RESEARCH ARTICLE OPEN ACCESS

An Optimized Approach for Attack Detection and Prevention in Wireless Sensor Network

Vishal Kumar [1], Shaveta Jain [2]
Assistant Professor
GGS College of Modern Technology
Kharar (Mohali)

ABSTRACT
The Detection and Prevention system against several attacks has been developed in wireless sensor networks to secure the information and to provide the uninterrupted service to the reliable clients. The formulation of opinion of nodes of different neighbors or Trust value plays important role in the detection system to avoid attacks. The attack detection system always follows the behaviors of nodes to identify the attack formats and prediction of future attacks. In this paper, the Genetic Algorithm theorem is designed that gives better result by employing different parameters. This proposed work is more reliable and efficient than the previous and the results are proved and verified in MATLAB. By using this algorithm truth values of nodes will be maintained better and the accuracy of system will be enhanced through this methodology.

Keywords:-Wireless sensor network, Genetic Algorithm, Crossover, Mutation, Throughput, Packet Delivery Ratio, Trustworthiness, attacks, nodes, routing methodologies.

I. INTRODUCTION

Different kind of applications have different kind of network bearing constraints and features but still most of the issues are common or same which makes them homogenous. The positions of the sensor node become most sensitive point while the process of deployment of nodes. But sometimes coverage area of networks creates an issue because it also directly depends upon the positions of the nodes.

Since many WSN include bulk of nodes and some of their features cannot be measured in a simple manner, the process of selecting the geographical positions of the nodes for an optimal resulting network referred to as WSN layout problem can make it very complex. This problem recalls the unicost set covering problem also known as NP. Therefore, Metaheuristic is a option to solve this problem. In most of the problems the focus is on to reduce the Energy consumption as well as nodes used in the network. The number of nodes can create a problem while covering the network. While display the network it has to face the various considerations.

The coverage has to follow some rules or restrictions and highly coverage area is preferred. The reduction of sensor nodes is not for a specific purpose it is just to reduce the cost factor. The lifetime of a network depends upon the energy consumption so energy management is the most critical issue in the network. WSNs are commonly used for real-world physical environments to measure various parameters. Therefore, the characteristics of a WSN must be considered for efficient deployment of a network.

II. TYPES OF SECURE ROUTING PROTOCOLS

Routing techniques are required for sending data between the sensor nodes and base station workstations for communication. Different routing protocols are introduced for wireless sensor network. These protocols are classified as given:

i) Proactive protocols: In proactive protocol the node switch on their sensor and transmitters, sense the environment and

transmit the data to a BS through the predefined route. Example: Destination Sequenced Distance Vector routing (DSDV).

ii) Reactive protocols: If there are sudden change changes in the sensed attribute beyond some predetermined threshold value, the nodes immediately react. This type of protocol is used in time critical applications. Example: Ad-hoc On-demand Distance Vector routing (AODV).

iii) Hybrid protocol: Hybrid protocols incorporate both proactive and reactive concepts. They first compute all routes and then improve the routes at the time of routing. Example: Temporally Ordered Routing Algorithm (TORA).

III. GENETIC ALGORITHM

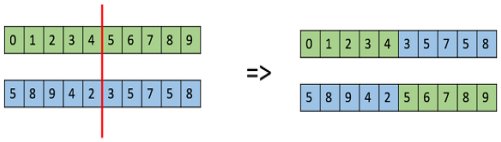
Genetic Algorithm (GA) is a search-based optimization method build on the principles of Genetics and Natural Selection. It is often used to find optimal or near-optimal solutions for difficult issues that otherwise would take a lifetime to solve. It is often used to solve optimization problems, in research, and in machine learning. There are different parameters of Genetic Algorithm given below:

a) Crossover

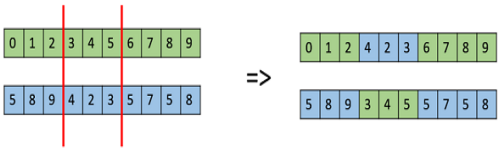
The crossover operation is similar to reproduction. In this method more than one parent path is selected and one or more off-springs paths are produced using the genetic material of the parent paths. Crossover is usually applied in a genetic algorithm with a high probability.

Types of Crossover

i) One Point Crossover: In this one-point crossover, a random crossover point is selected and the tails of its two parent path are swapped to get new off-springs.



ii) Multi Point Crossover: Multi point crossover is a generalization of the one-point crossover wherein alternating segments are swapped to get new off-springs paths.



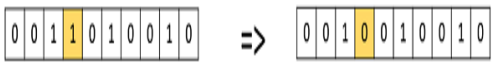
iii) Uniform Crossover: In a uniform crossover, we don't divide the paths into segments, rather we treat each path separately. In this, we essentially flip a coin for each path to decide whether or not it'll be included in the off-spring path. We can also bias the coin to one parent, to have more genetic material in the child from that parent.

b) Mutation

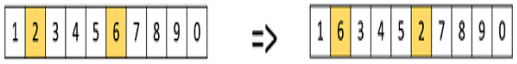
The mutation is similar to swapping. In this method the small random tweak is introduced in the parent and new solution is generated. Mutation is usually applied in genetic algorithm with a low probability.

Types of Mutation

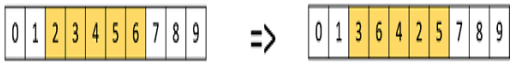
i) Bit Flip Mutation: In this bit flip mutation, we select one or more random bits from a given path and flip them and form a new path.



ii) Swap Mutation: In swap mutation, we select two positions on a given path at random, and interchange the values.



iii) Scramble Mutation: Scramble mutation is also popular with permutation representations. In this, from the entire path, a subset of path is chosen and their values are scrambled or shuffled randomly.



IV. PROPOSED WORK

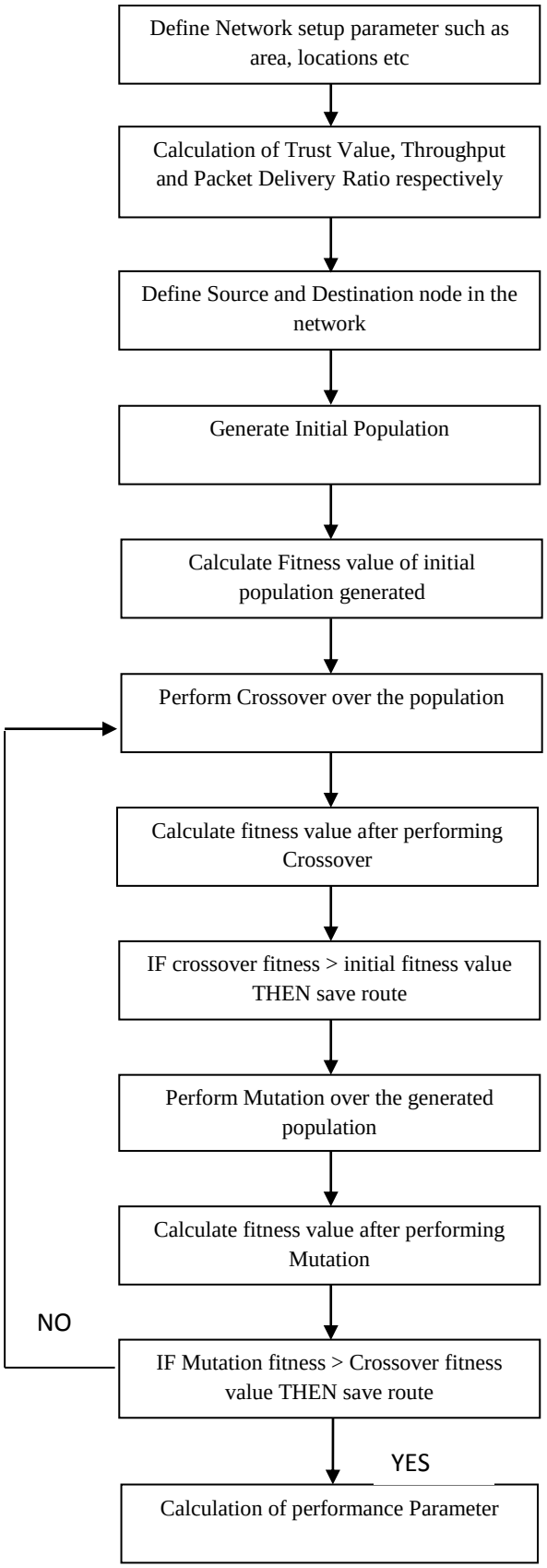
In the proposed technique the security of the system is increased by changing the standard for route selection. In the previous techniques only the reputation of nodes was considered for the selection of route but in this proposed technique some other quality of service parameters are also considered along with the reputation of nodes. The factors that are to be considered for route selection are:

- Trustworthiness of node
- Packet delivery ratio
- Throughput

The reputation of the nodes in WSN will be checked and then area will be defined along with the genetic algorithm for route selection to get the optimized solution of node selection in the route form source to destination which will be free from different types of attacks.

V. FLOWCHART

The flow chart for the proposed algorithm is shown as:



VI. METHODOLOGY OF PROPOSED WORK

Methodology for the proposed work is mentioned below:

1. Initialize the network layout with nodes in network, area , their locations etc
2. Calculate Trust Value, Throughput and Packet Delivery Ratio respectively for further evaluation.
3. Initialize source and destination node in the network for transmission of packet.
4. Generate initial population of the network.
5. Calculate fitness value of initial generated population for application of GA.
6. Next step is to apply GA for finalized route selection with maintaining the network requirement with high QoS. For that reason apply crossover over the initial population
7. Calculate fitness value after applying crossover to estimate the required fitness value obtained or not.
8. Checks whether the crossover fitness value is higher or greater than initial fitness value or not if so saves the respective route.
9. Now perform mutation over the initial population to acquire best fitness value.
10. Evaluate fitness value after performing mutation so that required fitness value can be acquired.
11. Checks whether the mutation fitness value is higher or greater than crossover fitness value or not if so saves route.
12. Repeat the process to the no. of iterations until desired results not found.
13. Parameter calculation for analyzing the results.

VII. RESULTS AND DISCUSSIONS

In this section of Results and discussion we have discussed about the results that were obtained by applying proposed method and the traditional method of routing. The graphs represent the network performance like delivery ratio. These results are obtained to show the efficiency of the proposed method. Thus, the following result shows the step by step method to calculate the path and find the best path to send the packet from source to destination.

This graph shows the routing path from the source to the destination. After the selection of the source and the destination node the route selection for sending the data is done.

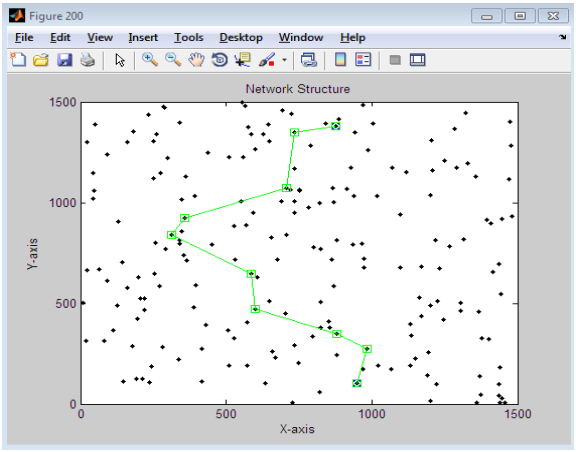


Figure 1 Selected route of network structure used by source to the destination

This graph below represents the packet delivery ratio at the initial and final stage of the selected route. After performing transmission, final PDR evaluation let the user know about the efficiency of the proposed work. Because Packet deliver ratio is increased so packet reached at the destination are higher in count.

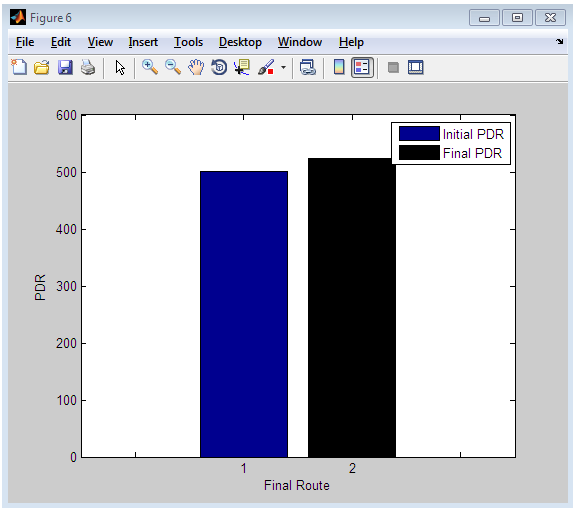


Figure 2 Packet Delivery ratio of the proposed method from initial to final

This graph below represents the trust value at the initial and final stage of the selected route. At the initial stage trust value is less as compared to the final trust of the network. Trust of the network helps to identify the reliability for the proposed work.

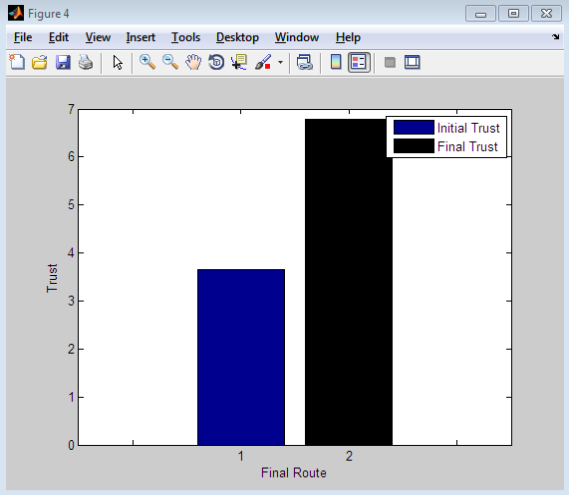


Figure 3 Initial and final trust value of the selected route

Throughput defines the rate of successful message or packet delivery over a communication channel. Thus it should be higher for the reliable network. At the final stage of the network throughout has increased which symbolized the effectiveness of the present work.

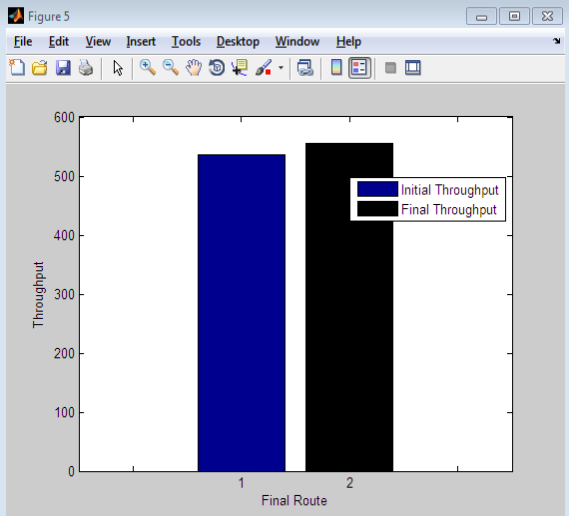


Figure 4 initial and final throughput of the present work.

The graph given below shows the comparison between the proposed and the traditional approach. From the results obtained it is concluded that proposed system is more efficient, reliable and accurate as compared to the traditional approach. So the proposed algorithm is considered to be a better technique in terms of Packet Delivery ratio, trustworthiness and Throughput.

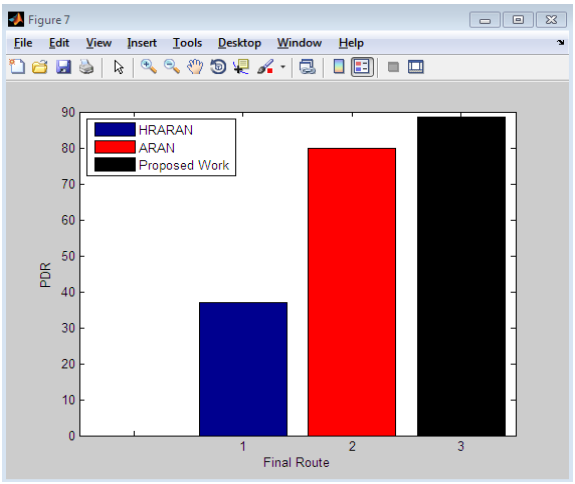


Figure 5 comparison of different techniques w.r.t present work in terms of Packet Delivery Ratio

The graph given below shows the throughput of the proposed system in comparison with the traditional algorithms. From the graph it shows that throughput of the proposed system hiked from the other traditional methods.

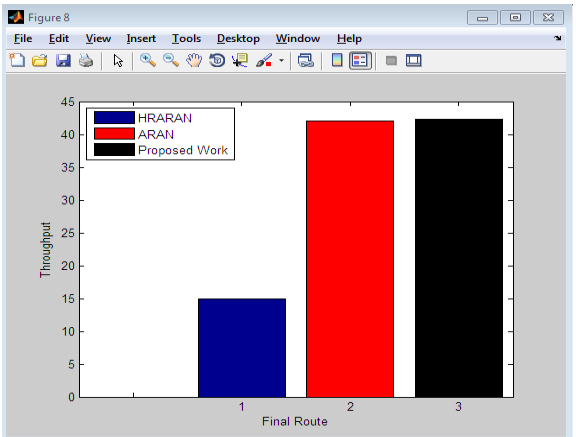


Figure 6 comparison of different techniques w.r.t present work in terms of Throughput.

VIII. CONCLUSION AND FUTURE SCOPE

To increase the efficiency and performance of the network and also find the optimal and shortest path we have implemented a new approach. In this new approach the different parameters are introduced such as throughput of nodes, trust and Packet delivery ratio. Growth in PDR, trust value and throughput concludes the efficiency of the network. The proposed methodology provides a network which is faster than earlier proposed approaches. Including this as security is main concern in today networking so this paper provide security for data transmission which make it an approach of fast secured data transmission.

In future more parameters such as distance, energy or range can be included with the proposed parameters to acquire high data transition.

REFERENCES

[1] Shesh Kumar Sharma, "Routing Protocols and Security Issues in MANET: A Survey", IJETAE, Vol 4, Issue 4, Pp 918-924, 2014

[2] Jingsha he, "Analysis of Typical secure routing protocols", IJSIA, Vol 8, Issue 6, Pp 41-50, 2014

[3] Rachid Haboub, "Secure Routing in WSN", IJDPS, Vol 2, Issue 6, Pp 291-300, 2011

[4] Kahina Chelli, "Security Issues in WSN: Attacks and Countermeasures", WCE, Vol 1, Pp 1-6, 2015

[5] Vikash kumar, "Wireless Sensor Network: Security Issues, challenges and solutions", IJICT, Vol 4, Issue 8, Pp 859-868, 2014

[6] Kimaya Sanzgiri, "A Secure Routing Protocol For Adhoc networks", Pp 1-10

[7] Sunil Tanewja, "Encryption Scheme for Secure Routing in Ad Hoc Networks", IJAT, Vol 2, Issue 1, Pp 22-30, 2011

[8] A Senthilkumar, "Secure Routing in WSN: Routing Protocols", IJCSE, Vol 2, Issue 4, Pp 1266-1270, 2010

[9] Amith Khandakar , " Step by Step Procedural Comparison of DSR, AODV and DSDV Routing protocol ", ICCET, vol 40, Pp 36-41, 2012

[10] Rajesh Sharma, " Dynamic Source Routing Protocol (DSR) ", ijarcsse, vol 3 (7), Pp 239-241, 2013

[11] Amit N. Thakare , "Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks", ijca, vol 4, 2010

[12] Rajeshwar Singh , "Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks. " ,ijana, vol 2(4), Pp 732-737, 2011

ABOUT AUTHORS

Vishal Kumar obtained B.Tech degree in Computer Science & Engineering (CSE) in 2013 from Ferozepur College of engineering & Technology, Ferozepur, Punjab. He is currently pursuing M.Tech degree in Computer Science & Engineering from GGS Collegee of Modern Technology, Kharar, Punjab. His research area are routing process and security in wireless sensor network.

Shaveta Jain received her B.Tech degree in Information Technology from Global College of Engineering & Technology, Khanpur Khui, Punjab, India in 2012, the M.Tech degree in Computer Science & Engineering from Maharishi Markandeshwar University, Mullana, Haryana, India, in 2014. She is working as Assistant Professor in Department of Computer Engineering, in GGS College of Modern Technology Kharar Chandigarh. Her research interests include Mobile Ad-hoc Networks.