AN ENERGY EFFICIENT V-LEACH ROUTING PROTOCOL IN WSN USING OPTIMIZATION TECHNIQUE

Manjit Kaur[1], Urvashi Sharma[2]

[1]Research scholar (CSE), Rayat Group Of Institutions, Railmajra, Punjab, India

[2]Assistant Professor (CSE), Rayat Group Of Institutions, Railmajra, Punjab, India

Abstract: Routing is the major challenge for sensor networks. It presents the trade- off between efficiency as well as responsiveness. There are various protocols exist in this category. In this work, we have analyzed Vice Cluster Head Low-energy adaptive clustering hierarchy (V-LEACH) hierarchical protocol for routing with the protocols on the basis of total energy consumed, sensors lifetime and provides a comparison with traditional methods. The optimization method used in the proposed work is ABC (Artificial Bee Colony). Utilization of V-LEACH is done as it is considered as a redirecting method and allows good routing. This method employs some sort of greedy approach beginning from the actual furthermost node and each of the sensor nodes form some sort of string just like composition. The proposed work is designed and implemented in WSN by using V- LEACH routing protocol. In this work, the performance analysis of the network with the scenario consisting of 50 nodes within the area (1000X1000) m^2 is being created in regards to the parameters packet delivery ratio, throughput, delay and energy consumption rate.

I. Introduction

WSN consists of numerous sensor nodes that are interconnected with each other through radio frequency link. These sensor nodes are very small in size that find applications in different areas like heath, industry, forest, weather broadcasting etc [1]. The main advantages of sensor nodes are that the sensor nodes can be deployed in remote areas which are away from human approach. In different areas such as in defense, navy, medical and in industry where security is the main concern, sensor nodes required to be implanted with higher energy [2]. The sensor node is used to collect information, process information and forwarded to the neighbor node[3]. The architecture of WSN is shown in figure below:

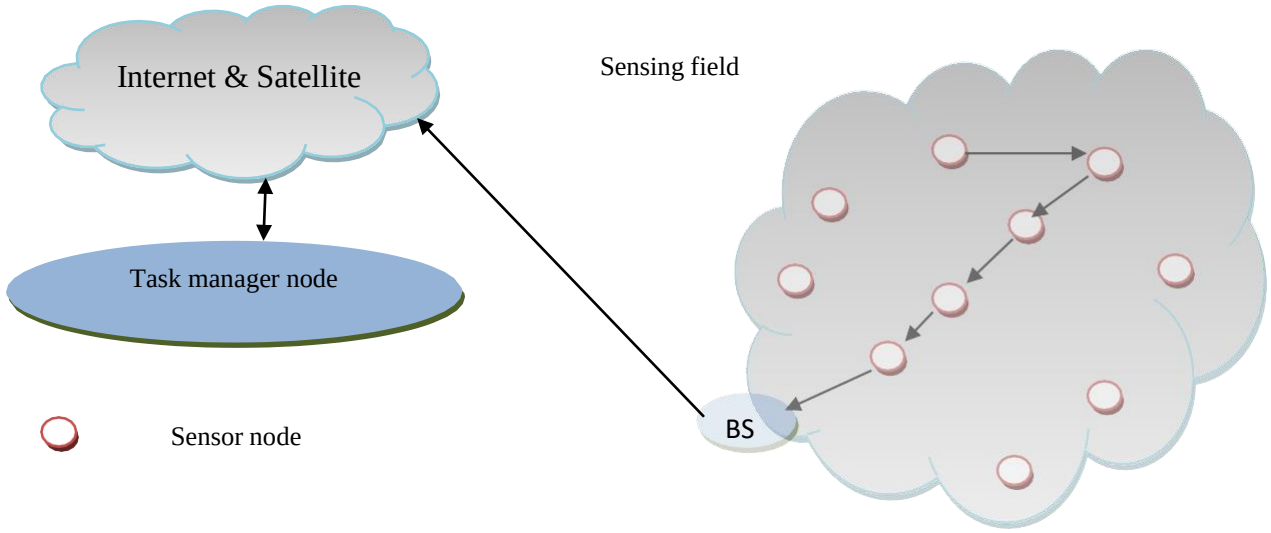

Figure 1: Wireless sensor network

The architecture of WSN is shown in figure 1 that comprises of single base station with number of sensor nodes. Sensor nodes are implanted randomly which is used to gather information and the base station is used to process and manage network and transmit the data to the network [4]. WSN's network layer is susceptible to various attacks such as Sybil attack, sink hole attack, black hole attack, DDOS attack. In this research paper, we are presenting the affect of DDoS attack in the designed wireless network [5]. DDoS attack is one of the rigorous attack which when appear in the network consume a large amount of energy and increase the data traffic [6]. To detect or to prevent the network from the DDoS attack a routing protocol is used which is used to form path between source and destination node [7]. In this research work we are using V-LEACH routing protocol. The description of which is provided below:

1.1 V-LEACH

In LEACH protocol, the route is formed by considered a node as a cluster head and other nodes in the network are behaving like cluster members and this process is repeated at every phase[8].

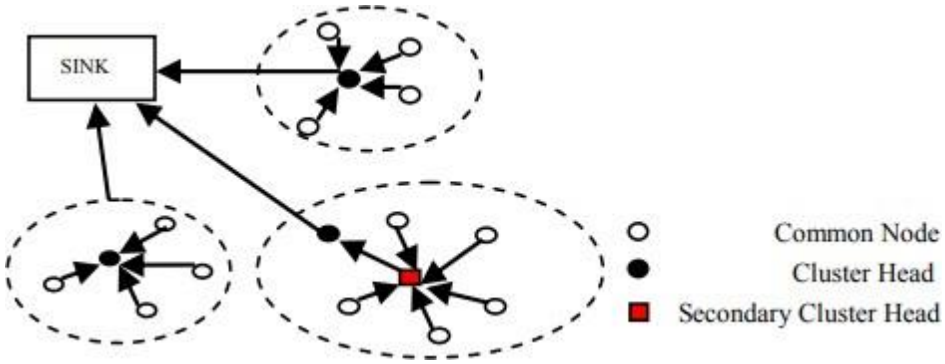

Figure 2: LEACH protocol

LEACH operation is mainly categorized into two steps:

i. Set up phase
ii. Steady state

During setup phase CH is formed using the equation written below:

$Y(n) = \frac{x}{1-x}$ if nc J

$either\ o$; if $n\ not$ c J

Here, J are the number of nodes that are representing the cluster members [9]

X represents the suggested percentage

Every sensor node forward sensed information to the nearest CH. The CH collects information from the cluster members and then transmits the collected information to the base station [10]. V-Leach (Vice Cluster Head Low Energy Adaptive Clustering Hierarchy) is the enhancement routing protocol of LEACH protocol. This protocol is utilized to select a new CH every time in case when a CH dies and the sensor node wants to transmit data to the BS .So that the lifetime of the network is increased [11].

1.2 ABC (Artificial Bee Colony)

ABC is an optimization algorithm that is inspired by the intellectual behavior of Bees. Here, ABC algorithm is used to optimize the route formed by V-LEACH routing protocol by using fitness function. If the fitness function of ABC algorithm is satisfied than considered sensor node as a genuine node and pass the data otherwise consider the node

as a node affected by DDoS attack [12]. ABC algorithm mainly consists of three components namely, employed bee, onlooker bee and scout bee. Employed bees are used to find an appropriate sensor node through which data can be transmitted effectively Onlooker Bee getting information from the employed bees and on the basis of collected information onlooker bees take decision. If an accurate node is not determined then the scout bee phase is used to repeat the process again [13].

II. Related work

Nagar et al. [14, 2017] proposed a Ad-hoc On-demand Multipath Distance protocol which has been used to protect the network against DDoS attack.The results have been obtained with normal AOMDV , AOMDV with DDoS attack and AOMDV with security mechanism. **Osanaiye et al. [15, 2018]** presented a statistical method to detect DoS attack. The arrival of DoS attack in the network has been analysed by using the EWMA (exponentially weighted moving average). **Dhuria et al. [16, 2018]** presented two techniques first one is light weight bi-directional authentication system which has been used to prevent network from various attacks. The other one is based on traffic analysis which has been used to filter data that is used to idetenfy and prevent DDoS attack in WSN. **Kumar et al. [17, 2018]** proposed a technique to detect and prevent network from black hole attack and DoS attack. The performance has been measured in terms of star and tree topology formed by sensor nodes. The performance on the basis of PDR and delay has been measured.

III. Methodology

The flow of the work that is carried out to detect and prevent the network from DDoS attack using ABC algorithm is described below:

Step 1. Design a wireless network with defined height and width.
Step 2. Initialize N number of sensor nodes within the network.
Step 3. Defined source node and destination node among the n number of sensor nodes.
Step 4. Defined the coverage area of every node along with source and sink node.
Step 5. Create route between source and destination using V-LEACH routing protocol and start data transmission.
Step 6. Determine QoS parameters and if the performance of the network degraded then initialize fitness function of ABC algorithm.
Step 7. If fitness function is satisfied then detect DDoS attack and create a new route without attacker node otherwise consider node as normal node.
Step 8. Determine performance parameters after preventing the node from DDoS attack.

The algorithm of ABC used in the proposed work is written below:

ABC Algorithm

Initialize the bees= Total number of nodes

Initialize the bee types - **Employed bee**
- **Onlookers bee &**
- **Scouts bee**

put threshold of properties=f_t

Defined S_{bee} as scout bee

For i=1 →Sensor node in route

Call objective function j

$$ABC_{obj} = \begin{cases} E_{Bee} > O_{Bee} \text{ then j True} \\ E_{Bee} \leq O_{Bee} \text{ then j false} \end{cases}$$

Return S_{Bee}j

Optimize_data = $ABC\ (ABC_{obj}, S_{bee}, f_t)$

End

$S_{Bee} = optimize\_data$

Return optimize_data and prevent the node using properties of node.

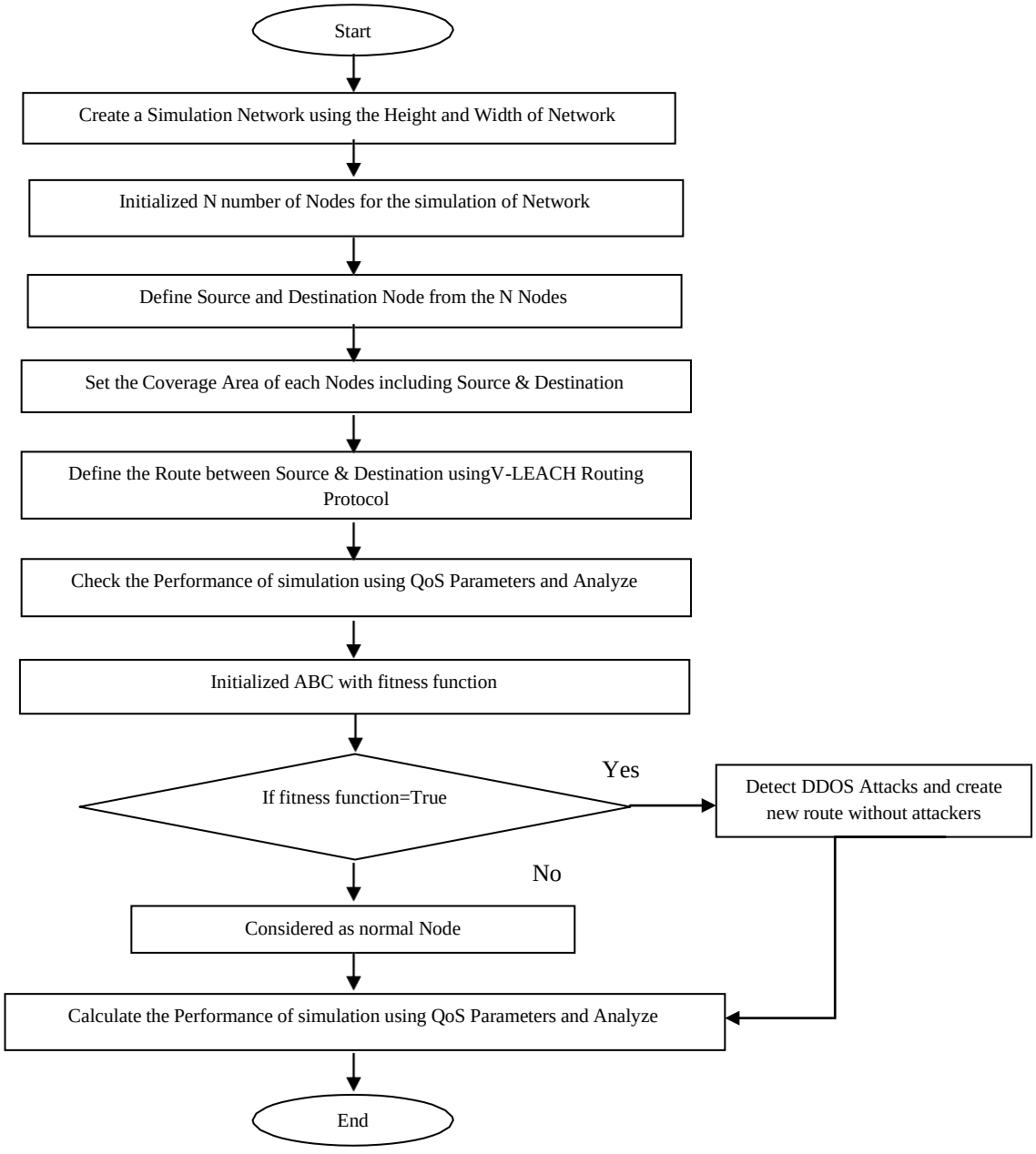

Figure 3: Flowchart of proposed work

IV. Simulation results

In this section, the experiment results measured by simulating the code in MATLAB environment are discussed in detail. The network of area 1000×1000 square meter with 50 numbers of nodes is designed. The simulation area of designed network is shown below:

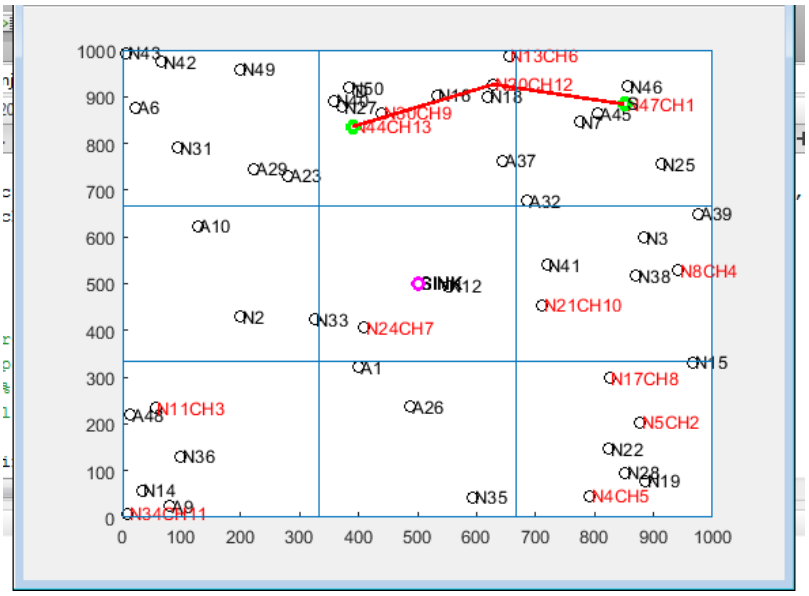

Figure 4: Network structure

The network of the proposed model is designed in MATLAB simulator is shown in figure 4. Here the network area is divided into six equal parts each having size of 300 ×300 or more. Cluster head formed in each section is denoted by CH.

Table 1: Throughput

Number of rounds	Throughput with distortion	Throughput with improvement
1	67	98
2	86	99
3	62	98
4	69	96
5	81	96

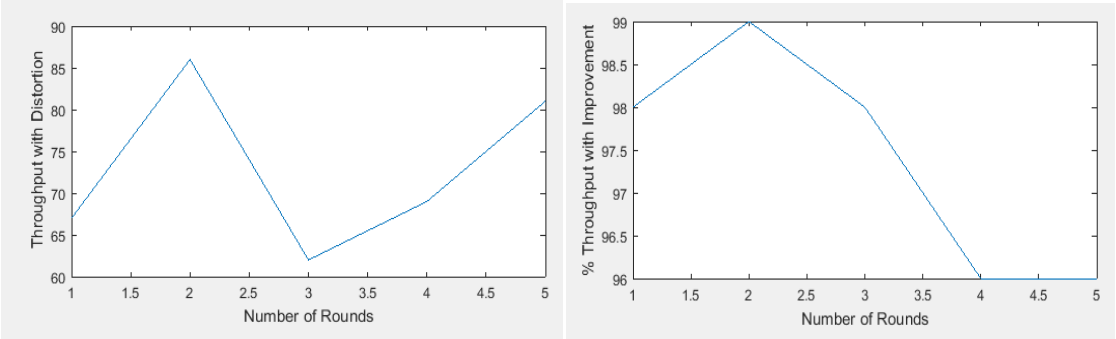

Figure 5: Throughput with distortion and with improvement

The above figure represents the graph plotted for throughput which is measured in the presence of DDoS attack and after preventing the network from DDoS attack by applying ABC algorithm in the proposed work. From the above figure it is clear that the average values of throughput measured for the proposed work in the presence of

DDoS attack and after applying ABC algorithm are 73 and 97.4 respectively. Thus it is clear that throughput value has been increased by 33.42%.

Table 2: PDR

Number of rounds	PDR with distortion	PDR with improvement
1	0.6596	0.47
2	0.9018	3.35
3	1.2892	4.16
4	1.6840	0.034
5	2.0782	0.768

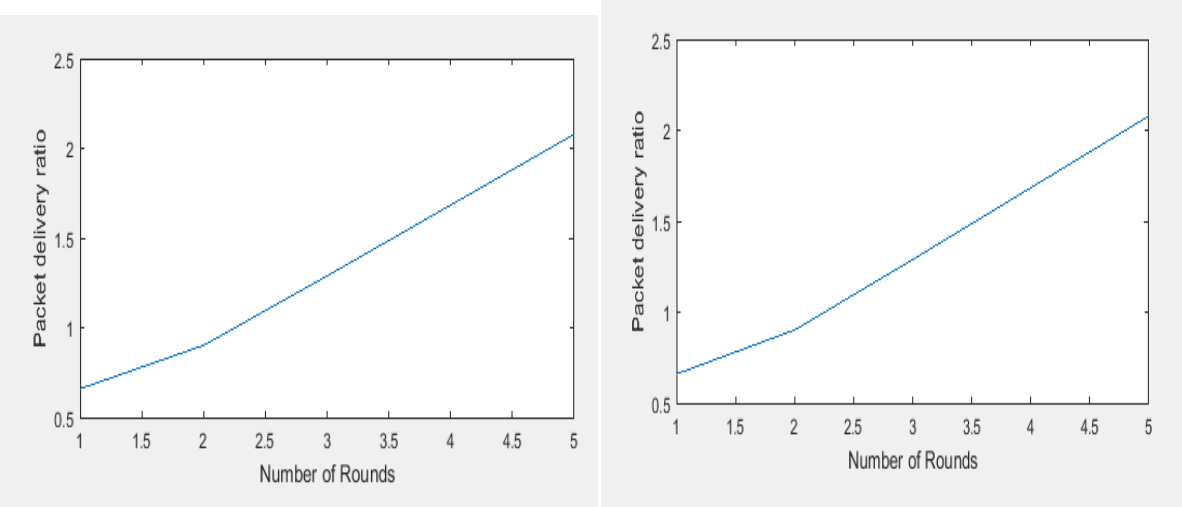

Figure 6: PDR with distortion and with improvement

The above figure represents the PDR values measured with distortion and with ABC in the proposed work. From the above figure it has been observed that the average values of PDR in the presence of DDoS attack and after applying ABC algorithm is high which is obtained due to the path change from the node which is affected by the attack towards the genuine node and hence increase the PDR value. The average values obtained with distortion and with improvement are 1.32 and 1.75 respectively. Thus, there is an increase in the PDR rate while applying ABC algorithm by 32.58%.

Table 3: Energy Consumption

Number of rounds	Energy consumption with distortion	Energy Consumption with improvement
1	14.39	11.33
2	19.68	14.61
3	28.13	24.07
4	36.75	35.68
5	45.36	40.29

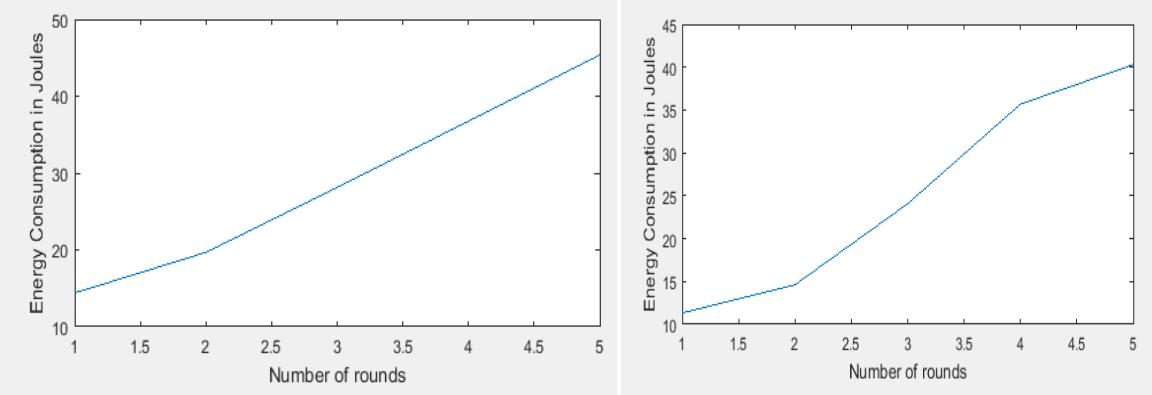

Figure 7: Energy consumption with distortion and with improvement

The values of energy consumptions obtained for the proposed work with distortion and with improvement are described in the figure above. From the figure it is clear that while applying ABC algorithm the energy consumed by the sensor nodes decreases. The average values of energy consumptions obtained for the proposed work in the presence of DDoS attack and while applying optimization algorithm are 28.86 and 25.19 respectively. The percentage decreases in the energy consumption rate while applying ABC algorithm in the proposed network is 12.72%.

Table 4: Delay

Number of rounds	Delay with distortion	Delay with improvement
1	297.38	295.07
2	392.59	387.28
3	544.25	541.95
4	700.26	695.95
5	854.80	850.49

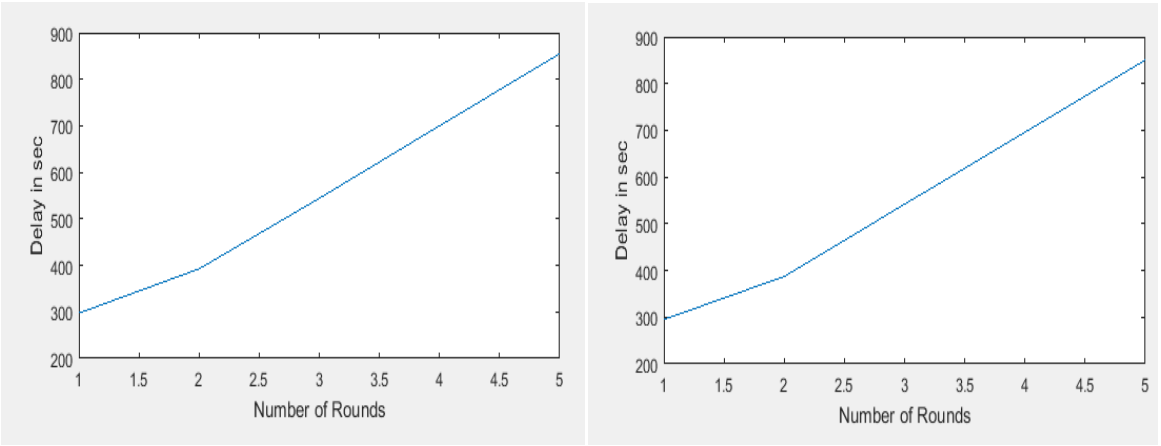

Figure 8: Delay with distortion and with improvement

The graph plotted in figure 8 shows the values of delay observed for the proposed work with route formed using V-LEACH protocol in the presence of DDoS attack and the route optimized using ABC algorithm in the proposed work. The average values of delay obtained for the proposed research work with distortion and with improvement are 557.85 J and 554.14 J respectively. Therefore, there is a decrement of 0.67% respectively.

V. COMPARISON OF PROPOSED WORK WITH EXISTING WORK

Singh et al.[11] presented V-LEACH routing protocol, which is the enhance version of LEACH routing protocol to save energy and hence increasing the life of sensor nodes. Author used PSO (particle swarm optimization algorithm) along with V_LEACH routing protocol, which helps to reduce the energy consumption in multi hop communication. The performance of the proposed work has been measured in terms of energy consumption, delay, number of live nodes with respect to number of iterations. The values observed by the existing work with the proposed work are listed below.

Table 5: Comparison of Energy consumption rate

Number of rounds	Energy consumption rate Existing work (J)	Energy consumption with proposed work (J)
1	0.75	11.33
2	30	14.61
3	140	24.07
4	280	35.68
5	510	40.29

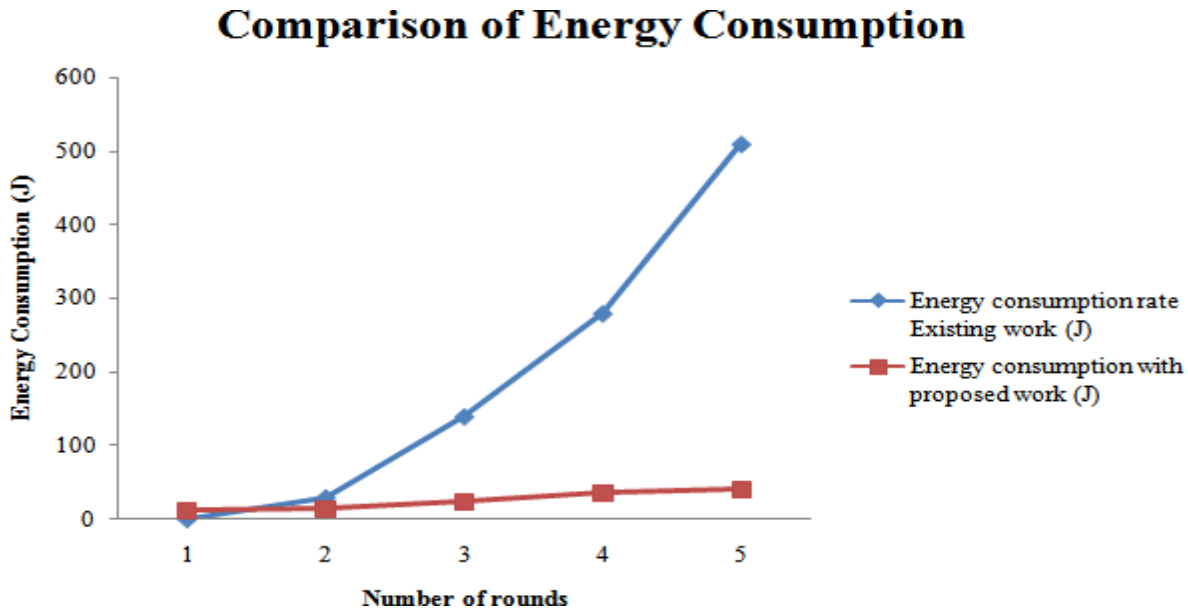

Figure 9: Comparison of Energy Consumption

The graph plotted above shows the values of energy consumption measured in Joule for the proposed as well as for the existing work. Here the blue line and the red line represent the values of energy consumption obtained for the existing work and proposed work respectively. From the above graph it is clear that the energy consumed by the sensor nodes in the wireless network by using V-LEACH routing protocol along with ABC has been reduced by 86.89 % respectively.

VI. Conclusion

In this paper, V-LEACH routing protocol has been presented for WSN.V-LEACH performs well as compared to LEACH routing protocol. From the experiments it has been concluded that when DDoS attack occurs in the network, the performance of the network degraded. To improve the efficiency of the network ABC algorithm has been used and hence the values of throughput, PDR, energy consumption and delay achieved after preventing the network from the DDoS attack are 33.42%, 32.58%, 12.72% and 0.67% respectively. At last, the comparison

between proposed work and existing work performed by Singh et al.[29, 2016] in the field of wireless sensor network using V-LEACH along with PSO (particle swarm optimization0 algorithm have been performed. The values of energy consumed by nodes for five rounds and the delay performed by the nodes to reach the message from source node to destination node have been performed. It has been concluded that the proposed work in comparison with energy consumption rate perform well and reduced energy consumption rate by 86.89 % from the existing work.

In future, to enhance the efficiency of the WSN classification algorithm can be used to classify the genuine node and the attacker node.

References

[1]. Weiwei Fang, Zhen Liu and Feng Liu, "A Cross-Layer Protocol For Reliable And Efficient Communication In Wireless Sensor Networks," International Journal of Innovative Computing, 2012, Vol. 8, No. 18, October 2012.

[2]. Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V., "Wireless Sensor Network Security: A Survey," Security in Distributed, Grid and Pervasive Computing, Vol. 1, pp.367, 2007.

[3]. Malathi, L., and R. K. Gnanamurthy, "Cluster Based Hierarchical Routing Protocol for WSN with Energy Efficiency," International Journal of Machine Learning and Computing 4.5 (2014): 474.

[4]. Meghna Chhabra, Brij Gupta1, Ammar Almomani, "A Novel Solution to Handle DDOS Attack in MANET," Journal of Information Security, Vol. 4, pp. 165-179, 2013.

[5]. Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys & Tutorials*, *18*(1), 602-622.

[6]. Fouchal, S., Mansouri, D., Mokdad, L., & Iouallalen, M. (2015). Recursive-clustering-based approach for denial of service (DoS) attacks in wireless sensors networks. *International Journal of Communication Systems*, *28*(2), 309-324.

[7]. Fouchal, S., Mansouri, D., Mokdad, L., & Iouallalen, M. (2015). Recursive-clustering-based approach for denial of service (DoS) attacks in wireless sensors networks. *International Journal of Communication Systems*, *28*(2), 309-324.

[8]. Bouyer, A., Hatamlou, A., & Masdari, M. (2015). A new approach for decreasing energy in wireless sensor networks with hybrid LEACH protocol and fuzzy C-means algorithm. *International Journal of Communication Networks and Distributed Systems*, *14*(4), 400-412.

[9]. Salim, A., Osamy, W., & Khedr, A. M. (2014). IBLEACH: intra-balanced LEACH protocol for wireless sensor networks. *Wireless networks*, *20*(6), 1515-1525.

[10]. Dhawan, H., & Waraich, S. (2014). A comparative study on LEACH routing protocol and its variants in wireless sensor networks: a survey. *International Journal of Computer Applications*, *95*(8).

[11]. Singh, A., Rathkanthiwar, S., & Kakde, S. (2016, March). LEACH based-energy efficient routing protocol for wireless sensor networks. In *Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on* (pp. 4654-4658). IEEE.

[12]. Karaboga, D., Gorkemli, B., Ozturk, C., & Karaboga, N. (2014). A comprehensive survey: artificial bee colony (ABC) algorithm and applications. *Artificial Intelligence Review*, *42*(1), 21-57.

[13]. Tosun, Ö. (2014). Artificial bee colony algorithm. In *Encyclopedia of business analytics and optimization* (pp. 179-192). IGI Global.

[14]. Nagar, S., Rajput, S. S., Gupta, A. K., & Trivedi, M. C. (2017, February). Secure routing against DDoS attack in wireless sensor network. In *Computational Intelligence & Communication Technology (CICT), 2017 3rd International Conference on* (pp. 1-6). IEEE.

[15]. Osanaiye, O., Alfa, A. S., & Hancke, G. P. (2018). A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks. *Sensors*, *18*(6), 1691.

[16]. Dhuria, S., & Sachdeva, M. (2018). Detection and Prevention of DDoS Attacks in Wireless Sensor Networks. In *Networking Communication and Data Knowledge Engineering* (pp. 3-13). Springer, Singapore.

[17]. Kumar, S., & Agnihotri, N. (2018). Design of a Novel Technique for Denial of Service Attack Detection in Wireless Network.