SSRG International Journal of Computer Science and Engineering
ISSN: 2348 – 8387 /doi:10.14445/23488387/IJCSE-V8I2P102

Volume 8 Issue 2, 6-9, February 2021

Jamming Attack in Wireless Sensor Networks using Ant Colony Algorithm

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

[#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 attack stops the nonstop communications and also vaporizes 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 installment 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 the Ant algorithm, and its performance analysis has been validated. The simulation outcomes demonstrate that the proposed scheme helps in accomplishing the most extreme dependability on DoS claims to enhance the Quality of Service (QoS) and the energy of WSN.*

Keywords — *Wireless sensor network, Jamming attack, Ant 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 a radio receiver end to end with an antenna, a microcontroller, an electronic circuit, an energy source, and a battery. It has numerous the application in our environment, community, military, home and beyond.

II. WIRELESS SENSOR NETWORKS (WSN)

Wireless sensor networks (WSNs) are 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 the 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 as 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 fast correspondence links, and another 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 various examples of passive attacks. In Active attacks, an attacker tries to remove or modify the messages which are transmitted on the network. Jamming, DoS, message reply, modification are 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 into the radio frequencies used by organize hubs [9]. DoS attack is "any event that wipes out a system's capacity to execute its customary limit" [10].

III. OVERVIEW OF NATURE INSPIRED PROCESS

Many natural systems of most of the creatures in the world are topics for scientific researchers. However, a simple individual behavior can help to create a system that could solve a really complex problem and perform very sophisticated tasks. Most of the social insects work without supervision and with self-organizing principles. Eric & Meyer (2001) stated that teamwork is largely self-organized, and coordination arises from a different interaction among individuals in the system. These interactions might be primitive, like ants follow odor trails, or more complex, like a honey bee dancing. The main idea is to use the self-organizing principles of insect societies to coordinate populations of artificial agents that collaborate to solve computational problems.

The collective behavior that emerges from a group of social insects has been artificially represented as a technique known as Swarm Intelligence (SI). The term swarm is used in a general manner to refer to any restrained collection of interacting agents or individuals. SI systems are typically made up of a population of self-organized individuals interacting locally with one another and with their environment. Although there is normally no centralized control structure dictating how each individual should behave, local interactions between all individuals often lead to the emergence of global behavior.

Ant Colony Optimization Algorithm

Marco Dorigo & Thomas Stützle (2004) investigated that ACO is a novel natural computation algorithm inspired by the natural behaviors of the ant colony. The parameters of ACO algorithms are chosen by means of a logical process such as a genetic algorithm in order to attain significant performance. The conventional ACO is a good combination optimization technique. ACO is originally developed to solve complicated combination optimization issues such as Travelling Salesman Problem (TSP). It looks for an optimal solution by taking into account both local heuristics and prior knowledge (Ahmed 2005). ACO is a meta-heuristic to handle combinational optimization issues through principles of communication about the paths to locate food sources by marking these paths with pheromone.

The pheromone trails can guide other ants to the food sources. It was observed that real ants were capable of choosing the shortest path between their nest and food resources in the presence of alternate paths between the two. Ants deposit a chemical substance called pheromone on their way. When the ants reach a decision point, they make a probabilistic choice influenced by the intensity of the pheromone substance. When the ants return, the probability of selecting the same path is higher because of the increase of pheromone. The new pheromone will be released on the selected path.

The ACO differs from the classical ant system in the sense that the pheromone trails are updated in two ways. Firstly, when ants construct a tour, they locally change the amount of pheromone on the visited edges by a local updating role. Secondly, after all the ants have built their individual tours, a global updating rule is applied to modify the pheromone level on the edges that belong to the best and tour found so far.

The fundamental principle of the technique is to have a population of artificial ants that cyclically construct a solution to a combinational optimization. The ants move along every branch from one node to another node and build paths representing solutions. Starting in an initial node, every ant chooses the next node in its path according to trail update and state transition rule in Dorigo et al. (2006) as below

Trail Update: Let $\tau_{ij}(t)$ be the intensity of the trail on edge (i,j) at time t. After n iterations of the algorithm, the trail intensity becomes,

$$\tau_{ij}(t+n) = \rho.\tau_{ij}(t) + \Delta\tau_{ij}(t, t+n) \qquad (1)$$

Where ρ is a coefficient such that (1- ρ) represents the evaporation of trail between time t and time t+n and

$$\tau_{ij}(t, t+n) = \sum_{k=1}^{m} \Delta\tau_{ij}^{k}(t, t+n) \quad (2)$$

Where $\Delta\tau_{ij}^{k}$ is the quantity per unit length of trail substance laid on edge (i, j) between time t and t+n by ant k. Pheromone values are updated on edge (i,j) every time an ant moves from node i to node j. The amount of new pheromone added to the edge is equal to

$$\Delta\tau_{ij}(t, t+n) = \begin{cases} Q & \text{if the kth ant goes from node i to j between time t and } t+1 \\ 0 & \text{otherwise} \end{cases} \qquad (3)$$

Where Q is the constant quantity of a pheromone.

Transition probability: The Transition probability from node i to j for k^{th} ant is,

$$p_{ij}^{k}(t) = \frac{\left[\tau_{ij}^{k}(t)\right]^{\alpha}\left[\eta_{ij}\right]^{\beta}}{\sum\left[\tau_{iu}^{k}(t)\right]^{\alpha}\left[\eta_{iu}\right]^{\beta}} \qquad u \in \text{allowed} \qquad (4)$$

Where η_{ij} is the visibility of node j from node i and it varies according to the processed application, α is sensitivity to the pheromone concentration, β is sensitivity to cost of the path.

The transition probability is a trade-off between visibility (which says that process should be chosen with high probability, thus implementing a greedy constructive heuristic) and trail intensity at time t (which says that if on edge (i,j), there has been a lot of traffic then it is highly desirable, thus implementing the autocatalytic process). The value α and β are parameters that control the effect of trail and visibility on the transition, respectively. By manipulating the value of α and β, one can transform the transition probability from greedy heuristic that values visibility over the trail ($\beta >> \alpha$), values are approximately in the same range then best results have been found.

The quantity $\tau_{ij}^{k}(t)$ is the pheromone concentration.

The pheromone level of each pair of sections is updated at the end of each trail when the ant has generated a valid dispatch of generated powers.

Mathematical Model for Ant System

The performance of the AS is determined by node spacing and parameters. The sensor network is distributed in a 2D plane, with Euclidean distance $D_{ij} = \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2}$ Where i is the source node, j is the destination node, and (Xi, Yj) are the cartesian coordinates of the node. The ant agents accumulate pheromones and dissipate energy as they traverse through the nodes controlled by path probabilities. The energy is dissipated from the sensor node after each ant passes through that node. The assumption is made that wireless nodes consume more energy than wired networks. Thus the distance is squared, and the energy dissipated for a wireless sensor node is given by Rajani Muraleedharan and Lisa Ann Osadciw (2006),

$$\Delta E_{ij} = \frac{k}{D_{ij}^2}$$

The link budget k is calculated with respect to the Bluetooth protocol. The node's remaining energy is computed by

$$E_i(t) = E_i(t-1) - \sum_j \Delta E_{ij} \qquad (6)$$

The three key elements of the ant system play an important role in making the network robust and de-centralized. The information on the resource availability at any node helps in predicting the link for the agent's next visit. The transition probability is the key factor for making decisions. Weights on each of the factors affect the movement of the ant agent in the network. Link factor is incorporated into the ant system. The transition probability is given as

$$p_{ij} = \frac{\tau_{ij}^{\alpha} . \eta_{ij}^{\beta} \left(\frac{1}{D_{ij}}\right)^{2\gamma}}{\sum_k \tau_{ik}^{\alpha} . \eta_{ik}^{\beta} \left(\frac{1}{D_{ik}}\right)^{2\gamma}} \qquad (7)$$

Where γ represent the power of the distance in probability function, and η_{ij} is then given by the normalized value of Hop(H_{ij}), Energy (E_{ij}), Bit Error Rate (B_{ij}), Signal to Noise ratio (SNR_{ij}), Packet Delivery (Pd_{ij}) and Packet Loss (Pl_{ij}) in Yun-Chia Liang and Alice E. Smith (1999).

$$\eta_{ij} = H_{ij} . E_{ij} . B_{ij} . SNR_{ij} . Pd_{ij} . Pl_{ij} \qquad (8)$$

IV. RESULTS AND DISCUSSION

The sensor network is built based on the following assumptions as[18], (1) All nodes are initialized with varying energy levels, thus giving each different capacity to transmit messages (2) Each node has a varied threshold. Therefore the probability of all nodes failing in the same coverage is very low. (3) The number of hops taken by the agent is adjustable, i.e., it is user-defined, but it depends on the number of active nodes. (4) The source and destination nodes are user-defined, (5) Tolerance are set for every packet loss and successful packet delivery, beyond which a node is penalized for its behavior; and (6) Sensor mobility is not considered, the links are heterogeneous. The probabilistic approach of the ant system depends on the energy depletion and the percentage of false decisions. The two factors need to be minimal. The accuracy of the decision is specified in terms of the rate, namely, false alarm rate, miss rate, and detection rate. The problem of Denial of Service using the jamming attack in the physical layer of a wireless sensor network can be formulated as a hypothesis testing problem where the two hypotheses are H_0: The DoS claim is false and H_1: The DoS claim is genuine. (5)

A sensor network with 16 nodes is considered in this simulation run with agents randomly placed on the nodes. After converging, the ant agents adapt to the network using the knowledge acquired from their neighbors. The figure below illustrates scenarios using different types of jammer and the effectiveness of the evolutionary algorithm in assessing the performance of the network. The proposed detection and defense mechanism is simulated using Matlab 6.5. The performance of the network, based on the distance, energy depleted, percentage of packet loss, and packet delivery, is shown in the figures.

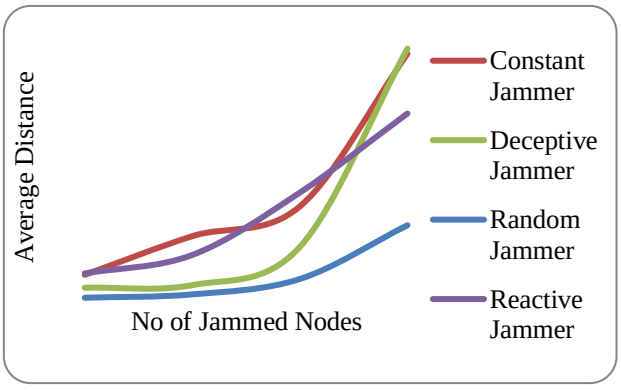

Fig. 1 Performance of Network-Based on Distance

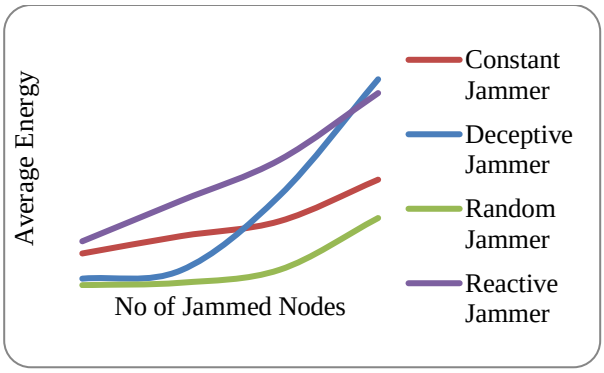

Fig. 2 Performance of Network-Based on Energy

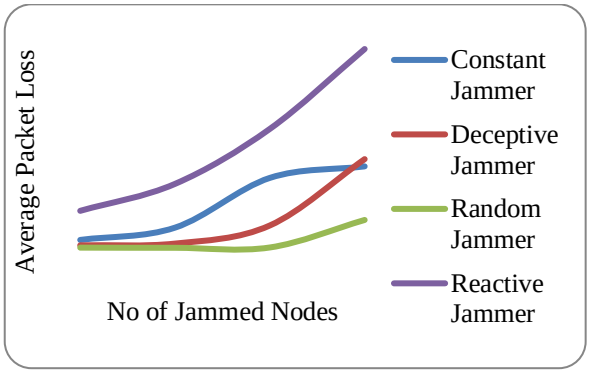

Fig. 3 Performance of Network-Based on Packet Loss

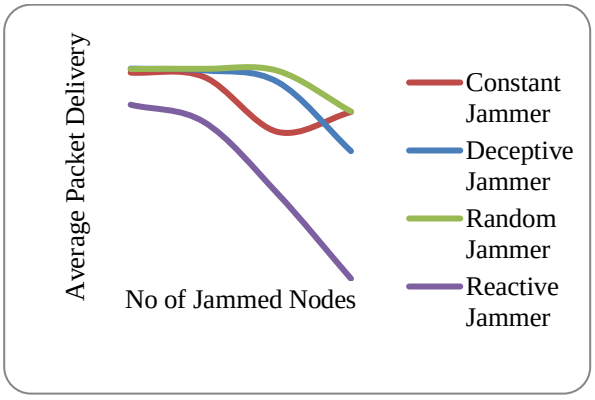

Fig. 4 Performance of Network-Based on Packet Delivery

V. CONCLUSION

This paper proposes a novel method to detect jamming attacks using a modified ant system. The performance parameters such as hops, energy, distance, packet loss, SNR, BER, and packet delivery influence the decision taken in anti-jamming techniques. The figure presented in the result section reemphasizes the fact that a sensor network remains functional and assesses the situation under all critical conditions. In the future, we hope to apply some applications that have to deploy a large number of nodes. We also will compare other optimal algorithms.

REFERENCES

[1] D. L. Adamy, D. Adamy, EW 102: A Second Course in Electronic Warfare, Artech House Publishers, (2004).

[2] E. Shi, A. Perrig, Designing Secure Sensor Networks, Wireless Communications Magazine, 11(6)(2004) 38-43.

[3] A. D. Wood and J. A. Stankovic, Denial of service in sensor networks, Computer, 35(10)(2002) 54-62.

[4] W. Xu, W. Trappe, Y. Zhang, T. Wood, The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, in Proc. 6th ACM international symposium on Mobile ad hoc networking and computing, (2005) 46-57.

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Commun. Mag., (2002) 102-114.

[6] Ali Hamieh and Jalel Ben-Othman, Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution, ANR (French Research National Agency) under CLADIS grant N. 05-SSIA-0018.978-1-4244-3435-0/2009 IEEE.

[7] Tao Jin, Guevara Noubir, and Bishal Thapa, Zero Pre-shared Secret Key Establishment in the Presence of Jammers, Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing, (2009) 219-228.

[8] Yao Liu, Peng Ning, Huaiyu Dai, and An Liu, Randomized Differential DSSS: Jamming-Resistant Wireless Broadcast Communication, IEEE INFOCOM, (2010) 1-9.

[9] Loukas Lazos, Sisi Liu, and Marwan Krunz,Mitigating Control-Channel Jamming Attacks in Multi-channel Ad Hoc Networks, Proceedings of the second ACM conference on Wireless network security, (2009) 169-180.

[10] Hong Huang, Nihal Ahmed, and Pappu Karthik, On a New Type of Denial of Service Attack in Wireless Networks: The Distributed Jammer Network, IEEE Transactions on Wireless Communications, 10(7)(2011).

[11] Alejandro Proan˜o and Loukas Lazos, Packet-Hiding Methods for Preventing Selective Jamming Attacks, IEEE Transactions On Dependable and Secure Computing, 9(1)(2012).

[12] Andrea Richa, Christian Scheideler, Stefan Schmid and Jin Zhang, A Jamming-Resistant MAC Protocol for Multi-Hop Wireless Networks, Distributed Computing Lecture Notes in Computer Science 6343(2010) 179-193.

[13] Varad A. Sarve, Dr. Swati S. Sherekar and Dr. Vilas M. Thakare, Learning the Channel Uncertainty for Defensive Security Enhancements in MANET with Trust Management SSRG International Journal of Mobile Computing and Application 4.1 (2017) 21-27.

[14] Jerry T. Chiang and Yih-Chun Hu, Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks, IEEE/ACM Transactions on Networking, 19(1)(2011).

[15] Mario Cagalj, Srdjan Capkun, and Jean-Pierre Hubaux, Wormhole-Based Antijamming Techniques in Sensor Networks Mario, IEEE Transactions on Mobile Computing, 6(1)(2007).

[16] Sisi Liu, Loukas Lazos, and Marwan Krunz, Thwarting Control-Channel Jamming Attacks from Inside Jammers,IEEE Transactions on Mobile Computing, 11(9)(2012).

[17] Zhenhua Liu, Hongbo Liu, Wenyuan Xu, and Yingying Chen, Exploiting Jamming-Caused Neighbor Changes for Jammer Localization, IEEE Transactions On Parallel And Distributed Systems, 23(3)(2012).

[18] E. M. Saad, M. El Adawy, H. A. Keshk, and Shahira M. Habashy Ant Algo Modification, Helwan University.

[19] Rajani Muraleedharan and Lisa Ann Osadciw, Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System, Syracuse University.