Enhancing the Energy of Wireless Sensor Network using Soft Computing Algorithm

[1]K. Manojkumar, [2]Dr. S. Devi

[1] Assistant Professor, Computer Science and Engineering, Government College of Engineering, Thanjavur, Tamil Nadu, India
[2] Professor, Electronics and Communication Engineering, PRIST deemed to be University, Thanjavur, Tamil Nadu, India

Abstract : The jamming attack is a standout amongst the most genuine danger in Wireless Sensor Networks (WSN). This sort of attacks stops the nonstop communications and also vapor the essentialness of the sensor hubs. In WSN, a couple of sorts of DoS attacks in different layers might be performed. The physical layer being the most lessened layer and the first to be attacked by jammers. The systems to deflect jamming attacks incorporate instalment for network assets, pushback, strong authentication and identification. In this paper, the physical layer DoS attack is analyzed, and a defense mechanism is proposed utilizing Artificial Bee Colony Algorithm (ABC) and its performance analysis have been compared and validated. The simulation outcomes demonstrate that the proposed scheme helps in accomplishing most extreme dependability on DoS claims to enhance the Quality of Service (QoS) and the energy of WSN**.**

IndexTerms **- Wireless sensor network, Jamming attack, Artificial Bee Colony Algorithm.**

I. INTRODUCTION

Wireless sensor network (WSNs) which permits the surveillance of the world comes up with innovative fangled resolve. Those systems comprise of an extensive number of small sensor nodes which is interconnected with a remote direct keeping in mind the end goal to screen the physical and natural condition such as temperature, sound, pressure, healthcare disaster etc., [1]. It consists of low cost and low power on-chip sensors which are distributed in the close vicinity [2]. The sensor node equipment comprises radio receiver end to end with an antenna, a micro-controller, an electronic circuit, energy source, and battery. It has numerous the application in our environment, community, military, home and beyond.

Types of WSN

There are several types of WSN [3], turning on the environment it is categorised. It includes

A Terrestrial WSNs

It consists of thousands of sensors node deployed as organised or unorganised manner. In this type, there is limited battery power. It accomplishes energy by a low duty cycle operation, diminishing delay, and routing so on. It is used for the land surface.

An Underground WSNs

These types of a network consisting of thousands of sensors node deployed under hidden manner in unground. It is very costly. To monitoring underground position, it is used. To relay information from nodes to BS additional sink node are deployed above the ground

A Multimedia WSNs

It is authorizing network which is used to permit tracking and monitoring of events in the form of multimedia. It can be made up of a very tiny sensor node and lesser cost fitted with microphones and cameras. For retrieving data, data processing, correlation of data, and compression of data these type of WSN is mainly used.

A Mobile WSNs

The network has many sensor nodes turned on by owned and communicating with the physical environment is called Mobile WSN.

II. WIRELESS SENSOR NETWORKS (WSN)

Wireless sensor networks (WSNs) is a developing region of research inside the general Wireless Sensor Network (WSN) region. Earth contains 70% of water, there is a requirement for broad research in check and investigating different parts of ocean environment. The characteristic approach is to adjust as of now accessible, and well demonstrated earthbound structures, for underwater use. The quantity of WSN-based applications is always increasing. Enormous WSN applications can be categorized for monitoring applications. Water quality investigation, contamination observing, checking of ocean currents, following of fishes or smaller scale creatures, weight and temperature estimations, and also conductivity and turbidity examination, are largely cases of ecological checking [4-5]. Observing underwater structures, for example, oil stages, oil and gas channels, covered correspondence fast links and other hardware checking would all be able to be accomplished utilizing WSNs.

Attacks in Wireless Sensor Networks

Two categories of attacks are possible in Wireless Sensor Networks, Active and Passive attacks [6]. In passive attacks, the realization of this attack is easy and it is difficult to detect. Traffic analysis, traffic monitoring and eavesdropping are the various examples of passive attacks. In Active attacks, an attacks, an attacker tries to remove or modify the messages which are transmitted on the network. Jamming, DoS, message reply, modification are the examples of active attacks [7].

Jamming is an amazing component of Denial of Service (DoS) attacks. Jamming drives electromagnetic strength towards a communication system to neutralize signal transmission [8]. In WSNs, jamming intrudes in to the radio frequencies used by organize hubs [9]. DoS attack as "any event that wipes out a system's capacity to execute its customary limit" [10].

III. Enhancing the Energy of WSN using Soft Computing Algorithm

Various soft computing algorithm have implemented for the performance evaluation of jamming attacks, a square grid network and different kinds of jammers are built up for an exploratory domain. Distinctive estimations of the accompanying parameters are chosen to modify the strength of attack of those jammers. The execution of the system could be broke down by thinking about differed Jamming to signal ratio (J/S), energy to jamming thickness proportion, energy to noise ratio, multi-way impedance. At first, the quantity of jamming node in a period t seconds is 12. Thus, the quantity of jammed nodes is 12 out of 100 in the system.

Thus, for each node jammed for t seconds. BAT and ABC algorithms results are evaluated. From the results, the proposed algorithms detects strategies identifies jamming attacks by checking the energy, distance. Packet loss, packet delivery ratio and researching the unusual conduct of neighbors' radio signals.

Artificial Bee Colony (ABC) Algorithm

Artificial Bee Colony (ABC) is also a swarm intelligence based optimization approach [11]. In the ABC algorithm, while onlookers and employed bees carry out the exploitation process in the search space, the scouts control the exploration process. The ABC algorithm is

1: Initialize the population of solutions P_i, i=1…….N
2: Evaluate the population
3: cycle = 1
4: repeat
5: Produce new solutions V_i for the employed bees V_{ij} by using and evaluate them
4. Apply Greedy Selection Process for the Employed Bee
7: Calculate the probability values P_i for the solutions X_i by prob(i)
8: Produce the new solutions V_i for the onlookers from the solutions X_i selected depending on P_i and evaluate them
9: Apply the greedy selection process for the onlookers
10: Determine the abandoned solution for the scout, if exists, and replace it with a new randomly produced solution X_i by X_i^j
11: Memorize the best solution achieved so far
12: cycle = cycle + 1
13: until cycle = MCN

Fig. 1 ABC Algorithm

Employed bees recognize neighbor source based on the following equation

$$v_{ij} = x_{ij} + r_{ij}(x_{ij} - x_{kj}) \quad (1)$$

where $j \in \{1, 2, \ldots d\}, k \in \{1, 2, \ldots SN\}$ is a randomly chosen index different from i and r_{ij} denotes a uniformly distributed real random number in the range (-1, 1). Here d is the number of variables of the problem. When the employed bees have stopped searching, the nectar amount and the position of their food source information are shared. An onlooker bee assesses the nectar data given by employed bees and selects food source with probability linked to the nectar amount. The probability value prob(i) is computed by the following expression.

$$\text{prob}(i) = \frac{\text{fit}(i)}{\sum_{i=1}^{SN} \text{fit}(i)} \quad (2)$$

Where fit(i) denotes the nectar amount (i.e., the fitness value) of the i^{th} food source X_i. If the probability value prob(i) linked with that source is higher than a random number (0, 1) then the onlooker bee formulates a new position of this food source by using Equation (1). The operation is defined by

$$x_i^j = x_{min}^j + \text{rand}[0,1](x_{max}^j - x_{min}^j) \quad (3)$$

IV. Results and Discussion

To assess the performance of the proposed technique with the nearness of jamming attacks, a square lattice network and distinctive kinds of jammers [13] are built up for a test situation. Diverse estimations of the accompanying parameters are chosen to alter the attacking quality of those jammers: jamming reach and number of jammers. The proposed detection and safeguard system are reproduced with the assistance of gr Theory toolkit in MATLAB. The performance of the network could be examined by thinking about fluctuated Jamming to flag proportion (J/S), vitality to jamming thickness proportion, vitality to commotion thickness proportion, multi-way obstruction. The radio-engendering model and the receiving wire demonstrate are taken for this

system is Omni-reception apparatus and Two Ray Ground show [14]. An established responsive steering convention called Ad hoc On-Demand Distance Vector (AODV) is considered for this work. A square framework of 100 immobile nodes (numbered from node 0 to node 99 section by segment) is found in the reenacted network. Node 0 as the source node and node 100 that spots at the inverse to node 0 as the goal node, where data stream that begins at a simulation time of the 20s.The source node starts User Datagram Protocol (UDP)/consistent bit rate (CBR) streams with a bundle size of 1024 bytes and a transmission rate of 0.02 Mbps to its expected goal, and for the jammer, the parcel size and transmission rate are shifted. More simulation parameters are recorded as takes after Frequency, wavelength and reception apparatus pick up are set to 864.536 MHz, 0.424 m and 1.5 dB, individually. The MAC convention utilized as a part of this proposed technique is BMAC. The transmitted power for a sensor network is 8.56 × 10-4 W and for the jammer, its changed. The receiver affectability and way misfortunes are 3.652 × 10-4 W and 1.5 dB. At first, the quantity of stuck node in a period t seconds is 12. Subsequently, the quantity of nodes stuck is 12 out of 100 in the network. Mainly, for each situation nodes are stuck for t seconds.

The jammer was altered to transmit at a comparative power level as the hubs which is control level 1. Dependent upon the circumstance of a node in the system network, the amount of neighbours for a node contrasted from 6 to 14 nodes. In spite of the way that the nodes were not time synchronized, they were all running at a comparative interval of time between time. Nodes which lies on the edge of the system were having less number of neighbours and hubs which lies inside the system network were having more number of neighbours. Tests were finished to record the discovery time, identification rate, and the false alarm rate of the convention. The Fig. 3 depicts different types of jammer and the execution of the system in perspective of the energy drained, detachment, and package incident and package movement extent. The ABC strategy is surveyed with the eventual outcomes. From the result, the proposed system recognizes jamming attacks by checking the energy, detached. Package incident, package movement extent and looking at the abnormal practices of neighbor's radio signals. The proposed technique recovers the system network from jamming attacks using way exchanging. Likewise, the proposed system is intense to shield the system network from attacks impelled by different jammers. Generated results were shown in Figs. 4-6. From the figures the transcendence of ABC system for jamming attacks have illustrated.

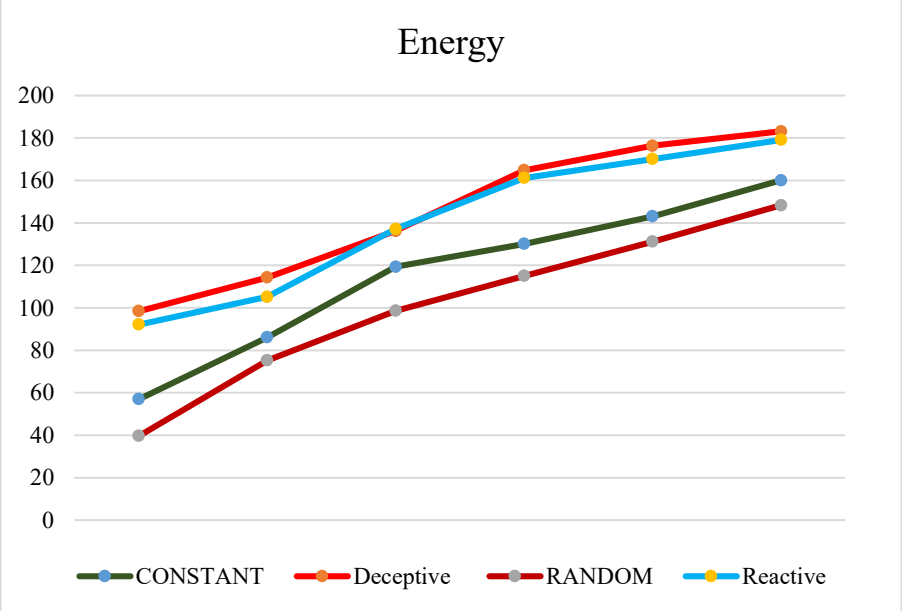

Fig. 3 Energy with ABC System

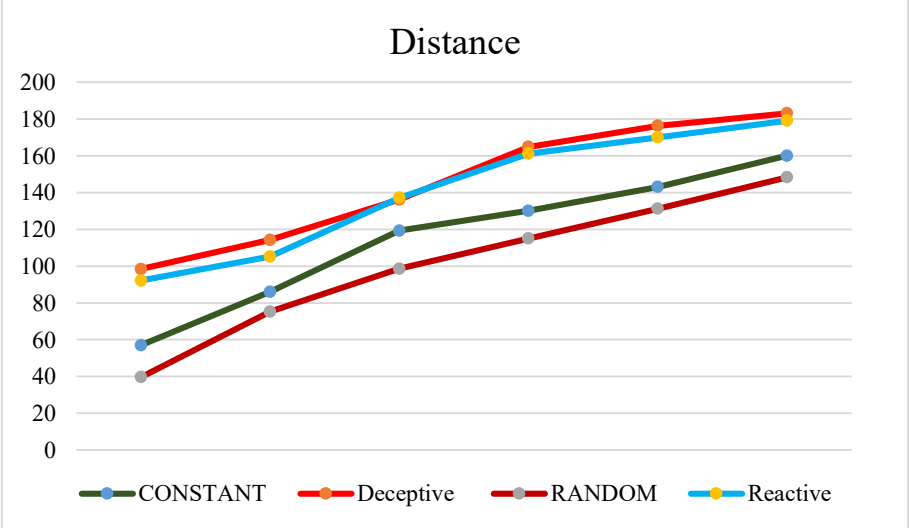

Fig. 4 Distance with ABC System

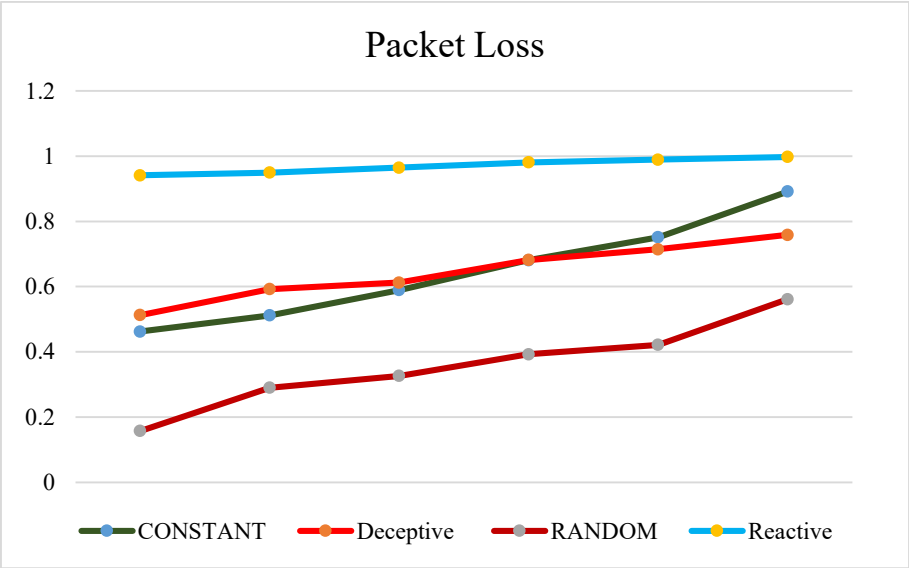

Fig. 5 Packet Loss with ABC System

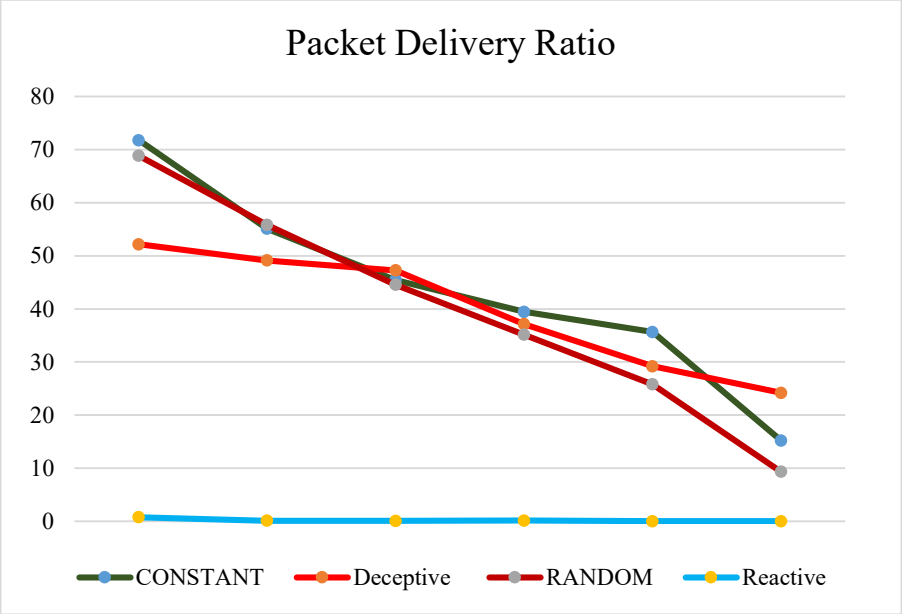

Fig. 6 Packet Delivery Ratio with ABC System

V. CONCLUSION

This paper proposes a novel strategy to distinguish jamming attack utilising ABC algorithm. The performance parameter, for example, vitality, remove, parcel misfortune, and bundle conveyance impacts the choice taken in against jamming systems. The plan of DoS attack in light of each layer can be joined to enhance the attacks by utilising a basic advancement algorithm. The proposed algorithms can isolate network conditions caused by different kinds of jammers or cause by characteristic sources from each other alongside high detection rate and low false positive rate to upgrade the vitality of the Wireless Sensor Networks. Another preferred standpoint is that no extra equipment is required to execute the algorithms on existing Wireless Sensor Nodes. In the following examination arranged, the algorithms will be actualised on genuine wireless sensor nodes and, therefore, the performance accomplishment of the algorithms in a genuine situation will be expounded.

REFERENCES

1. Gowrishankar, S, T.G., Basavaraju, Manjaiah, D.H., and Subir Kumar Sarkar, (2008), Issues in Wireless Sensor Networks, Proceedings of the World Congress on Engineering, Vol. 1
2. Kazerooni, A.A., Jelodar, H., and Aramideh. J., (2015), Leach and heed clustering algorithms in wireless sensor networks, Advances in Science and Technology: Research Journal, Vol.9(25), pp. 7-11,
3. Yick., Jennifer., Biswanath Mukherjee., and Dipak Ghosal., (2008), Wireless sensor network survey, The International Journal of Computer and Telecommunication Networks, Vol. 52(12), pp. 2292-2330.
4. J. Partan, J. Kurose, and B.N. Levine, "A survey of practical issues in underwater networks," in 1st ACM international workshop on Underwater networks, New York, 2006, pp. 17-24.
5. I.F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," Elsevier, vol. Ad Hoc Networks, no. 3, pp. 257-279, February 2005.

6. Sunil Ghildiyal, Amit Kumar Mishra, Ashik Gupta, Neha Garg, "Analysis of Daniel Of Service (DoS) attacks in WSN" International Journal of Research in Engineering and Technology, Vol.3, June 2014.
7. Sunil Gupta, Harsh K Verma, A L Sangal, "Security attacks & Prerequisite for WSN", International Journal of Engineering and Advanced Technology, Vol.2, June 2013.
8. D. L. Adamy and D. Adamy, "*EW 102: A Second Course in Electronic Warfare*", Artech House Publishers, 2004.
9. E. Shi, A. Perrig, "Designing Secure Sensor Networks", *Wireless Communications Magazine*, 11(6), 2004, pp. 38-43.
10. A.D Wood et al.," JAM: A Jammed-Area Mapping Service for Sensor Networks", *24th IEEE Real-Time Systems Symposium (RTSS'2003)*, 2003, pp. 286-297.
11. Dervis Karaboga, "Artificial bee colony algorithm", Scholarpedia, 5(3):6915, 2010.
12. X. S. Yang, A New Metaheuristic Bat-Inspired Algorithm, in Nature Inspired Cooperative Strategies for Optimization, (NISCO 2010) (Eds. J. R. Gonzalez et al.), Studies in Computational Intelligence, Springer Berlin, 284, 2010, pp.65-74.
13. V. Tereshko and A. Loengarov, "Collective decision-making in honeybee foraging dynamics", Computing and Information Systems Journal, Vol. 9, No.3, 2005.
14. Asaju La'aro Bolaji et al., "University course timetabling using hybridized artificial bee colony with hill climbing optimizer", *Journal of Computational Science, 2014.*