International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Research Article)

Check for updates

Genetic algorithm-based Wormhole attack detection in WSN

Pranav Dhama * and Prashanth K

Department of Computer Applications, R V College of Engineering, Bengaluru-560059, India.

International Journal of Science and Research Archive, 2023, 09(02), 795–802

Publication history: Received on 23 June 2023; revised on 08 August 2023; accepted on 11 August 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.9.2.0629

Abstract

Wireless Sensor Network (WSN) technology has received a lot of attention and has opened new applications. Examining security assaults on the network layer and coming up with a solution for them is one of the difficult topics in modern networks. Therefore, to achieve our goals, we must develop a technique that can identify an attack, prevent the attacker from accessing the network, and do so while consuming the fewest amounts of battery power. This technique must also use a simple, reliable algorithm. The use of a genetic algorithm is suggested in this research as a detection of wormhole attacks in WSNs. The strategy makes use of a genetic algorithm to investigate and identify the ideal group of parameters for a wormhole detection technique. Even in the case of enormous networks, the search for the most effective parameters may be carried out quickly and effectively by using this genetic algorithm.

Keywords: Wireless sensor network; Detecting attack; Genetic algorithm; Fuzzy function; Energy

1. Introduction

The many resource-constrained sensor nodes that make up wireless sensor networks (WSNs) are placed in a hostile environment. These sensor networks are made up of a lot of little sensor nodes that are used to gather and interpret environmental data. These small sensor nodes are made up of three components: sensors, information processing, and wireless information sharing. A significant attack known as a "wormhole" occurs when two attackers spread over the network build a virtual tunnel to communicate with one another. Through this tunnel, the attackers can exchange data far more quickly than they could through the real network. Data theft, network routing protocol disruption, and other attacks may all be carried out using this.

For many sensor network applications, security is a crucial need. This topic is particularly difficult due to the constrained 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.).

A simple internal attack can be carried out by the attacker by changing data, ignoring messages, choosing forwarding, producing obnoxious noises, etc. Internal attackers have a severe negative impact on network performance.

A possible method to choose the best set of parameters for a wormhole detection methodology is to use a genetic algorithm to detect wormhole assaults in Wireless Sensor Networks (WSNs). A population of possible solutions to a problem is created and evolved repeatedly via genetic algorithms, which are inspired by the process of natural evolution. In this situation, the genetic algorithm generates several combinations of parameters for the wormhole detection method to explore the parameter space. The method iteratively refines the population through a process of selection, crossover, and mutation to settle on the ideal set of parameters that maximize the performance of the detection approach.

* Corresponding author: Pranav Dhama

A low-cost sensor is unable to produce a log file for tracking and recognizing internal threats since it has a small memory capacity and limited computational power. Additionally, the central station cannot use the gathered data to identify the attacker node due to the networks massive scale and their infrastructure-less structures. To save battery life and bandwidth, a detection strategy should be locally focused and computationally effective. Additionally, since there are just a few communication activities that may be used as resources for tracing methods, finding internal attackers will become more difficult. considered that the algorithm needs to be based on regional information.

Sensing environmental events and sending the data to the base station for additional processing are the two basic tasks of wireless sensor networks. As a result, routing is a crucial process in sensor networks. For sensor networks, a variety of routing protocols have been put forth. Thus, the best method for ensuring security and identifying assaults in wireless sensor networks is routing. [7]

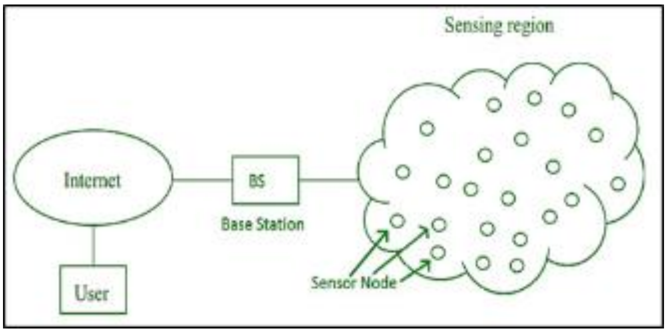

Figure 1 Diagram of Wireless sensor Network [13]

2. Literature review

[1] A method to ascertain the transit time of packets in wireless sensor networks was put out in the paper by Lakshmi Narayanan, K., Santhana Krishnan, R., Golden Julie, E., and their team. By transmitting this data to a specified judge node, a quick and precise estimation of the usual transit time to the destination was made possible. By employing this strategy, they hoped to improve the network's effectiveness and dependability by learning important information about packet transit times. This knowledge might be used to help with resource allocation and routing algorithm optimisation, which would eventually increase overall performance and make better use of the network infrastructure. The results of this study add to the expanding body of knowledge in wireless sensor networks and offer useful information for future developments in network organizations and management.

[2]Particle swarm optimization (PSO) was used by Tamilarasi N. and Santhi S.G. to spot wormhole threats in wireless sensor networks. PSO is an evolutionary optimization system that draws social behavior cues from schooling fish or flocking birds. They used PSO to determine the best method for detecting wormhole assaults, a particular kind of security risk that can obstruct communication and jeopardise the integrity of data in WSNs. Their suggested approach was successful, and the Network Simulator NS2, a popular simulation tool for researching and assessing network protocols and algorithms, adopted it as a result. NS2 now has improved security features thanks to the addition of PSO-based detection, making it a useful tool for researchers and developers working in the wireless sensor industry.

[3]Concentrated on automated defect detection and counting in radiographic weldment images, with a focus on flaws in weldment images. Various industries depend on weldment pictures, and finding flaws is essential for guaranteeing structural integrity and safety. They sought to speed up the inspection process and increase accuracy by using automated flaw detecting techniques. The research focused on creating methods and algorithms for quickly and accurately identifying potential flaws in radiographic weldment images. In industries that rely on weldment photos for essential evaluations, such developments have the potential to drastically minimize human errors and inspection time while also improving overall quality control procedures.

[4]A fresh approach was put out by Marcus Okunlola Johnson, Arish Siddiqui, and the research group to improve security in wireless sensor networks (WSNs). The strategy required confirming the legitimacy of the two-hop neighbours in charge of sending packets throughout the network. They did this to spot and identify prospective attacks when the neighbours' identities were fabricated, indicating hostile intent. This authentication procedure acted as a vital defence mechanism against various assaults that sought to take advantage of the weaknesses in WSNs. The network's overall integrity and data integrity were strengthened by confirming the authenticity of neighboring nodes, allowing for

more dependable and secure communication. The use of such a technique considerably supports ongoing efforts to strengthen the security of WSNs against sophisticated and malicious attacks.

[5]A unique method for spotting malicious wormhole attacks in wireless sensor networks (WSN) has been put forth by M.-H. Jao and colleagues. The strategy combines evolutionary algorithm Quantum-inspired Tabu Search (QTS) with popular finance metaheuristic algorithms (MA). The goal of the combination of QTS and MA is to increase the effectiveness and precision of detecting wormhole attacks, which can impair data integrity in WSNs and disrupt communication. While the use of MA improves robustness and adaptability in the detection process, QTS offers a search mechanism influenced by quantum mechanics that makes it possible to effectively explore enormous search regions. This creative combination of techniques offers a potentially effective way to improve WSN security, advance anomaly detection, and counteract sophisticated cyber threats in sensor networks.

[6]D.G. Anand, Dr. H.G. Chandrakanth, and Dr. M.N. Giriprasad's study looked closely at a number of attacks that compromise the layer's properties in wireless sensor networks. The study also concentrated on locating barriers and viable solutions to successfully fend off these assaults. The purpose of this analysis was to raise awareness of the WSN vulnerabilities and provide appropriate mitigation strategies. The study also posed important, unanswered research concerns that may open the door to further research into how to strengthen the security and resilience of wireless sensor networks against new dangers.

[7]Genetic algorithm (GA) was suggested as a method to accomplish decreased complexity intrusion detection in sensor networks in the work of Khanna et al. (2009). The researchers wanted to increase the effectiveness of intrusion detection procedures in wireless sensor networks (WSNs), thus they applied the GA. The system can recognise intrusions and efficiently react to them thanks to the evolutionary algorithm's robust and adaptive methodology. Additionally, because GA-based detection maximises resource utilisation and reduces pointless overhead, it helped extend the lifespan of WSNs. This method presents a viable technique for protecting the integrity and security of sensor networks while reducing the effects of intrusions, which will ultimately result in an increased network lifespan and better overall performance.

[12]Clustering techniques for wireless sensor networks (WSN) were fully investigated in the survey by Younis et al. (2006). The goal of the study was to determine the best clustering technique for enhancing routing and increasing the lifespan of WSNs. According to the study, some clustering algorithms outperformed others in terms of routing effectiveness and network durability. These algorithms optimised data transmission, lowered energy usage, and extended the network lifetime by clustering sensor nodes. The results of this survey provide insightful guidance for choosing appropriate clustering tactics, making a substantial contribution to the development of WSN architecture and management, ultimately improving the effectiveness and sustainability of the network.

Overall, the different methods put out for improving the security and effectiveness of wireless sensor networks (WSNs) are covered in this overview of the literature. The investigations cover techniques for measuring packet transit times, identifying wormhole assaults, automating weldment defect detection, authenticating two-hop neighbours, identifying malicious wormhole attacks, and employing evolutionary algorithms for intrusion detection and clustering. These methods aid in the general development of WSNs and open the door for additional study in this area.

3. Material and methods

In genetic algorithms, each solution could be shown as a binary string (chromosome) and the measurement of the relevant fitness function. A selected solution in an evolutionary process picks a person to set the standard for the following generation. The likelihood of selecting a solution is shown as follows:[11]

$$\mathbf{Pi}= \frac{F_i}{\sum_{j=0}^{N} F_j} \text{ ....}\mathbf{(1)}$$

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

In this study, a clustered network of randomly installed sensors is distributed using a genetic algorithm. The cluster heads partition the network into the ideal number of independent clusters. The suggested technique, which aims to identify the attacker nodes routing, executes the routing based on fuzzy selection and employs the evolutionary algorithm for clustering.

Due to an analysis of the sensor events in its neighborhood, the incompatible (malicious) nodes add to the observations of the network behavior.

The cases being considered include.

- The active trend of traffic routing, sensor location, data massage patterns, massage collision, and synchronized events.
- Increasing lifespan is a crucial concern in these networks. In a wireless sensor network, a long communication distance between the sensors and the sink uses up a lot of energy and reduces the network lifetime.[10] Clustering may greatly lower the wireless sensor network's energy consumption, which allows us to shorten communication distances and extend network lifetime.
- We first cluster the network using a genetic technique. It significantly contributes to reduced energy use and improved routing.
- In this study, a clustered network of randomly installed sensors is distributed using a genetic algorithm.
- The cluster heads partition the network into the ideal number of independent clusters.
- The suggested technique, which aims to identify the attacker nodes routing, executes the routing based on fuzzy selection and employs the evolutionary algorithm for clustering.
- Another trustworthy component that establishes the necessary safe connections between various nodes is the sink. The most trustworthy connections are made by the nodes closest to the sink node.
- Messages are sent and received between the various sensor nodes, and the sink oversees node authentication. The attack detection GA has monitoring nodes that keep an eye on the network and spot any conflicts with network requirements (such as communication costs and battery energy), which improves network dependability.

3.1. Algorithm

```
•  Start
•  node= Distribute (round (200))
•  Read Fuzzy function
   [center_ch] = GA; //GA start to select ch and membership of ch

   o  Random initial population (selection at random from distance and energy)
   o  Crossover (node); // A new kid with two parents is generated. After that, the separation between the new
      node and the sink is calculated.
   o  Mutation (node); // Each parent's chromosome undergoes a modification. After that, the separation
      between the new node and the sink is calculated.
   o  Merge (2new populations);
   o  Sort (node); // (energy, sink distance)
   o  population=size(new population)
   o  Sort (new population); //then (distance, energy) a second time.
   o  Making a cluster head; //calculating the separation between membership and clustering.
•  while(size(node) >= (sink_number + cluster_number))
      {
   o  [select1] = fuzzy_select(node);
   o  node_find = find(select_find == [select1]);
      // The selected route's node is added to the selected nodes list.
   o  if size (node_find)>1
       count1 = count1 + 1

       size-node--;

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

      End
   o  if (D < 1)
      Size-node--; // The node is dead.
       if size_node!= threshold
      [center_ch] = GA; //GA select ch
      } end while
      End
```

4. Simulation

In MATLAB, the suggested approach is simulated. We consider a 100 by 100 square. The network contains 200 nodes with a total starting energy of 1000 J. Ten clusters are thought to exist. The first and second dimensions of a three-dimensional (3D) matrix are made up of coordinates, and the third dimension is made up of energy. At the center of the plate, at coordinates (0, 0), is the sink.

Our definition of the genetic algorithm's values is as follows: initial population = 10, length of each chromosome = number of Ch * 2 = 10, crossover = 0, mutation = 4, mutation rate = 0. Each node serves as a hop counter to the sink.

Prior to choosing the best optimal route, MOGA first performs clustering and routing on the nearby nodes. A fresh clustering is carried out after the death of a node. The nodes along the ideal path are examined using GA. Then it finds and disables each node that meets the attack requirements. At the conclusion, a fresh clustering is performed. After disabling the attack nodes, the algorithm proceeds to select the optimal route based on the remaining active nodes and the information gathered from the GA-based examine of nodes along the ideal path for wormhole attack detection.

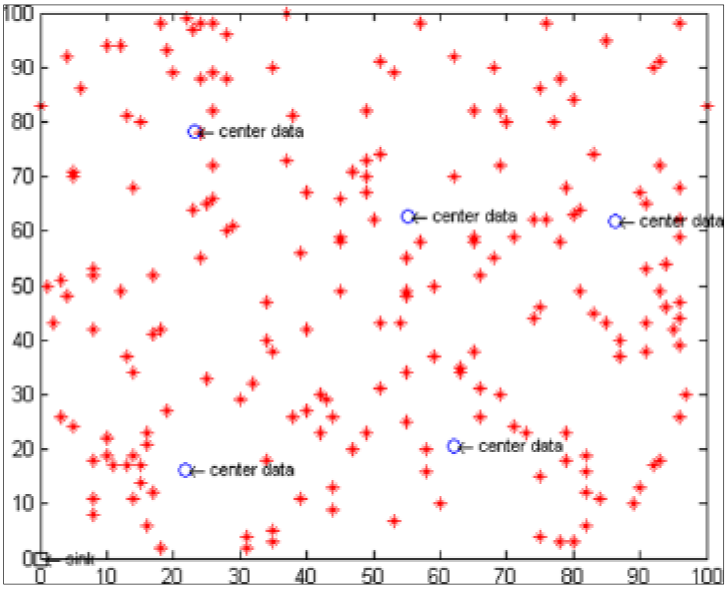

Figure 2 WSN in 100*100

Finally, a fresh clustering is performed once again to adapt to any changes caused by the disabled nodes and optimize the network structure based on the updated set of active nodes. This ensures the network maintains its efficiency and resilience in the face of node failures and potential attacks.

Using this adaptive clustering technique, the network is able to remain effective and resilient even in the face of node failures or possible assaults. The enhanced clustering assists in spreading network load, allowing for greater utilization of the resources at hand. While reducing the negative effects of disabled nodes on overall network performance, it enables effective data aggregation, routing, and communication inside the network.

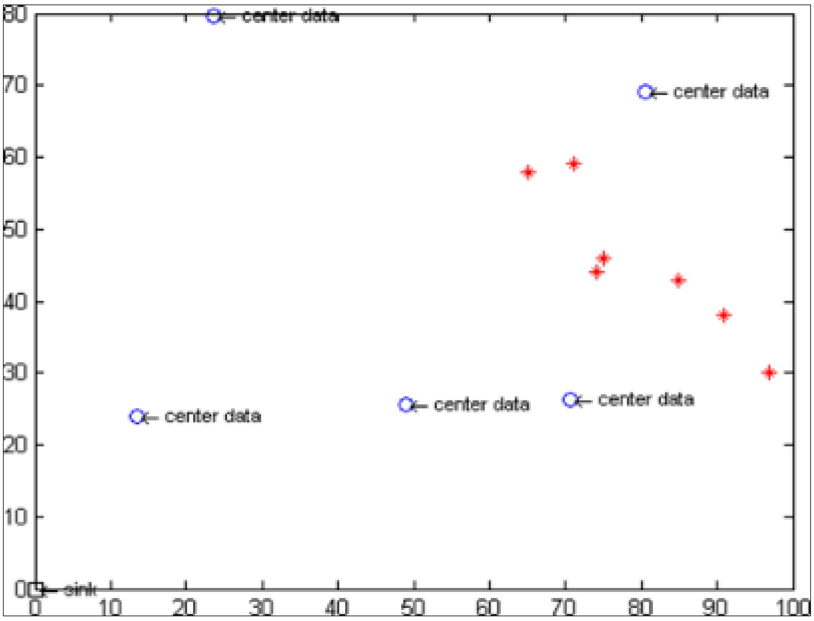

Figure 3 End of network lifetime

5. Result and discussion

In MOGA, the best route and battery usage are two criteria for optimality. The fuzzy technique is suggested to choose the best route out of those chosen by the genetic algorithm since it chooses numerous optimum routes. The route that has the lowest density and is closest to the sink is selected as the answer in the fuzzy technique.

As nodes are packed closer together, their energy consumption increases, as do the energy requirements of the routes that pass through them. Furthermore, the network's energy is conserved on nodes that are close to the sink since they need less energy to forward messages.

The network lifespan using the suggested approach and the network lifetime using genetic are contrasted. This approach has been tested on more than 200 different node counts.

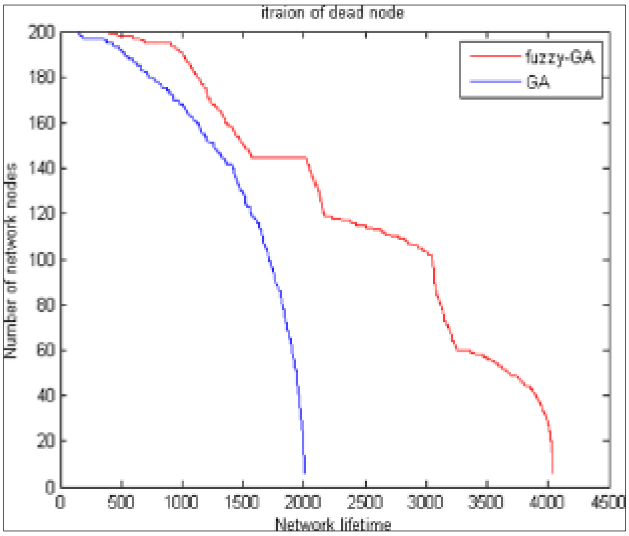

Figure 4 The network lifetime with the proposed method compared to the network lifetime with genetic algorithm

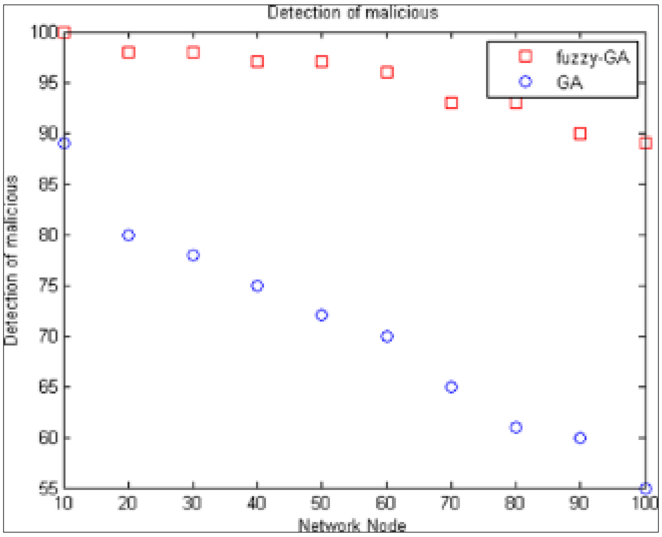

Figure 5 Detection of malicious with Fuzzy-GA

Only the chosen path is validated by a fuzzy algorithm in our suggested solution, leaving the rest of the sensor network unchecked for the attacker node. As a result, we don't verify all the nodes; we just consider the ones we've chosen.

The various cases considered are as follows

- The cluster head seems to be another node.
- There is a persistent message.

6. Conclusion

This research suggested a GA strategy to improve attack detection protocols. We showed that clustering is an effective way to lower the network's energy consumption, and as a result, the intrusion detection technique is suggested. The following is a summary of the outcomes

Due to the noticeable network overhead associated with packet transmission, the nature of clustering as a means of integrating data and minimizing network traffic is highly desirable and crucial.

- Other sensor nodes are not required to maintain this service during clustering since security and administration duties are expensive in cluster head nodes. It will aid in lowering the network's nodes' average energy use.
- Only the chosen path is validated by a fuzzy algorithm in our suggested solution, leaving the rest of the sensor network unchecked for the attacker node. As a result, we don't verify all the nodes; we just consider the ones we've chosen. The various cases considered are as follows:
  - The cluster head seems to be another node.
  - There is a persistent message.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Lakshmi Narayanan, K., Santhana Krishnan, R., Golden Julie, E. et al., Machine Learning Based Detection and a Novel EC-BRTT Algorithm Based Prevention of DoS Attacks in Wireless Sensor Networks, Wireless Pers Commun 127, 479–503 (2022).

[2] Tamilarasi N., Santhi S.G., Detection of Wormhole Attack and Secure Path Selection in Wireless Sensor Network, *Wireless Pers Commun* 114, 329–345 (2020).

[3] Shaymaa Al Hayalia, Osman Ucana, Javad Rahebib and Oguz Bayata, Detection of Attacks on Wireless Sensor Network Using Genetic Algorithms Based on Fuzzy, Int. Journal of Renewable Energy Development 8(1) 2019.

[4] Marcus Okunlola Johnson, Arish Siddiqui et al., A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks, International Journal of Computer Applications (0975 - 8887) Volume 174 - No.4, September 2017.

[5] M. -H. Jao et al., A Wormhole Attacks Detection Using a QTS Algorithm with MA in WSN, IEEE International Conference on Systems, Man, and Cybernetics, Hong Kong, China, 2015.

[6] D.G. Anand, Dr. M.N. Giriprasad, and Dr. H. G. Chandrakanth, Security Threats & Issues In Wireless Sensor Networks,International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 1,Jan-Feb 2012.

[7] 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.

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

[9] 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.

[10] 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.

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

[12] 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.