belonging relationship between keys and nodes. Key node participation matrix KN = $[\text{KN}(i, j)]K \times N$ can be represented as follows:

$$\text{KN}\,(i, j) = \begin{cases} 1 & \text{If Key } k_i \in n_j \\ 0 & \text{Otherwise.} \end{cases} \tag{4}$$

Here, k_i represents ith key of key pool. To evaluate number of keys a node has in their memory, we calculate the key participation matrix that represents number of key belongs to a particular node of the network. We denote the key participation matrix as $K = [K_j]1 \times N$, where

$$K_j = \begin{cases} \displaystyle\sum_{i=1}^{K} \text{KN}\,(i, j) & \text{If some Keys belong to Node } n_j \\ 0 & \text{Otherwise.} \end{cases} \tag{5}$$

Here, K_j represents the number of keys assigned to node n_j. In the node capture attack, another issue the adversary must pay attention towards is the resource expenditure or energy cost. The adversary seeks for compromising a set of nodes that consumes least energy together with maximum participation and maximum key to wreaking the security of the network. Therefore, we calculate capturing cost matrix that represents the energy cost or resource expenditure for each node in the network. Capturing cost matrix $W = [w_i]1 \times N$ is denoted as follows:

$$W_i = \begin{cases} w_i & \text{Capturing Cost of Node } n_i \\ 0 & \text{Otherwise.} \end{cases} \quad (6)$$

Here, w_i represents the resource expenditure for node n_i. The capturing cost of each node is related to the environment that is exposed by a node and the capability of an attacker. So it is very difficult to elaborate on energy cost in capturing a node. Here, we consider that the resource expenditure of capturing a node ranges between $(0, 1)$.

After evaluating route node participation matrix RN, key participation matrix K, and capturing cost matrix W, we need to find optimal nodes in the network that provide best result on the basis of multiple objectives which are taken into the consideration. To find such kinds of nodes, PSO algorithm is utilized here that provides best optimal nodes that creates maximum destructiveness in the network.

Before applying PSO algorithm, first we evaluate the objective function to achieve the required goal. The objective function can be written as follows:

$$f_j = \sum_{i=1}^{\mathrm{NA}} \sum_{i=1}^{R} \frac{1}{\mathrm{RN}(i, j)} + \frac{1}{K_j} + W_j. \quad (7)$$

Here, f_j represents the objective function of jth node, $\mathrm{RN}(i, j)$ shows participation of jth node in route R_i, K_j stands for keys assessable through jth node in all the possible paths or routes, and W_j represents the capturing cost or resource expenditure of jth node in all the possible paths or routes.

After evaluating objective function, PSO algorithm is initiated to find optimal nodes from the available network nodes, which minimize the value of objective function to provide the best results. In order to find the optimal set of nodes that creates maximum destructiveness in the network using PSO, we define a location mapping equation as

$$X_i = \mathrm{Round}\left(X_i * (\text{Total sensor nodes} - 1)\right) + 1. \quad (8)$$

Equation (8) represents that if the positions of the particles cannot corresponds to node id, then we can find the nearest node id.

The set of compromised nodes is returned by FiRAO-PG that contains node indexes, which provide optimal results based on all the three objectives. Maximum node participation, minimum resource expenditure, and maximum key participation. These three objectives provide following features: (1) it seeks for the maximum participated node that induces maximum destructiveness in the network because if a node has maximum participated value that means it belongs to the higher number of paths and provides maximum capturing of transmitted packets, (2) it takes least resource expenditure to compromise the network, and (3) it acquires maximum keys of key pool that helps to compromise a higher number of paths either directly or partially. The attacking algorithm of node capture attack ends when the whole network is compromised and it returns set of compromised nodes C_n as output of this algorithm. From the perspective of an attacker, the set of compromised nodes C_n (returns by FiRAO-PG) causes maximum destructiveness in the network. But from the defenders point of view, this algorithm provides vulnerable nodes of the network to strengthen the security of the network.

4.1. FiRAO-PG Algorithm. (1) Input: $G(N, l)$, K, w_i.

(2) Output: C_n.

(3) Calculate route node participation matrix using (3).

(4) Calculate key participation matrix using (5) and calculate key node participation matrix using (4).

(5) Calculate capturing cost matrix using (6).

(6) The objective function is then formulated to achieve the required goals using FiRAO-PG algorithm and can be written as

$$f_j = \sum_{i=1}^{\mathrm{NA}} \sum_{i=1}^{R} \frac{1}{\mathrm{RN}(i, j)} + \frac{1}{K_j} + W_j. \quad (9)$$

(7) Optimization algorithm is initiated to find the set of optimal nodes of the available nodes, which minimizes the value of the objective function.

Here, each set of different combinations of nodes are defined as particles of the randomly generated population and dimensions of each particles are defined as number of nodes required to capture. The algorithm works as follows.

Step 1. Initialize population to random size m ($m < n$). Initialize position and velocity of each particle (representing node ids) i to random value.

Step 2. Compute the fitness of each particle using (6) and obtain the optimal value of the individual and of the population.

Step 3. Update position and velocity of each particle using (2), and then adjust position of particles using (8) to find node ids.

Step 4. Test for convergence conditions, if not, go to Step 2; else provide a set of optimal nodes and return index of that nodes to perform node capture attack.

(8) GA algorithm is initiated to find the set of optimal nodes.

Step 1. Initial population random (random selection from nodes).

Step 2. Crossover (node), // a new chromosome is created with 2 parents.

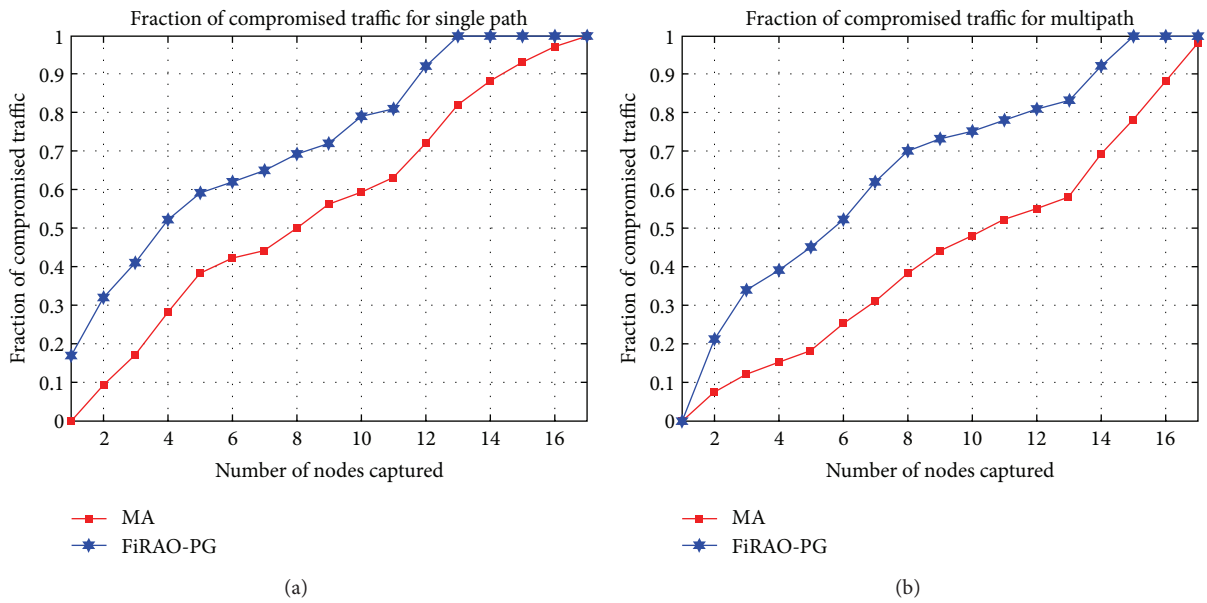

Figure 1: (a) Fraction of compromised traffic versus number of nodes captured for single path routing. (b) Fraction of compromised traffic versus number of nodes captured for multipath routing.

Step 3. Mutation (node), // a chromosome from each parent changes. Then the distance between the new node and the sink is determined.

Step 4. Merge (2 new populations).

Step 5. Sort (node), // (distance to sink, energy).

Step 6. Size (new-population) = size (population).

Step 7. Sort (new population), // the second time.

Step 8. Creating cluster head.

(9) Return C_n based on the best values from PSO and GA.

Table 2: Simulation parameters.

Parameters	Values
Number of sensor nodes	200
Region size	100∗100
Number of source nodes	5
Sensing range	20 m
Number of destination nodes	3
Key pool size	100
Number of keys assigned to a node	20
Set of source and destination nodes	R
Population size	50
Number of iteration	200

5. Result and Analysis

To analyze the performance of multiple objectives node capture attack algorithm based on PSO and GA (FiRAO-PG), we performed the following simulation. The experimental parameters are shown in the Table 2.

In the simulation work, 200 nodes are deployed in the sensor network. From the total deployed nodes, 5 source sensor nodes and 3 destination nodes are randomly selected. Random key predistribution scheme is used to assign keys to different nodes in the sensor network. Keys are assigned randomly from the key pool to each sensor node, when the network is deployed. Sensor nodes located in 20 m can communicate with each other in the simulation. Two kinds of routing protocol are used that are single path routing protocol and multipath routing protocol. An attacking algorithm for node capture attack is analyzed on single path and multipath routing protocol to check influence of this attacking algorithm. The proposed FiRAO-PG algorithm runs 200 iterations. We measure the performance of our proposed work in terms of fraction of compromised traffic.

To show the advantage of our proposed algorithm, we provide a comparison with an MA (matrix algorithm) [9] in terms of fraction of compromised traffic. Both algorithms MA [9] and multiple objectives node capture attack algorithm based on PSO (FiRAO-PG) have same input parameters in the simulation that are $G(N, l)$, K, w_i.

5.1. Fraction of Compromised Traffic. Fraction of compromised traffic represents the ratio of compromised paths among all the paths in the network. Figure 1 illustrates the fraction of compromised traffic of FiRAO-PG and MA for single path and multipath routing. In this experiment, x-coordinate represents the number of nodes captured by an adversary while the y-coordinate indicates the fraction of the traffic that are compromised by an adversary. The fraction of compromised traffic can indicate attacking efficiency of an algorithm. As soon as the fraction of compromised traffic

reaches 1, higher will be the attacking efficiency of that algorithm. Figure 1 illustrates that multiple objectives node capture attack algorithm based on PSO (FiRAO-PG) can quickly approach 1 due to this algorithm that aims to capture node that maximally participates in the network together with keeping maximum keys and consuming less resource expenditure. Therefore, this algorithm causes maximum destructiveness in the sensor network by compromising the maximum number of paths. MA needs comparatively more nodes to break the confidentiality of the network. So, we can conclude that FiRAO-PG provides higher attacking efficiency than MA.

6. Conclusions

We proposed that a FiRAO-PG (finding robust assailant optimization-particle swarm optimization and genetic algorithm) has been used for enhancing the attacking efficiency of the node capture attack in the wireless sensor network. FiRAO-PG takes three objectives into consideration that are maximum key participation, bare minimum resource expenditure, and maximum node participation to find optimal nodes that provide the best combination for all the objectives and causes maximum destructiveness in the network. The simulation result shows that FiRAO-PG provides a higher fraction of compromised traffic, when compared with a matrix algorithm (MA). Therefore, FiRAO-PG provides higher attacking efficiency than MA by capturing a limited number of nodes that compromises whole network.

(i) How to further minimize the number of captured nodes using ACO (ant colony optimization, binary-PSO, simulated annealing) to compromise the whole network to enhance the attacking efficiency of the node capture attack algorithm.

(ii) We can also check performance of FiRAO-PG in the clustered sensor network.

(iii) Performance of the FiRAO-PG can be checked in high mobility networks (VANET, DTN, etc.)

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Authors' Contribution

Piyush Kumar Shukla deplored the algorithms for this work and generates the idea of how a robust assailant using optimization functions (FiRAO-PG) in wireless sensor network can be designed. Sachin Goyal contributed to implementation of the work using genetic algorithm. Rajesh Wadhvani contributed to summery of the work done in a relevant area till date and also developed understanding of the base paper's work. M. A. Rizvi contributed to summery of the work done in a relevant area till date and also developed understanding of the base paper's work. Poonam Sharma contributed to implementation of the work using particle swam optimization and also purified and tuned the work done using genetic algorithm. Neeraj Tantubay contributed to improving the language of the paper as well as technical content of the paper.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proceedings of the IEEE Symposium on Security And Privacy*, pp. 197–213, May 2003.

[3] K. Chan and F. Fekri, "Node compromise attacks and network connectivity," in *Defense Transformation and Net-Centric Systems*, Proceedings of SPIE, Orlando, Fla, USA, April 2011, http://trove.nla.gov.au/work/34974076?citationFormat=BibTeX&selectedversion=NBD42326214.

[4] A. K. Mishra and A. K. Turuk, "Adversary information gathering model for node capture attack in wireless sensor networks," in *Proceedings of the IEEE International Conference on Devices and Communications (ICDeCom '11)*, pp. 1–5, Mesra, India, February 2011.

[5] T. Bonaci, L. Bushnell, and R. Poovendran, "Node capture attacks in wireless sensor networks: a system theoretic approach," in *Proceedings of the 49th IEEE Conference on Decision and Control (CDC '10)*, pp. 6765–6772, Atlanta, Ga, USA, December 2010.

[6] P. De, Y. Liu, and S. K. Das, "Modeling node compromise spread in wireless sensor networks using epidemic theory," in *Proceedings of the IEEE 7th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '06)*, pp. 237–243, June 2006.

[7] P. de, Y. Liu, and S. K. Das, "Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory," *ACM Transactions on Sensor Networks*, vol. 5, no. 3, pp. 1–33, 2009.

[8] G. Wu, X. Chen, M. S. Obaidat, and C. Lin, "A high efficient node capture attack algorithm in wireless sensor network based on route minimum key set," *Security and Communication Networks*, vol. 6, no. 2, pp. 230–238, 2013.

[9] C. Lin and G. Wu, "Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach," *The Journal of Supercomputing*, vol. 66, no. 2, pp. 989–1007, 2013.

[10] P. Tague and R. Poovendran, "Modeling adaptive node capture attacks in multi-hop wireless networks," *Ad Hoc Networks*, vol. 5, no. 6, pp. 801–814, 2007.

[11] P. Tague and R. Poovendran, "Modeling node capture attacks in wireless sensor networks," in *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1221–1224, Urbana, Ill, USA, September 2008.

[12] P. Tague, D. Slater, J. Rogers, and R. Poovendran, "Vulnerability of network traffic under node capture attacks using circuit theoretic analysis," in *Proceedings of the 28th IEEE International Conference on Computer Communications*, pp. 161–165, IEEE, Rio de Janeiro, Brazil, April 2009.