ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 8, August 2016

A Defense Mechanism to Prevent Wireless Sensor Network from Sybil Attack

Dinesh Mittal[1], Ashok K.Goel[2]
Department of Electronics and Communication Engineering
Giani Zail Singh Campus College of Engineering and Technology
Bathinda – 151001, India
[1]M.tech, [2]Professor & Head of Department

***Abstract*— Wireless Sensor Network (WSN) network consists of a number of communicating wireless sensor nodes which do not have any form of fixed infrastructure. The security in such networks has become a significant topic within the research community. In WSN some attacks aimed at specific node and some on multiple nodes. Sybil attack is different from all that attacks because the attack occurs on a specific node and that node acts like multiple nodes. We propose a technique to do this in AODV using Genetic Algorithm approach. GA helps to detect and prevent the attack by its fitness function optimization technique. Unfit nodes are successfully avoided and fittest nodes are selected for the communication path. In this way, new attack free path is proposed for communication from source to destination.**

***Keywords*—AODV, Genetic Optimization Algorithm, Security, WSN**

I. INTRODUCTION

Wireless sensor networks consist of a number of wireless communicating nodes which collaborate with each other to perform sensing tasks in given environment. They sense the changes occur in different parameters of the environment. These sensing nodes are distributed or placed according to the requirements of the application. Basically these nodes are of low performance. These work with other nodes collectively to perform specific tasks.

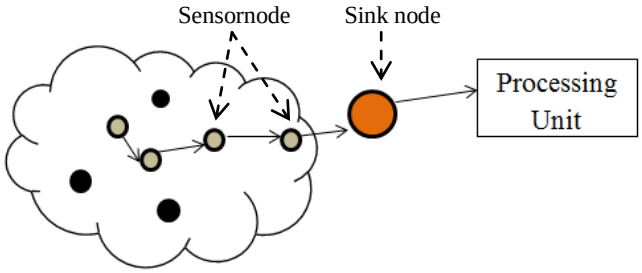

Fig. 1: Wireless sensor network Model

WSNs experience the ill effects of mixed bag of security attacks and dangers, for example, denial of service (DoS), flooding attacks, wormhole attack, blackhole attack, etc[2].

A. *Sybil Attack*

When multiple identities from same malicious node have been created then that attack is the Sybil attack. The malicious node acts like two or mode nodes instead single node. By act as multiple nodes or identities, the attacker utilized more energy of the sensor nodes and minimizes the life period of same.

Initially depicted by Microsoft specialist John Douceur, a Sybil attack depends on the way that a system of PCs can't guarantee that every processing component is an unmistakable, physical PC. Various powers have tried to set up the identities of PCs on a system (or hubs) by utilizing software, for example, VeriSign, utilizing IP locations to recognize hubs, passwords and usernames, etc.

This attack makes more threatening problems in distributed storage, voting and resource allocation. This attack is very vulnerable to wireless sensor network and can be gateway of other attacks such as wormhole, sinkhole, selective forwarding etc.

B. *AD HOC On-Demand Distance Vector (AODV) Protocol*

AODV is one of reactive routing protocol which creates path from source node to destination node only on demand. Itdoes not maintain any routing table like DSDVwhich maintains multiple route cache entries for each and every destination. This protocol is very sensitive to any change occur in the link conditions. In case when a link fails to communicate then whole information is sent only to the effected node. Besides it has an advantage that the network has least routing traffic as routes are built only on demand. There are three messages used to discover and maintain the route from source to destination node that are Route Request (RREQ), Route Error (RERR) and Route Replies (RREP). RREQs and RREPs are the rouse establishing messages whereas RERRs generated when there is failure of link occur.

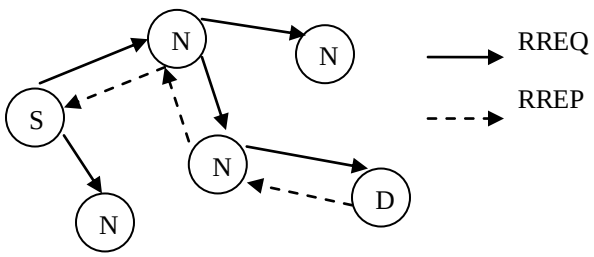

Fig. 2: AODV Protocol

c. *GA (Genetic Algorithm)*

According to Goldberg et al., 1989, GA is commonly used in applications where search space is huge and the precise results are not very important. The advantage of a GA is that the process is completely automatic and avoids local minima. The main components of GA are: crossover, mutation, and a fitness function. A chromosome represents a solution in GA. The crossover operations used to generate a new chromosome from a set of parents while the mutation operator adds variation. The fitness function evaluates a chromosome based on predefined criteria. A better fitness value of a chromosome increases its survival chance. A population is a collection of chromosomes. A new population is obtained using standard genetic operations such as single-point crossover, mutation, and selection operator. The proposed GA is used to generate balanced and energy efficient data aggregation trees for wireless sensor networks.
The genetic algorithm uses following types of rules at each step to create the next generation from the current population:
Initialization: Many individual solutions are randomly generated to form the population.

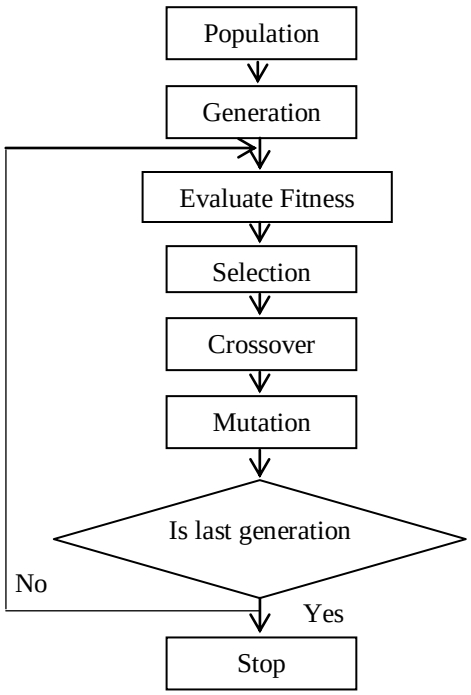

Fig. 3: Genetic Algorithm

Selection: Individual solutions are selected through fitness based process where fitter solutions are selected.
Reproduction: Second generation population of solution are generated through genetic operators that are crossover and mutation. This process continues until a new population of solution is generated.
Fitness Function: It is particular type of objective function which is used to summarize as a single fig. of merit how close a given design solution is to achieve the set aims.
Termination: Process of reproduction is repeated until a termination condition has been reached.

II. RELATED WORK

Guo, Wang and Han talked about the three different kinds of enhanced genetic algorithms that are hybrid, interval and hybrid interval genetic algorithms. They applied GA to interval optimization process first time[13].

Sharma and Ghose presented that all the security threats reduces the network performance. They also concluded that the exact solution to avoid these attacks depends upon the motive of wireless sensor network[5].

Sujatha developed a specification based intrusion detection system to detect blackhole attack using GA in WSN with AODV and successfully detect the blackholeattack[4].

Vamsi and Kant applied sequential hypothesis test based technique to detect Sybil attack and this method accurately detect the attack. They also concluded that the network traffic seriously effected if the number of Sybil node increases in the network[6].

Kasiran and Mohamad concluded that Sybil attack give more impact on performance of mobile adhoc network than wormhole attack. They took throughput as a network parameter for comparison[14].

III. SIMULATION MODEL

The main objective is to establish a Sybil attack free communication path between source and destination. For this, Genetic Algorithm is used with fitness function optimization. Genetic Algorithm uses the law of selection and evolution. In this method, first of all data sets called population are identified. After this, new chromosomes are formed by encoding these data bits using bits, characters or integers. Now the next operation is to determine the genuine chromosome by evaluation function process. During this process, crossover and mutation are performed[5]. The selection of chromosome is performed until fit chromosome is selected. Figure 4 shows the proposed model.

The genetic algorithm is applied to the each and every node who replied with RREP message to the source node. In the process of “Threshold Evaluation”, threshold value of energy consumed by the node, is evaluated and threshold comparison is performed using this value. In last only fit nodes are selected to establish attack free path from source to destination node.

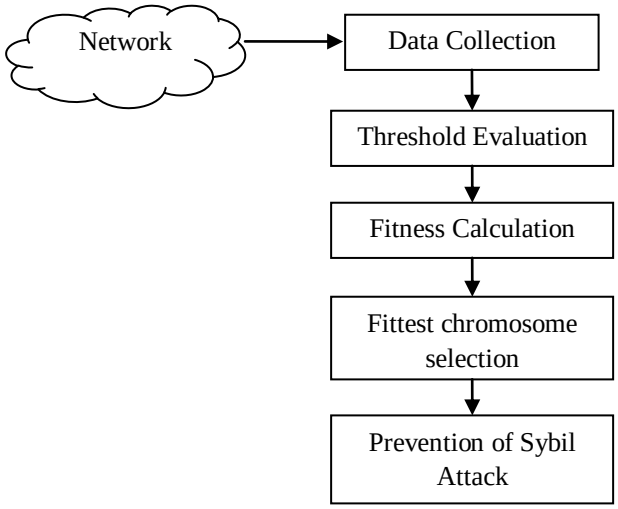

Fig.4: Proposed Model

IV.SIMULATION RESULTS

The given technique is applied to a WSN with 50 node density in area of 1000m x 1000m. The sensor nodes are distributed in the given region randomly. The first job is to select the source node and destination node that is from which node information is to be transfer to which node. When source and destination nodes are selected from the given region then a communication path is built. This path is shown by green colored nodes. Till no optimization technique is applied on them.

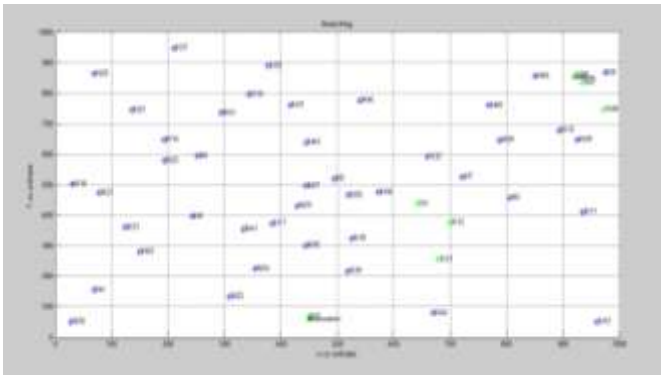

Fig. 5: Network Deployment

After this, GA is applied to the network and initialize from the source node. The node fail the threshold comparison is declared as unfit for the path and marked red as attack affected node.

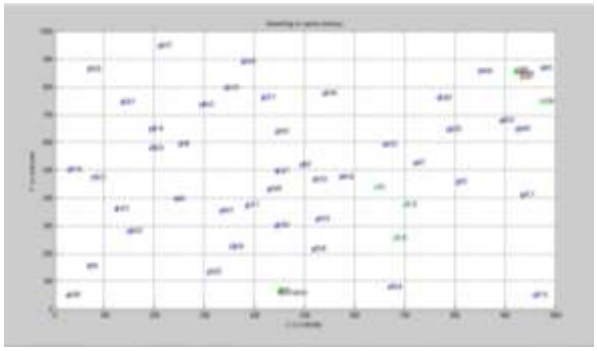

Fig. 6: Detection of Sybil node

The node successfully passed the threshold comparison is declared as the fit node and selected as path node for path from source to destination. In following fig. the path from source to fit node is shown:

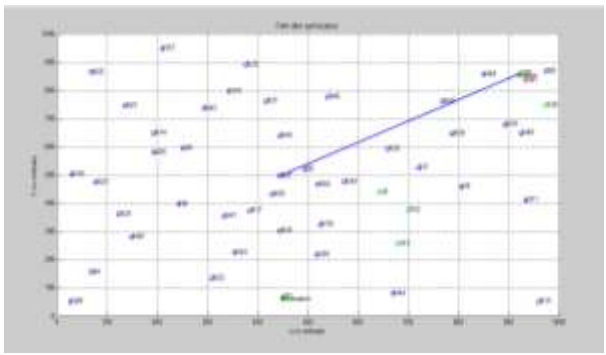

Fig. 7: Path from source to 1st node

After selecting 1st node, same process is repeated on this node as on source node to select next path node and the next node is shown in next fig.:

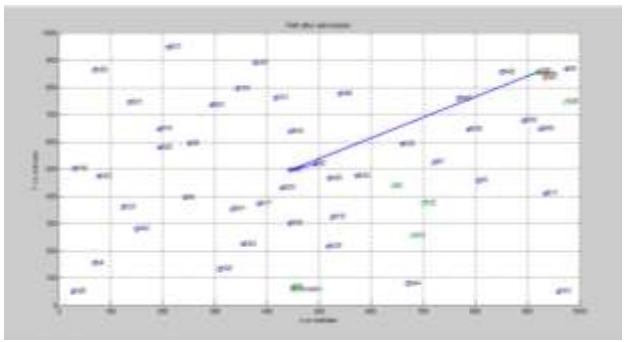

Fig. 8: Path 1st node to 2nd node

Again GA is applied to the 2nd node and searched for next fit node. The process is repeated on every node to find next fit node for path till destination node as shown in following fig.s:

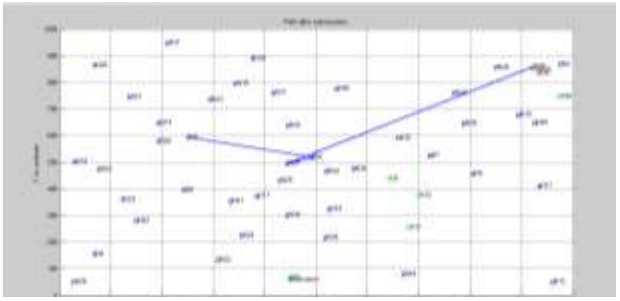

Fig. 9: Path 2nd node to 3rd node

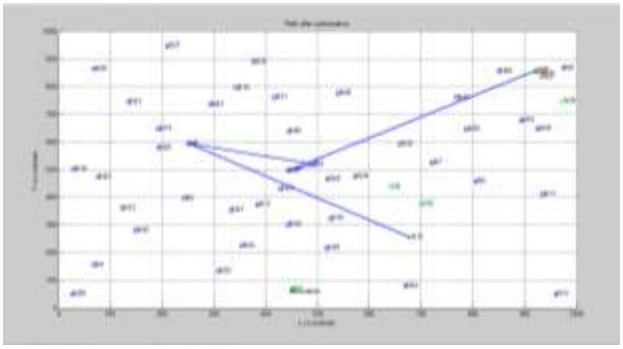

Fig. 10: Path 3rd node to 4th node

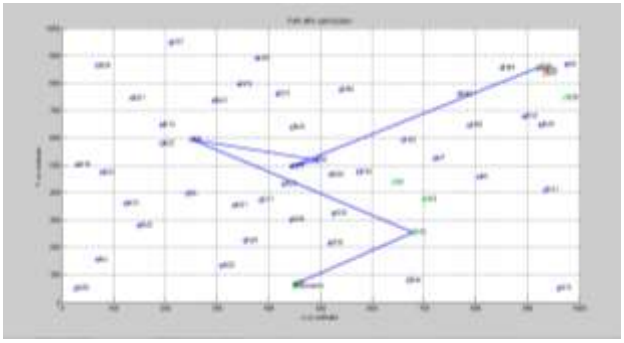

Fig. 11: Path 4th node to destination

Hence, new attack free communication path is built from source to destination by ignoring the affected node from the path.

V. CONCLUSION

Peer-to-peer systems play an ever-increasingly important part of our daily lives. However, most of the peer-to-peer systems are vulnerable to Sybil attacks. In order to design more efficient and practical Sybil defenses, an implementation based on Genetic algorithm is presented. It has been seen that the affected node was successfully removed from the communication path and a new attack free path has been formed. It is concluded that Sybil attack prevention is achieved at greater rate when Genetic Algorithm has been used. This mechanism can also be tested for more number of nodes in network.

REFERENCES

[1] C.Piro, C.Shields and B.N.Levine (2006), "Detecting the Sybil attack in mobile ad hoc networks," in Proc. Securecomm Workshops 2006, pp.1–11.

[2] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," IEEETrans. Mobile Comput., vol. 2, no. 3, pp. 257–269, Jul.–Sep. 2003.

[3] E.E.Khin and T.Phyu (2014), "Impact of black hole attack on AODV routing protocol", International Journal of Information Technology, Modeling and Computing, vol. 2, pp. 66-70.

[4] James Newsome, Elaine Shi, Dawn Song and Adrian Perrig (2004), "The Sybil Attack in Sensor Networks: Analysis and Defenses", IPSN 04, April 26-27,2004, Berkeley, California, USA.

[5] K.S.Sujatha, V.Dharmar and R.S.Bhuvaneswaran (2012), "Design of Genetic Algorithm based IDS for MANET", International Conference on Recent Trends in Information Technology (ICRTIT), IEEE, pp.28-33.

[6] Kalpana Sharma and M.K.Ghose (2010), "Wireless Sensor Networks: An Overview on its Security Threats", International Journal of Computer Applications (IJCA) special issue on MANETs, pp.42-45.

[7] P.RaghuVamsi and Krishna Kant (2014), "Sybil Attack Detection using Sequential Hypothesis Testing in Wireless Sensor Networks", International Conference on Signal Propagation and Computer Technology (ICSPCT), IEEE, pp.698-702.

[8] PengfuiGuo, Xuezhi Wang and Yingshi Han (2010), "The Enhanced Genetic Algorithms for the Optimization Design", 3rd International Conference on Biomedical Engineering and Informatics (BMEI 2010), IEEE, pp.2990-2994.

[9] Rajeshwar Singh (2011), "Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks", International Journal for Advanced Networking and Applications 732 Vol. 02, issue. 04, pp. 732-737.

[10] S.Hazra and S.K.Setua (2012), "Sybil attack defending trusted AODV in ad-hoc network", 2nd International Conference onComputer Science and Network Technology (ICCSNT), IEEE, pp.643-647.

[11] SimranjeetKaur, Gagangeet Singh Aujla and SahilVashist (2014), "Detection and Optimisation Techniques against Sybil Attack on MANET", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol. 4, issue 8, pp.369-375.

[12] T.N.Manjunatha, M.D.Sushma and K.M.Shivakumar (2013), "Security Concepts and Sybil Attack Detection in Wireless Sensor Networks", International journal of Emerging Trends and Technology in Computer Science (IJETTCS), vol. 2, issue 2, pp.383-390.

[13] T.G.Dhanalakshmi, Dr.N.Bharathi and M.Monisha (2014), "Safety Concerns of Sybil Attack in WSN", International Conference on Science Engineering and Management Research (ICSEMR), IEEE, pp.1-4.

[14] YutengGuo, Beizhan Wang, Xinxing Zhao, XiaobiaoXie, Lida Lin and Qingda Zhou (2010), "Feature selection based on Rough set and modified genetic algorithm for intrusion detection", 5th International Conference on Computer Science and Education (ICCSE), IEEE, pp.1441-1446.

[15] ZolidahKasiran and Juliza Mohamad (2014), "Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV", Fourth International Conference on Digital Information and Communication Technology and it's Applications (DICTAP), IEEE, pp.81-84.