Analysis of Swarm Intelligent Based Defense Algorithm for Detecting Jamming Attack in Wireless Sensor Networks (WSNS)

E. Sasikala and N. Rengarajan

1AP/CSE, SRM University, Chennai, India
2Principal, Nandha Engineering College, Erode, India

Abstract: Wireless Sensor Networks (WSNs) are one of the most widely used technologies in our daily lives. However, since wireless sensor networks are based on communication within radio channels, WSNs are susceptible to malicious attempts to block the channel. One of the most frequently used attacks is a jamming attack. This type of attack not only blocks the ongoing communication but also exhaust the energy of the sensor nodes. This paper attempts to detect jamming attack and defense mechanism is proposed through intelligent system. The proposed system is simulated using MATLAB. According to the simulation results obtained, the intelligent system detects jamming attack with high detection rate of 99.8% and low false positive rate.

Key words: Ant Colony Optimization • Artificial Bee Colony • Bat Algorithm • Jamming Attack • Wireless Sensor Networks

INTRODUCTION

A Wireless Sensor Network is a self-configuring network of small sensor nodes communicating among themselves using radio signals and deployed in quantity to sense, monitor and understand the physical world. WSN can be used for a wide variety of applications dealing with monitoring, control and surveillance. The design and development of a successful network must address many challenges dictated by WSN characteristics are small node size, low node cost, low power consumption, limited hardware resources, massive and random deployment, scalability, data aggregation, quality of services and security.

One of the most frequently used attacks in wireless sensor networks is a Denial of Service (DoS) attack known as a jamming attack. This type of attack not only blocks the ongoing communication but also exhaust the energy of the sensor nodes.

Many security solutions for WSNs currently exist as external modules, separate from fundamental functions of the protocol stack. Some rely upon physical-layer features that would be impractical for direct deployment in a realistic network, or impose excessive overheads or computational complexity that would be insufficiently scalable. Furthermore, it is not possible for cryptographic solutions to guarantee security in the presence of attacks with external devices that modify the topology.

Motivation and Objective: It is meticulous to know about the existing methods of detecting the jamming conditions is decentralized, where the individual nodes are solely responsible for taking decisions in the complete process of data collection and processing. The noticeable drawback of this approach is complete processing and decision making is done at the node level. This is not practicable as the WSN nodes are resource-starved and that because nodes may not be able to communicate with others during jamming. Therefore, the author chose the centralized approach instead of decentralized approach.

The main objective of this work is to detect jamming attack in wireless networks with the objective function of high detection rate and low false positive rate. Based on the investigations, in this research, the author utilizes intelligent techniques such as ant colony optimization, artificial bee colony algorithm and bat algorithm for obtaining the best solution for jamming detection.
Jammer and its Types: Jammer is defined as an individual who is intentionally obstructing the legal wireless communication. It is treated as an active attacker depending upon its intentions and actions. Jamming is a special category of DoS attack used in wireless networks. Handling of Jamming attacks is more difficult than other attacks. Jamming attack can be categorized as academic and military jammers. The academic jammer focuses on data-link layer with RF power levels that are balanced with the existing transmission power of WSN node. This type of jammer have few resources with partial or wide knowledge related to protocols that are intended to attack network from within the geographical area of WSN. Whereas military jammer focus on RF power.

Academic Jammers: According to Xu et al [1], the academic jammers are categorized as follows

Constant Jammer: Continually emits a radio signal without following any MAC layer etiquette.

Random Jammer: Operates randomly in both sleep and jam intervals. During sleep interval, it sleeps irrespective of any traffic on the network and during its jamming phase, it can either behave like a constant jammer or a deceptive jammer. It does not follow any MAC protocol.

Deceptive Jammer: Is similar to constant jammer. Their similarity is due to the fact that both constantly transmit bits. The main difference is that with the deceptive jammer, the transmitted bits are not random. The deceptive jammer continually injects regular packets on the channel without any gaps between the transmissions. This makes the overhearing user to believe that there is a legitimate transmission going on.

Reactive jammer activates when it senses the transmission on the channel. If the channel is idle, it remains inactive and keeps sensing the channel.

Law et al [2], have suggested four types of energy-efficient jammers for attacking a network following the S-MAC protocol:

Periodic Listening Interval Jammer: Attacks when the nodes are in listening period and sleeps at all other times.

Periodic Control Interval Jammer: attacks when the nodes are in the control period and sleeps during rest of the time.

Periodic Data Packet Jammer: Listens to the channel during the control interval and attacks the data segment.

Periodic Cluster Jammer: Is meant for attacking networks following encrypted packets. It uses k-means clustering algorithm to separate clusters of the network and statistical estimations to determine the timing of the data segment and then attacks the same accordingly.

According to Wood et al [3] jammers are classified in to four types. They are described as below:

Interrupt Jammer: Gets activated by means of a hardware interrupt when a preamble and start of frame delimiter (SFD) are detected from a received frame.

Activity Jammer: Gets activated when it detects SFD, otherwise not possible.

Scan Jammer: Is similar to the Sweep Jammer. Instead of detecting a packet in a single channel, it searches out all possible channels for a packet during a defined period of time and having succeeded, it then attacks the channel.

Pulse Jammer: Is similar to the Constant Jammer; it sends small packets constantly to jam a channel.

Muraleedharan et al [4] have described four jammers. They are, the Single-Tone Jammer attacks one channel at a time, the Multi-Tone Jammer can attack some or all the channels of a multi-channel receiver, while the Pulsed-Noise Jammer is a wide band jammer, sending pulsed jamming signals by turning on and off periodically at a slow or fast rate. ELINT, as they describe, is typically a passive system that tries to break down or analyze radar or communication TCF signals and thus, strictly speaking, is not a jamming attack model.

Military Jammer: Military jammers are classified in to three types. They are described as below:

Spot Jammer: The attacker focus on a single frequency that the target uses and jam that with less power is called as spot jammer. It is more efficient and effective jammer. The disadvantage of this jammer is that the target network can change the channel to evade jamming.

Sweep Jammer: This type of jammer sweep across the probable spectrum either periodically or aperiodically, thus jamming the affected networks temporarily. They are less efficient and effective than the spot jammer.
**Barrage Jammers:** The attacker jams the range of frequency at the same time is known as barrage jammers. It requires high RF power to jam the multiple frequencies at one time.

**Selection of Jammers:** The proposed method uses the Constant Jammer, Deceptive Jammer, Reactive Jammer and Random Jammers, which are in fact, the models proposed by Xu *et al.* [1] & Misra *et al.* [5].

**Selection of Metrics:** The selected metrics for this research work is Packet Delivery Ratio (PDR), Energy, Distance, Packet Loss and signal to noise ratio (SNR). The reason for the selection have been discussed and summarized.

- PDR and Packet Loss are very good metrics which are capable of being measured accurately by the node without any computational overhead.
- The energy and distance enable to decide whether the current path is capable of communicating with its neighbors or not.
- The received power level at a node is easily measurable as nodes are/can be provided with RF power meter.

**Related Works:** A novel method of avoiding sensor network under jamming attack by using evolutionary algorithm, the ant system has been proposed by Muraleedharan & Osadciw [4]. In the system, the agents minimize energy and keep track of network requirements. As the ant moves from node to node, energy is lost through communication. The ant stops traversing a node once its energy is depleted. New paths are set up to avoid the node so that communication continues without the degraded sensor. These agents ensure that the optimal route to the destination using limited resources and also learning the network environment. The performance parameters such as hops, energy, distance, packet loss, SNR, BER and packet delivery influences the decision taken in anti-jamming techniques. Initially, the computational cost and time is high but this drops drastically once the agents learn the network and environment.

Periyanayagi & Sumathy [6] proposed a swarm based defense technique for jamming attacks in wireless sensor networks. Swarm intelligence algorithm is proficient enough to adapt change in network topology and traffic. The sender and receiver change channels in order to stay away from the jammer, in channel hoping technique. The jammers remain on a single channel, hoping to disrupt any fragment that may be transmitted in the pulse jamming technique. Using the swarm intelligence technique, the forward ants either unicast or broadcast at each node depending on the availability of the channel information for end of the channel. If the channel information is available, the ants randomly choose the next hop. As the backward ants reaches the source, the data collected is verified to find out in which channel there is prevalence of attacker for a long time and those are omitted. Simultaneously the forward ants are sent through other channels which are not detected before for attacks. This scheme helps limit the channel maintenance overhead. By simulation results, it is clear that this swarm based defense technique for jamming attack is more effective than the existing works.

Pintea & Pop [7] proposed a new defense mechanism for different jamming attack on Wireless Sensor Network (WSN) based on ant system is introduced. The artificial sensitive ants react on network attacks in particular based on their sensitivity level. The information is re-directed from the attacked node to its appropriate destination node. It is analyzed how are detected and isolated the jamming attacks with mobile agents in general and in particular with the newly ant-based sensitive approach.

In multi-agent systems, digital pheromone swarming algorithms are used to coordinate the agents to achieve complex and intelligent behaviors. Studies have shown that pheromone swarming systems are versatile, efficient and resilient to failures and thus are applicable in various scenarios such as border control, area coverage, target tracking, search and rescue, etc. Due to their reliance on wireless communication channels, which are vulnerable to interference and jamming attacks, it becomes important to study the security of these systems under malicious conditions. Kelly *et al.* [8] investigated the security of pheromone swarming under different types of jamming attacks. In particular, this work exposed novel types of stealthy attacks that aim to maximize the damage inflicted on the swarm while reducing the risk of exposure. Unlike complete Denial of Service (DoS) attacks, the attacks exposed to select which signal interferes with, based on the current state of the swarm. This work has assessed the impact of the attacks through new metrics that expose the tradeoff between damage and cost.

Junjea *et al.* [9] proposed a routing algorithm that detects congestion and DDoS attack. Although researchers have proposed a number of mechanisms for preventing congestion and attacks in WSN but very few of them have thought of deploying ants as intelligent...
entities. Moreover, the previous works had been focusing on using parameters like energy, hop and distance but none have used age and reliability of node as important parameters. This work uniquely contributes an ant-based routing algorithm that considers all of the above mentioned parameters.

Research Methodology

Enhanced Ant Colony Optimization (EACO): In Ant Colony Optimization algorithm, the fundamental principle of the technique is to have a population of artificial ants that cyclically construct a solution to combinatorial optimization. The ants move along every branch from one node to another node and so build paths representing solutions. Starting in an initial node, every ant selects the next node in its path based on trial update and state transition rule, as discussed in Dorigo et al [10].

The transition probability from node i to j for k\textsuperscript{th} ant is

\[ p_{ij}(t) = \frac{(r_{ij}^\alpha)^\alpha(r_{ij}^\beta)^\beta}{\sum(r_{in}^\alpha)^\alpha(r_{in}^\beta)^\beta} \]  (1)

The transition probability is a trade-off between visibility and trail intensity at time t. The values \( \alpha \) and \( \beta \) are parameters that control the effect of trail and visibility on the transition respectively. The main drawbacks of ACO are slow convergence rate and the random number is stochastic. To overcome the above drawbacks, a enhanced ACO is presented. This aims to direct the ants’ search towards very high quality solutions. This avoids premature convergence so as to exploit more strongly, good quality solutions during the search.

ACO algorithms can be enriched with additional capabilities to improve the efficiency and efficacy of the system. For example, the improvements are made by updating pheromones, changing evaporation coefficient or the amount of released pheromones in order to avoid stagnation. In this work the improvements are made by updating pheromones and the new updated pheromone equation is given below:

Pheromone Update: Let \( \delta_{ij}(\text{new}) \) be the intensity of the trail on edge \((i,j)\) at time t. After initialization/first iteration/n iterations of the algorithm the trail intensity becomes.

\[ \tau_{ij}(\text{new}) = (1-\rho)\tau_{ij}(t) + \Delta \tau_{ij}^{opt} \]  (2)

where,

\[ \Delta \tau_{ij}^{opt} = \begin{cases} \left(\frac{f_{ij}^A - r_{ij}^A}{f_{ij}^A - f_{ij}^G}\right)x\left(\frac{f_{ij}^G - f_{ij}^H}{f_{ij}^G - r_{ij}^G}\right) & \text{if } (i,j) \in F \\ 0 & \text{Otherwise} \end{cases} \]

where \( \rho \) is evaporation rate, F – fitness function \( \Delta \tau_{ij}^{opt} \) - required optimal trail/path for ant x.

In the existing algorithm (Dorigo et al [11]), pheromone update is a function of scalar distance travelled by the ants between the nodes, whereas in the proposed algorithm pheromone updation is a function of vector distance travelled by the ants between the nodes. The graphical representation of proposed pheromone update function is shown in Figure 1.

As from the figure, updated global distance is not in the same direction as previous global best location C-A can’t be a function not in the same direction that of previous global best, whereas proposed equation is function of the direction as well as magnitude of distance travelled by ant which increases the better convergence of the algorithm.

Enhanced Artificial Bee Colony (EABC): In the ABC algorithm, a food source position denotes a probable solution of the problem to be optimized which is denoted by a d-dimensional real-valued vector. The nectar amount of a food source equivalent to the quality (fitness) of the connected solution, is described by Dervis Karaboga [12]. The number of employed bees or the onlookers is identical to the number of the food sources (solutions) in the population. Alternatively, for every food source, there is only one employed bee. The basic ABC algorithm is a simple, robust and effortlessly controlled algorithm. But, as a random optimization algorithm, ABC algorithm has slow convergence features and easily gets stuck on local solutions. The basic ABC algorithm is enhanced to obtain a better optimization value. In this finding, sensibility based ABC technique has been employed. An improvement has introduced to increase the sensitivity of bee search path to give importance to all the food sources, which an important criteria for constrained problems. There is possibility of having minimum food sources found by the employee bees, (i.e) multiple fitness values having less than global fitness (F\(_{\text{gb}}\)) value in the current search space.
Enhanced Bat Algorithm (EBAT): BAT algorithm (BA) is a meta-heuristic algorithm, based on the echolocation behavior of bats was developed by Yang [13]. Echolocation of bats works as a type of sonar, it produces a loud and small beat of sound and waits as it hits into an object, after a few seconds the sound turns back to their ears. Therefore, bats can calculate how far they are from an object.

Bat Algorithm is powerful at exploitation but has some insufficiency at exploration, thus it can easily get trapped in local minimum on most of the multimodal test functions. In order to overcome this problem of standard BA, modifications are applied to improve exploration capability of BA.

Contrary to Bat Algorithm, Artificial Bee Colony (ABC) Algorithm is good at exploration. Scout Bee phase of ABC provides algorithm to explore new areas in search space. In order to fix the lack of exploration of BA, it hybridized with this part of ABC to improve exploration capability of BA. For this, limit values are defined for all bats. In the case of a solution cannot be further improved, it will start to exceed predetermined number of trials called as “limit”. If a solution exceeds the threshold value “limit,” then that solution replaces with new one by random search. This decreases lack of exploration capability of BA.

Simulation Setup and Results Discussion
Simulation Setup: To evaluate the performance of the proposed method with the presence of jamming attacks, a square grid network and different types of jammers are established in an experimental environment. Six sets of inter-nodal distances: 5, 10, 15, 20, 25 and 30 meters; and four positions for the jammer: two inside and two outside the grid were selected for the simulation. Four sets of total number of nodes: 25, 50, 75 and 100 were considered. Thus a total of 384 simulations with corresponding aforesaid parameters, were done using the MATLAB simulator.

The details of the input parameters used for the simulation in respect of the WSN and those parameters which are globally applicable to the jammer-simulation are given in Table 1.
RESULTS DISCUSSION

The performance evaluation of any model that detects a jamming attack is a difficult proposition because there is no known theoretical or practical model that can be taken as a benchmark for comparison. It is perhaps because of this that all of the authors related with jamming detection quoted so far, except, Cakiroglu & Ozcerit (2011) have chosen not to evaluate their methods. Even the performance evaluation method described by Cakiroglu & Ozcerit (2011), is ambiguous because they have neither defined the ‘fitness value’ nor have they described the method to calculate it; and but have used it to study the performance parameters, ‘detection rate’ and ‘false positive rate’. The mean detection rate and false positive rate from these simulations were collated for different jammed node ratios (JNR) under different configurations for different types of jammers. The values of detection rate and false positive rate for different types of jammers are shown in Figure 2 & Figure 3, respectively. It is demonstrated in the Figure 2 and 3 that the proposed Enhanced BAT approach of the constant, deceptive, reactive and random jammer attains the detection rate of 99.61, 99.5, 99.25 and 98.95 for 50 nodes and false positive rate of 0, 0.2, 0.09 and 0.01 for 50 nodes. It is clearly observed from the figure that the proposed approach produce high detection rate of 99.8% and low false positive rate.

CONCLUSION

It is inferred from the investigations of the results, the proposed Enhanced BAT algorithm approach performs better than the other approaches namely EACO and EABC in terms of high detection rate and low false positive rate. The objective of this research has been achieved in short time because of the faster convergence of this EBAT optimization technique.

The future enhancements of the present work would be to use adaptive hybrid Optimization algorithms. Also in the future work, the proposed routing algorithm needs to be improved effectively for those nodes with high mobility.

REFERENCES


