International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 3, Issue 1, pp: (103-109), Month: January - March 2015, Available at: www.researchpublish.com

Prevention of Sybil Attack on LEACH Protocol in WSN Using BCO

Chitwan Bedi[1], Er. Harpal Singh[2]

[1,2]M.Tech in Electronics and Communication Department
[1,2]Rayat and Bahra Institute of Engineering and Biotechnology, Mohali, India

Abstract: **In this paper, a technique is proposed to prevent the Sybil attack on LEACH protocol in WSN. An optimized path is obtained when Sybil attack occurs on LEACH protocol during routing using an optimized algorithm. The proposed technique is based on Bee Colony Optimization (BCO) that helps to prevent the attack. The parameters chosen for the work are True Positive Rate, False Positive Rate and Detection Rate. The Detection Rate obtained using BCO is 96.5%. It also includes comparison with previous prevention methods of Sybil attack based on Detection Rate. The whole result simulation has been taken place in MATLAB environment.**

Keywords: **WSN, LEACH protocol, Sybil attack, BCO.**

1. INTRODUCTION

Wireless sensor network(WSN) consists of a large number of sensor nodes which are equipped with limited battery source and are linked each other by wireless medium and performs various sensing tasks[1].These sensor nodes interface with the physical environment where data can be collected , processed, analysed and send the final aggregated data to an external base station. WSN's are widely used for a variety of applications such as area monitoring, tracking, health applications, military application (surveillance) etc[2].There are various routing protocols in WSN which govern the movement of the information collected by sensor nodes. One such protocol is LEACH protocol in WSN which is discussed as follows.

1.1 LEACH Protocol:

LEACH stands for Low energy Adaptive clustering Hierarchy [3] is a hierarchical based routing protocol for sensor network. This clustering hierarchy helps in fragmenting the network into small region called clusters. Each cluster consists of group of nodes and a cluster head (CH).It is the responsibility of cluster head to aggregate and transfer the data collected from the sensor node of a cluster to the base station.[4] The LEACH protocol operates in rounds and each round consists of two phases as shown in fig.1: setup phase and steady phase.

(i) Setup phase: In the setup phase, the cluster head is elected. The sensor nodes elect a cluster head based on the Threshold equation T(n)[5]:

$$T(n)=\begin{cases}\dfrac{P}{1-P*(r \bmod \frac{1}{P})} & \text{if } n \in G \\ 0 & \text{otherwise}\end{cases}$$

Where p is the desired percentage to become a cluster head, r is the current round and G is the set of nodes that have not become the cluster head in the last 1/p rounds. Each node chooses a random number between 0 and 1.If this random number is less than threshold value T(n) then the node becomes the cluster head for the current round.

(ii) Steady state phase –In the steady state phase the cluster head collects the data from the nodes using TDMA schedule and after aggregating and processing the data transfer it to the base-station as shown in fig.2.The steady state phase is much longer than the set-up phase.[5]

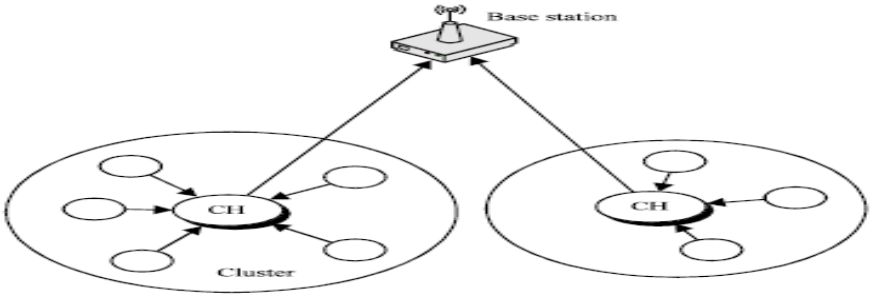

Fig.1 LEACH Protocol clustering

Fig. 2: LEACH Protocol Phases

1.2 Sybil Attack:

Wireless sensor network provides services in hostile environment which makes them vulnerable to various attacks. One such attack is identity based attack known as Sybil attack [6] which poses great threat to the routing based protocol such as LEACH protocol. In Sybil attack an individual identity appears as multiple simultaneous identities in the network as shown in fig.3.In other words a particular node in the network is present at more than one place simultaneously. This attacks were first observed in p-to-p networks [7].Sybil attack has the ability to disable the legitimate nodes from accessing the resources and in such cases unjust resources are assigned directly. The Sybil attack violates the one-to-one mapping between entity and identity. This attack causes its adverse impact on different schemes like multipath routing, data aggregation, voting, fair resource allocation and misbehaviour detection.[8]

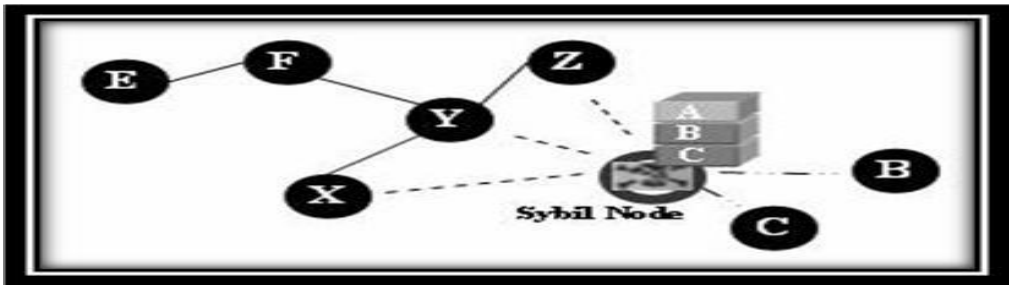

Fig. 3 Sybil Attack

The rest of the paper is organised as: Section 2 presents the proposed scheme to prevent Sybil attack in LEACH protocols. Section 3 presents the results and analysis section 4 concludes the work.

2. PROPOSED SCHEME

The proposed scheme is introduced to prevent the Sybil attack on LEACH protocol in WSN. An optimized path is obtained when Sybil attack occurs on LEACH protocol during routing using an optimized technique known as Bee Colony optimization (BCO) [9] to prevent the attack.

2.1 Bee colony optimization:

The BCO is inspired by the behaviour of bees in nature. Many natural and biological processes affect this optimization technique.BCO has been proposed by Lucic and Teodorovic [9]. The process of BCO is inspired by foraging behavior in honeybees. To efficiently solve difficult combinatorial optimization problems, the multi agent system was to be build. This forms the need to form BCO. The artificial bee colony acts slightly similar and slightly in a different way from bee colonies available in natural system. To solve big and complex real-world problems the BCO meta-heuristic technique is is used as an efficient tool. BCO has the tendency to solve and obtain high quality solutions of hard combinatorial problems within a less time as such in computers. The stochastic, random-search technique is used in BCO. The BCO technique uses the same behavior relation between the way by which the bees search their food, and the way in which

combinatorial optimization problems are searched by optimization algorithms. The technique behind the BCO is to build the multi agent system that is capable of solving difficult combinatorial optimization problems. Artificial bees investigate through the search space looking for the feasible solutions. The artificial bees coordinate and exchange information in order to get best of best solutions. By using collective information and sharing it between themselves, artificial bees lay more concentration on promising places, and slowly stop solutions from the less promising areas. So through step by step process, artificial bees collectively generates and/or modifies their solutions. Until and unless some stopping criteria is fulfilled the BCO search runs in iterations. To represent a good basis for parallelization the BCO technique performs in a self-organized and in decentralized way. It also has the ability to keep itself away from being trapped in local minima. Swarm intelligence is the part of Artificial Intelligence. The Bee Colony optimization Algorithm [10] has been introduced in the field of Swarm Intelligence. It is originated from the behaviour of Bees in the environment. Lucic was the father of BCO algorithm. This algorithm consists of two phases:

Forward phase: In forward phase each and every bee explores the search space .The number of moves are constant and predefined.

Backward phase: In backward phase all artificial bees discuss their solutions to problems.

2.1.1 BCO-Sybil attack algorithm:

STEP 1. Initialization of network;

STEP 2. For every user: // the forward pass

i. If Sybil node occurs.

ii. Set k = 1; //counter for constructive moves in the forward pass;

iii. Evaluate all possible constructive moves;

iv. According to evaluation, choose one move

v. k = k + 1; If k ≤ NC Go to step ii.

STEP 3. All users are back to the hive; // backward pass starts

STEP 4. Evaluate all solutions and find the best path so that Sybil node don't come in path;

STEP 5. Output the best solution found

2.2 FLOWCHART:

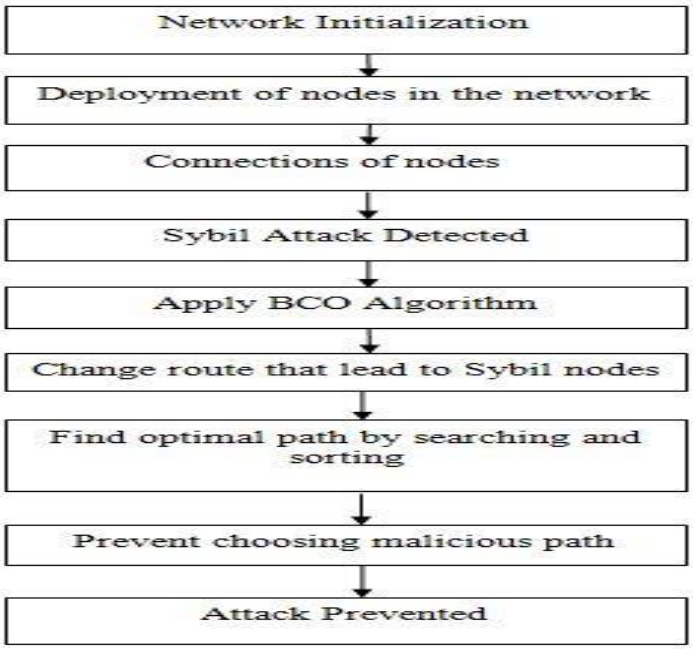

Fig. 3: Proposed Flowchart

3. RESULTS AND ANALYSIS

The result simulations have taken place in MATLAB environment. Based on the proposed algorithm to prevent the attack the results and analysis are shown as follows:

3.1 Result Snapshots:

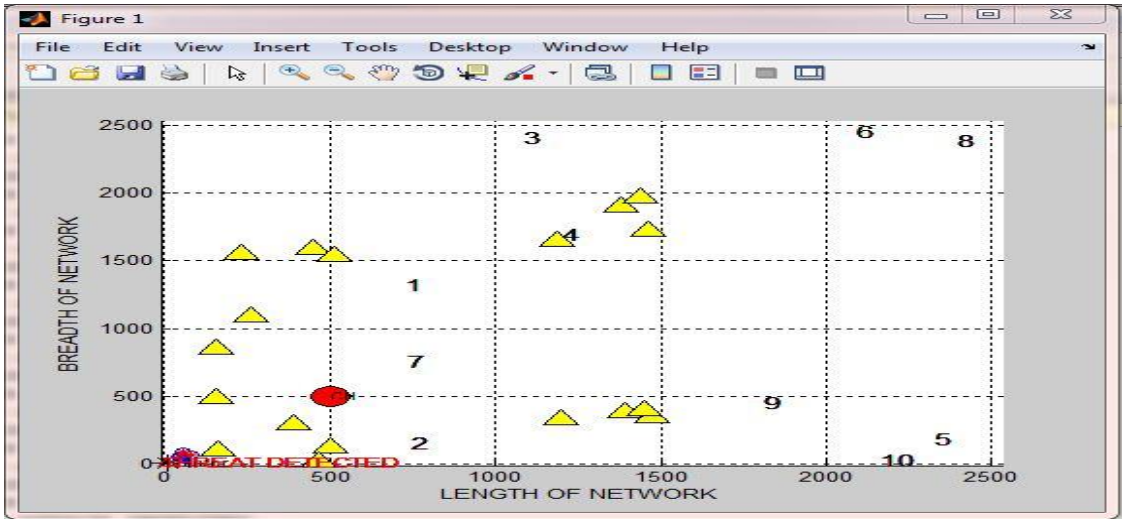

Fig. 4 Length versus Breadth of network

In fig. 4 Length vs breadth of the network, the channel (CH) captures the routing information from the initiator(source node) and then sends the data from the source to destination node. In this figure a total of 10 nodes are considered. The yellow triangles represent the nodes which can be either active or Sybil nodes.

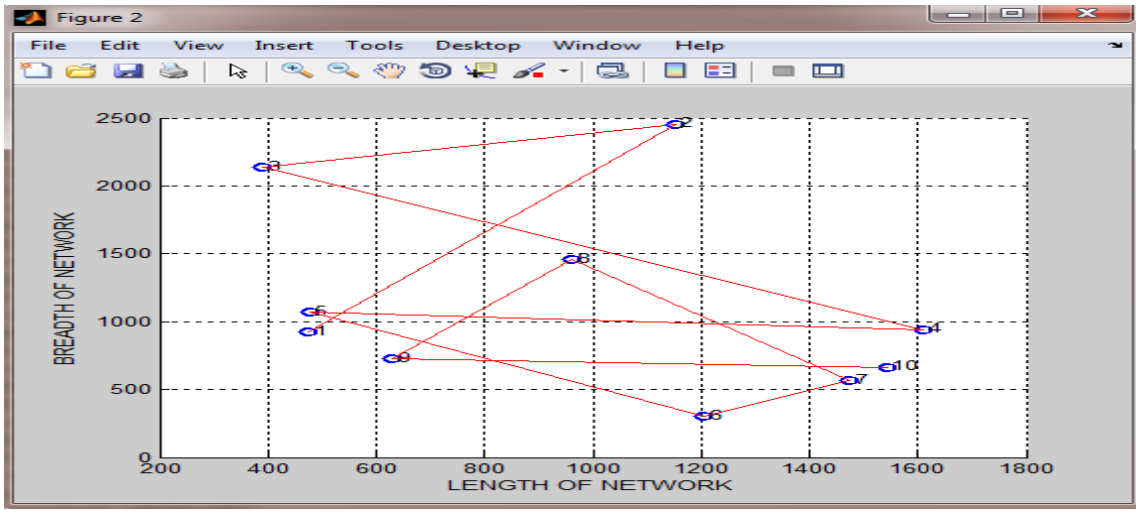

Fig. 5 Connections between nodes

Fig. 5 shows the connections between the nodes. Here 10 nodes are taken and the connections between them are shown which were made at the time of initialization of network and deployment of nodes.

Fig. 6 Optimized route obtained

Fig. 6 shows optimized route to be followed from source to destination using Bee Colony Optimization. In this particular example the path to be followed is from node 3 to destination node 5 via nodes 2 and 3, so that the threat can be prevented.

3.1.1 Parameters used:

i.) True Positive Rate – True positive rate measures the proportion of actual positives which are correctly identified, and calculated using the equation:

True Positive: Σ True positive/ Σ Condition positive

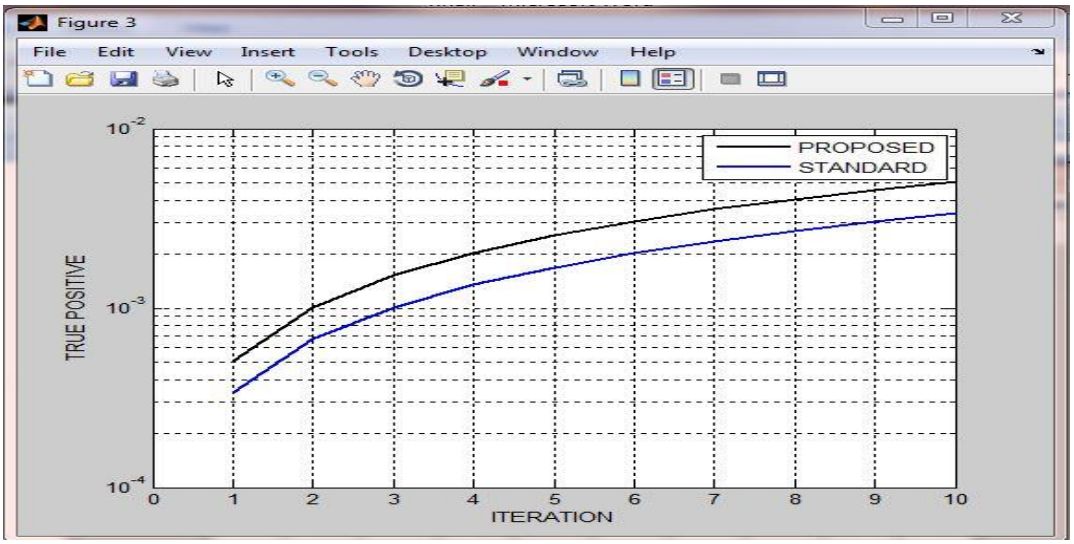

Fig. 7 True Positive Rate vs Iteration

In fig.7 True Positive Rate vs Iteration. The black line represents the true positive rate of Proposed method and blue line indicates the true positive rate of the Standard protocol. It is clear from the graph that the True Positive rate of the Proposed method is higher than that of the Standard Protocol.

ii.) False Positive Rate- The false positive rate (FP) is the proportion of negatives cases that were incorrectly classified as positive, and calculated using the equation:

False Positive: Σ False positive/ Σ Condition negative

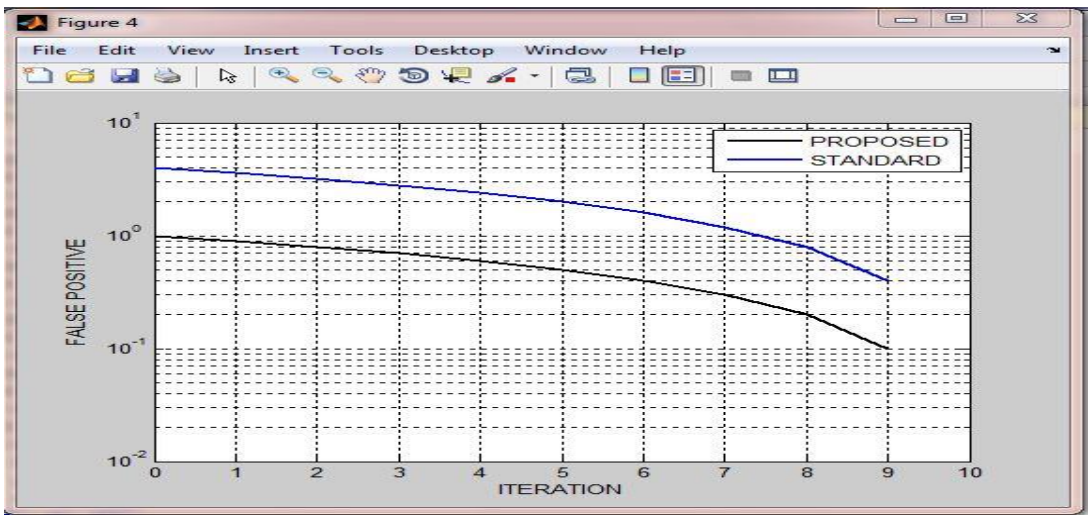

Fig. 8 False Positive Rate vs Iteration

In fig.8 False Positive Rate vs Iteration. The black line represents the false positive rate of Proposed method and blue line indicates the false positive rate of the Standard protocol. It is clear from the graph that the False Positive rate of the Standard Protocol is higher than that of the Proposed method.

iii.) Detection Rate- The detection rate or accuracy is the proportion of the total number of predictions that were correct. It is determined using the equation:

Detection rate= ((true positive + false positive)/ total population)*100

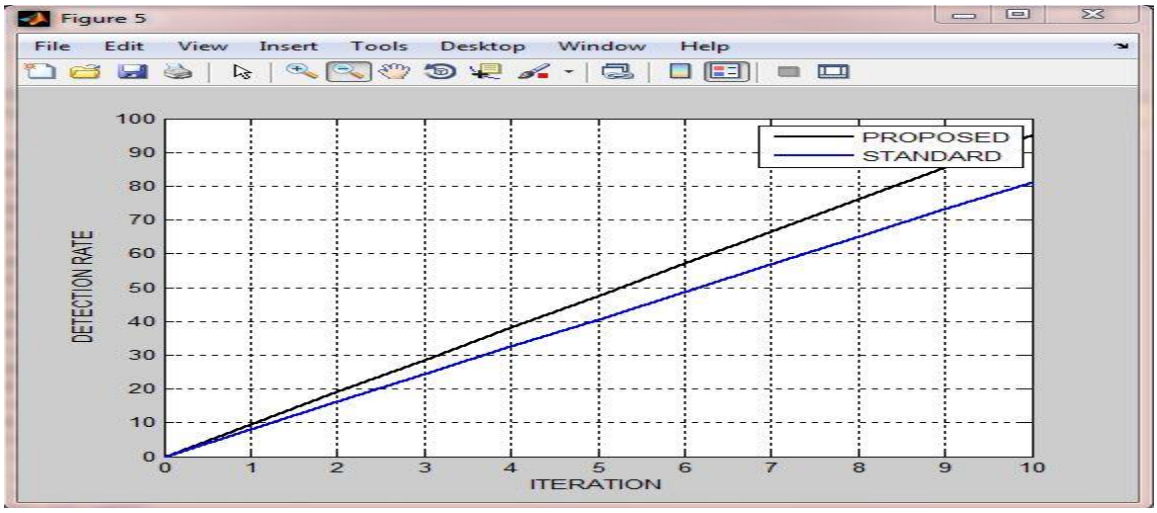

Fig. 9 Detection Rate vs Iteration

In the fig.9 Detection Rate vs Iteration, The black line represents the detection rate of Proposed method and blue line indicates the detection rate of the Standard protocol. It is clear from the graph that the detection rate in case of proposed method is high upto 96.5% whereas in case of detection by the system the detection rate is upto 81% since no prevention algorithm is applied.

3.2 Comparison based on Detection Rate:

TABLE 1 Performance Comparison

S.No	Method	Detection Rate (in %)
1	Proposed Method	96.5%
2	RSSI Method (11)	89%
3	State Information Method (12)	94%

Table 1 shows the comparison on basis of detection rate of various methods of prevention of Sybil attack developed in recent years. The Detection rate of the Proposed method is more in comparison to the previous methods considered.

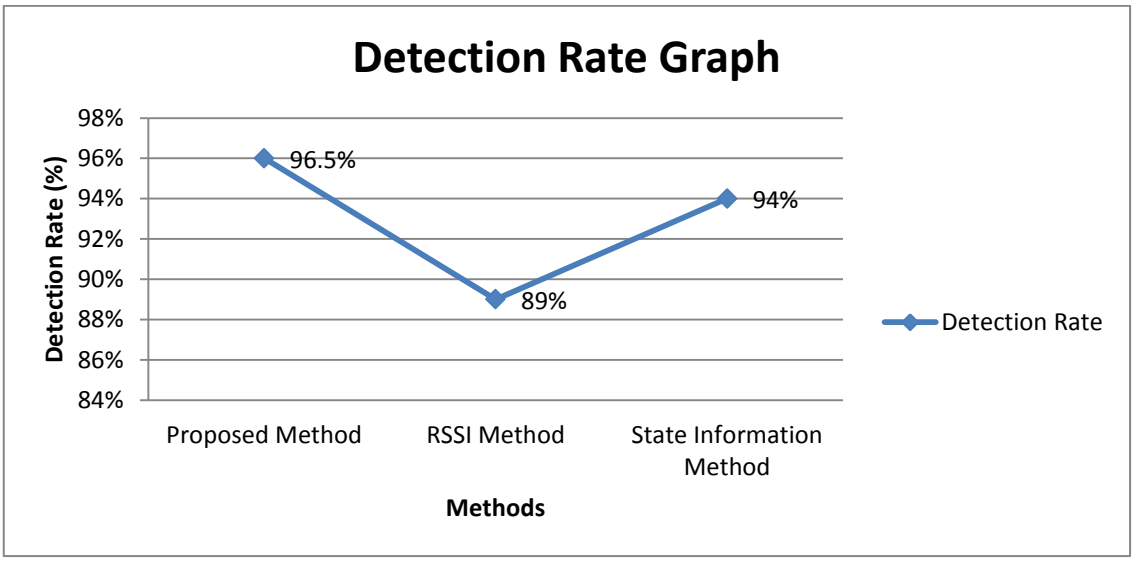

Fig. 10 Detection Rate Graph

Figure 10 shows the Detection Rate Graph of the proposed method and the previous methods of Sybil attack prevention. It is clear from the graph that the Detection rate of the proposed method of Sybil attack prevention is more and hence the proposed method is more efficient for use in future.

4. CONCLUSION

The scope of this paper lies in preventing the Sybil attack on LEACH Protocol in WSN. We attentively analyze the malicious behaviours of the Sybil nodes, and put forward a proposed scheme to detect and prevent the attack. This attack is very harmful and affects different routing protocols in WSN. The results based on proposed scheme demonstrate that our scheme can efficiently find the optimized path when Sybil attack occurs during routing using Bee Colony optimization (BCO). The proposed technique based on optimization algorithm helps to detect and prevent the Sybil attack. This thesis also includes comparison with previous prevention methods of Sybil attack. It also includes comparison with previous prevention methods of Sybil attack based on detection rate. The whole result simulation has been taken place in MATLAB environment.

REFERENCES

[1] I.F. Akyildiz, W.Su,Y. Sankarasubramanium, E.Cayiri, "Wireless Sensor Network: a Survey," Elsevier- Computer Networks, pp 393-422,2002.

[2] T. He, P. Vicaire, T. Yan, Q. Cao, L. Luo, L. Gu, G. Zhou, J. Stankovic, and T. Abdelzaher, "Achieving Long Term Surveillance in VigilNet, Infocom," April 2006.

[3] Heinzelman, W. Rabiner, A. Chandrakasan, and H. Balakrishnan. "Energy-efficient communication protocol for wireless microsensor networks." In System Sciences, 2000.

[4] Wendi B. Heinzelman, A.P. Chandrakasan, and H.Balakrishan, "An applocation-specific protocol architecture for wireless microsensor networks", IEEE Transaction on Wireless Communication, Vol. 1, No. 4,pp. 660-670, October 2002.

[5] S.Lee,Y.Lee and S.G.Yoo, "A Specification Based Intrusion Detection Mechanism for the LEACH Protocol, Information Technology Journal," pp 40-48, 2012.

[6] J. R. Douceur, "The Sybil attack," presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.

[7] S.Sharmila, G.Umamaheswari, Detection of Sybil attack in Mobile Wireless Sensor Networks, International Journal of Engineering Science & Advanced Technology, Vol.2 No.2, pp. 256-262, 2012.

[8] S.Lv, X.Wang,X.Zhao and X.Zhou, Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks, IEEE, pp 442-446, 2008.

[9] Lucic and D.Teodorovic, "Transportation Modelling- An artificial life approach," In Proceedings of 14th IEEE, International Conference on Tools with Artificial Intelligence, Washington DC, pp 216-223,2002

[10] Karaboga, D., & Ozturk, C., "A novel clustering approach: Artificial bee colony (ABC) algorithm." Applied Soft Computing, pp 652–657, 2011.

[11] S.Chen, G.Yang and S.Chen "A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks," International Conference on Communications and Mobile Computing, pp 143-146, 2010.

[12] X.Li, Han, A.Qian, L.Shu and J.Rodrigues "Detecting Sybil Attack based on State Information in Underwater Wireless Sensor Networks," IEEE, 2013.