Detecting Attacks in Wireless Sensor Network Using Genetic Algorithms

[1]Novin Makvandi, [2]Seyyed Mohsen Hashemi, [3]Peiman Haghighat
[1] Student of Department of Computer Engineering, Islamic Azad University (IAU), UAE Branch, Dubai, UAE,
nmakvandi@yahoo.com,

[2] Faculty of Department of Software Engineering and Artificial Intelligence, Science and Research Branch,
Islamic Azad University, Tehran, Iran
isrup@yahoo.com,
[3]Faculty of Department of Computer Engineering, Islamic Azad University (IAU), UAE Branch Dubai, UAE,
P_haghighat@iau.ae

ABSTRACT

Wireless Sensor Network (WSN) technology has attracted much attention in recent years and enables new applications but it requires nonconventional paradigms for the protocol design due to limited amount of energy source, memory, and computation constraints. This technology is used in military, medicine, environmental and industrial monitoring applications. Many attempts have been done, to promote these networks in order to meet objectives such as increasing lifetime, speed of transfer information, quality of service and security. One of the challenging subjects in these networks is surveying the security attacks to the network layer and finding a solution for them. Thus, we need to establish a method which can detect the attack and disable the attacker from the network access, by using the minimum battery consumption, and with a simple, effective and robust algorithm to perform our objectives.

The purpose of this research is to identify the threats detected by clustering genetic algorithm in the clustered sensor networks, which will lead to prolong the network lifetime. In addition, the optimal routing is done by applying fuzzy function. The simulation results show that the simulated genetic algorithm has speeded up the detection and improved the energy consumption cost.

KEYWORDS
Wireless sensor network, detecting attack, genetic algorithm, fuzzy function, energy

1 INTRODUCTION

Sensor networks consist of a large number of tiny sensor nodes that are used to collect and process environmental information. These tiny sensor nodes consist of three parts: sensors, information processing and information exchange (in wireless format). Security is a vital requirement for many applications of sensor networks. However, with the limited capabilities of smart sensors (battery storage, CPU, memory, etc.) and the unfavorable development environment of a sensor network (infrastructure-less, unattended, wireless, ad-hoc, etc) makes this problem so challenging.

The attacker can easily perform an internal attack with converting the data, ignoring the messages, selected forwarding, making disruptive noise, etc. The internal attackers are highly destructive for the network performance.

An inexpensive sensor has a limited memory capacity and limited computing capabilities so it cannot create a log file for tracking and identifying the internal attacks. Moreover, due to the large scale of the networks and their infrastructure-less architectures, the central station cannot use the data collected to identify attacker node. A detection plan should be designed locally and computationally efficient to reduce battery power and bandwidth. In addition, the only resources available for tracing *algorithms are the communication activities within a limited range, which will create a new challenge in detecting internal attacker. Considered the algorithm should be based on local data.*

The attacks in wireless sensor networks can be categorized to the ones occurring at physical, communication (access control to media or interface), network, transfer, and application layers attacks. The attacks can also be divided into two categories: internal and external [3].

The main function of wireless sensor networks is sensing the environmental events and transferring the information to the base station for further processing. Thus, routing is an essential operation in sensor networks. A number of routing protocols has been proposed for sensor networks. So routing in wireless sensor networks is the best way of providing security and detecting attacks in these networks [7].

2REVIEW

Many universities and research institutions have started to work on these networks. Most of them were performed with the financial help of DARPA. Briefly, the projects are as follow: Building an operating system for sensor nodes, creating sensors of very small size and up to a dollar, known as Smart Dust, at UC Berkeley, Using sensor nodes to create pervasive computing at Carnegie Mellon University and the Massachusetts Institute of Technology.

Guo[2010]et.al has shown that the genetic algorithm is an appropriate solution to find the optimal path for WSN[4].

Younis[2006]et.al , have proposed a survey on clustering algorithms for WSN. The result shows that this clustering has best routing and long lifetime for WSN [6].

Khanna[2009] et.al, have proposed Reduced Complexity Intrusion Detection in Sensor Networks Using Genetic Algorithm. The proposed method increases lifetime in WSN with GA [2].

3 PROPOSED METHOD

Evolutionary algorithms can be an effective method for finding the path with optimal consumption of energy in wireless sensor networks.

In Genetic algorithms, each solution might be shown as a binary string (chromosome) and the measurement of the related fitness function. Successive solutions are parts of an evolutionary process, in which one of the selective solutions chooses an individual to set for the next generation. The probability of choosing a solution is presented as follows:[1]

$$p_i = \frac{F_i}{\sum_{j=0}^{N} F_j} \qquad (1)$$

In which P_i is the probability of choosing a specific solution for the parent population. F_i is the fitness function of the candidate solution and N is all of the optimal ways for a population.

In this treatise, genetic algorithm is used to distribute the randomly deployed sensors with the clustered network. The network is divided to optimal number of independent clusters with the cluster heads. The proposed method uses the genetic algorithm for clustering and performs the routing based on the fuzzy selection, which is addressed to detect the attacker nodes routing.

The incompatible (malicious) nodes provide extra observations of the network behavior due to analyzing the sensor events in its neighborhood.

The considered cases consist of:

Data massage patterns, massage collision, the active trend of traffic rout, sensor positioning, and synchronized events.

An important issue in these networks is increasing the lifetime. Long communication distance between sensors and the sink in a wireless sensor network consumes a lot of energy and decreases the network lifetime [5]. As clustering can reduce energy consumption for the wireless sensor network, we can reduce the communication *distance significantly and prolong the network lifetime as a result.*

First, we use genetic algorithm for clustering the network. It has a significant role in decreasing the energy consumption and optimized routing.

In this treatise, genetic algorithm is used to distribute the randomly deployed sensors with the clustered network.

The network is divided to optimal number of independent clusters with the cluster heads.

The proposed method uses the genetic algorithm for clustering and performs the routing based on the fuzzy selection, which is addressed to detect the attacker nodes routing.

Also sink is considered as a reliable element, which creates the required secure connection between different nodes. The nearest nodes to the sink make the most reliable connections.

Different sensor nodes communicate with each other by sending and receiving messages and the sink is responsible for the node authentication. The attack detection GA contains monitoring nodes that control the network and determine any conflict with network criteria (communication cost and battery energy) which increases the reliability of the network.

The cluster head or any of the cluster nodes can act as the monitoring node. This node receives the information about the other nodes and after comparing them to the previous information from the initial configuration of the network; it detects the attacker and transmits the information to the sink.

4 ALGORITHM

```
1. Start
2.node= Distribute (round (200))

3. Read Fuzzy function

4.[center_ch] = GA; //GA start to select ch and membership of ch

    a. Initial population random (Random selection from distance, energy)

    b. Crossover (node); // A New child is created with 2 parents. Then the distance between the new node and the sink is determined

    c. Mutation (node); // A chromosome from each parent changes. Then the distance between the new node and the sink is determined

    d. Merge (2new populations);

    e. Sort (node); // (distance to sink, energy)

    f. size( new-population)=size(population)

    g. Sort (new population); // the second time (distance, energy)

    h. Creating cluster head; // Identifying the distance between clustering and membership

5. while( size(node)>=(sink_number + cluster_number))

{

5.1[select1]=fuzzy_select(node);
5.2 node_find = find(select_find == [select1]); // The selected route’s node is added to the selected nodes list.

5.3 If size (node_find)>1

          count1 = count1 + 1;
         Size-node--;


5.4 if (node==in_cluster)
          D = distance from data;
     Else
        D = D1 + D2 + d_center;
//D1=distance node to ch1 D2=distance chi to ch2, d_center = distance from center

     End
5.5 If (D < 1)
     Size-node--; // The node is dead.

     if size_node!= threshold

         [center_ch] = GA; //GA select ch
} end while

6. End
```

5- SIMULATION

The proposed method is simulated in MATLAB. We consider an area of 100×100. 200 nodes with the initial energy of 1000 J are randomly distributed in the network. The number of clusters is considered 10. A 3D matrix is taken with the first and the second dimensions involving coordinates and the third dimension involving energy. The sink is located at the point (0, 0) of the plate.

*We define the values of genetic algorithm as: Initial population=10, length of each chromosome = number of Ch * 2=10, Crossover=0.7, mutation=0.4, mutation rate=0.2. Every node acts as a counter of hops to the sink.*

First, MOGA performs clustering and routing on the nodes in the area, and then the best optimal route is chosen using fuzzy method. If a node dies, it is omitted and a new clustering is done. GA checks the nodes in the optimal route. Then it detects and eliminates every node matching the attack criteria. A new clustering is done at the end.

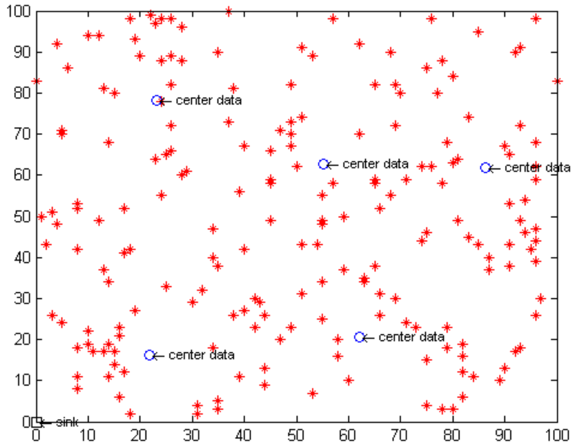

***Figure1.** WSN in 100*100*

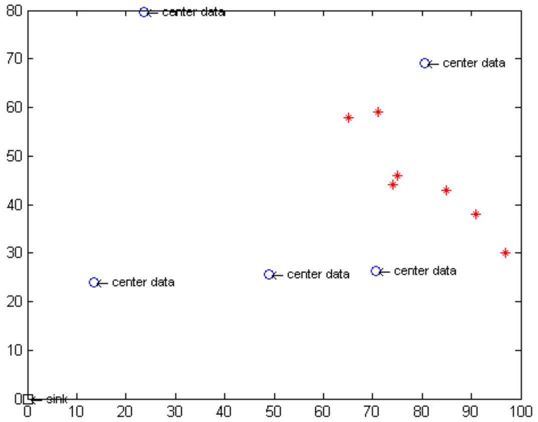

***Figure2.** End of network life time*

5.1 Simulation Results

In MOGA, two criterions for optimality are considered, battery consumption and the best route. Since the genetic algorithm chooses multiple optimal routes, fuzzy method is proposed to select the best route among them. In fuzzy method, the route with the lowest density and the shortest distance from the sink is chosen as the response.

At higher densities, the nodes have also higher energy consumption, and the routes through these nodes consume more energy. In addition, the nodes with a short distance to the sink have less energy waste in forwarding the message and save the energy of the network.

In multi-purpose genetic algorithm, two criterions for optimality are considered, battery consumption and the best route. Since the genetic algorithm chooses multiple optimal routes, fuzzy method is proposed to select the best route among them. In fuzzy method, the route with the lowest density and the shortest distance from the sink is chosen as the response.

The network lifetime with the proposed method is compared to the network lifetime with genetic algorithm; in figure 3.This algorithm is examined for over 200 numbers of nodes.

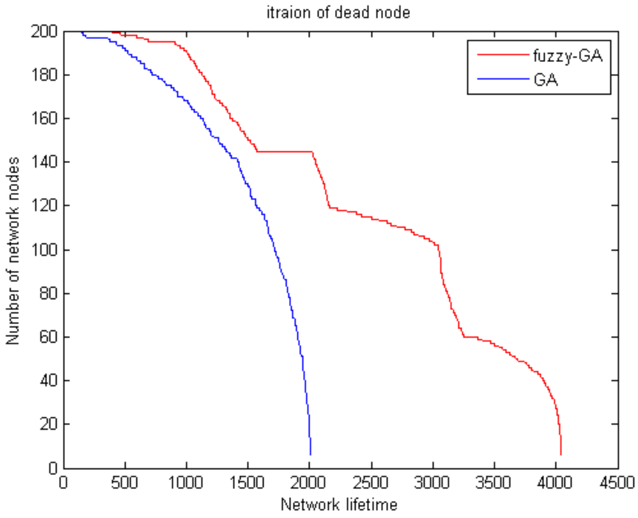

Figure3. *The network lifetime with the proposed method compared to the network lifetime with genetic algorithm.*

In our proposed method, the whole sensor network is not checked to detect the attacker node and only the selected route is checked by fuzzy algorithm. As a result, we just consider the selected nodes instead of checking them all.

Different Cases considered are as follows:

•Another node presents itself as the cluster head.

•A message repeats constantly.

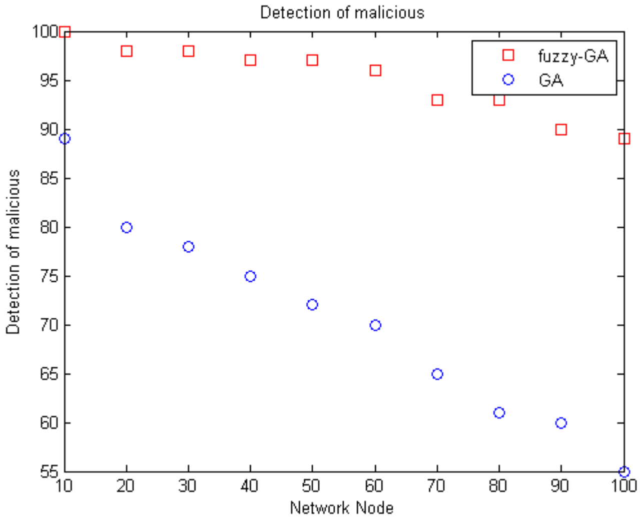

Figure4. *Detection of malicious with Fuzzy-GA*

6 REASEARCH SUMMARIES

We proposed a GA approach to raises the attack detection schemes. We demonstrated that clustering is a suitable method to reduce the energy consumption of the network and accordingly, the intrusion detection algorithm is proposed. The obtained results are summarized as follows:

1- Due to perceptible overhead of packet transmission in the network, the nature of clustering idea in integrating data and reducing the network traffic is highly desired and significant.

2- Considering that security and management tasks are costly in cluster head nodes, there is no need for other sensor nodes to keep this service active during the clustering. It will help reducing the average energy consumption of each node in the network.

3-In our proposed method, the whole sensor network is not checked to detect the attacker node and only the selected route is checked by fuzzy algorithm. As a result, we just consider the selected nodes instead of checking them all. Different Cases considered are as follows:

- ✓ *Another node presents itself as the cluster head.*
- ✓ *A message repeats constantly.*

7- REFERENCES

[1] R. Khanna, H. Liu and H. H. Chen,"Self-organization of sensor networks using genetic algorithms," in Proc. IEEE ICC, Istanbul, Jun. 2006.

[2] R.Khanna, H.Liu, and H-H. Chen "Reduced Complexity Intrusion Detection in Sensor, Networks Using Genetic Algorithm", IEEE ICC 2009

[3] F. Liu, X. Cheng , "Insider Attacker Detection in Wireless Sensor Networks" IEEE INFOCOM 2007.

[4] L.Guo, Q. Tang, "An Improved Routing Protocol in WSN with Hybrid Genetic Algorithm" Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), Vol.: 2, pp. 289 – 292, 2010.

[5] K. Lee, H. Jeon, and D. Kim, "Wormhole Detection Method based on Location in Wireless Ad-Hoc Networks", in

New Technologies, Mobility and Security: Springer Netherlands, 2007, pp. 361-372.

[6] O.Younis, M.Krunz , "Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges," IEEE Network (special issue on wireless sensor networking), vol. 20, issue 3, pp. 20-25, May 2006

[7] M.Ismail , M.Y Sanavullah, "Security Topology in Wireless Sensor Networks With Routing Optimisation", Authorized licensed use limited to: Korea Advanced Institute of Science and Technology, IEEE Explore, August 26, 2009