International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 10849-10858

http://www.ripublication.com

Physical Layer Security In Wireless Sensor Networks (WSNs): Bat Algorithm

Sasikala E and Dr.N.Rengarajan

Abstract

The wireless sensor networks (WSNs) has become vulnerable to jamming attacks due to open share of physical medium. As such attacks encourage strong interferences resulting in denial of service. This paper attempts to detect jamming attack in wireless sensor networks using BAT algorithm. The proposed method can be simulated by using MATLAB. Simulation results expose the effectiveness of the proposed method which could defeat the jamming attack and maintain considerable performance of the overall network.

Keywords: Wireless Sensor Networks; Jamming Attack; Denial-of-Service (DoS) attacks; Intelligent Technique; BAT Algorithm.

Introduction

Wireless sensor networks have a large number of tiny low-power sensor nodes and those nodes are mainly for their low energy consumption, low cost and wireless communication [1]. Their role is noteworthy in many applications such as Military, Medical, Object Tracking, Nuclear Power Plant and Environment Monitoring, etc., they lack security in many applications such as military sensing and tracking because of their resource constraint nature [2].

Jamming is a notable feature of Denial of Service (DoS) attacks. Jamming drives electromagnetic energy towards a communication system to prevent signal transmission [3]. In WSNs, jamming interferes in to the radio frequencies used by network nodes [4]. DoS attack as "any event that eliminates a network's capacity to execute its normal function" [5]. Xu et al. [6] discussed various jamming methods.

Jamming causes many problems in real world applications. For example, in border security, an intruder can jam the communication and cross the border without being detected. Thus, in hostile environments, it is essential to detect the place where the channel is jammed [7-8] or deliver the messages out of the jammed area [7], [9-11]. In this paper, we focus on optimization techniques to detect jamming attacks. Previous studies have shown that the nodes being jammed will see a substantial drop in the packet delivery rate (PDR) [12]. Hence, once a node realizes that its packet delivery

ratio drops significantly, a jamming alert can be produced. However, current PDR-based schemes use the end to end packet delivery ratio, which requires one to observe communication for a long time before any good decision is made. The selected research work focuses on quick detection of jamming attacks with the assistance of Packet Delivery Ratio (PDR), Energy, Distance, Packet Loss and Received Signal Strength (RSS) to determine the jamming attacks in WSN using meta-heuristic optimization techniques.

Related Works

In [13], the ant system forms an agent (ant) that proactively makes use of the WSN node's information, to predict jamming, and changes the route accordingly to avoid jamming. Parameters such as hops, energy, distance, packet loss, SNR, Bit Error Rate (BER) and packet delivery affect the probability of selecting a specific path or solution. Limitations of the work are increased computational and energy cost.

In [14], a fuzzy inference system-based jamming detection method is a centralized approach, where in the jamming detection is done in the base station based on the jamming detection metrics received from the respective nodes. Three inputs are used in the base station to compute PDPT and SNR values. To get 'Jamming Index' (JI) as output of the system, the base station uses the values of PDPT and SNR as inputs. The JI value varies from 0 to 100, signifying 'No Jamming' to 'Absolute Jamming' respectively.

In [15], to defeat the reactive jamming, an immunological anti-jamming method based on adaptive immune system of human beings has been proposed by the author. The system consists of three function modules such as monitoring agent, decision agent and recovery agent. A monitoring agent monitors the behaviors of its neighbors and sends results to the decision agents. The decision agent detects jamming attacks based on the features of known jamming attacks from the local jamming pattern database. Jamming pattern database gets updated when new jamming attacks are recognized by examining both abnormal behaviors of jammers'. Finally, recovery agents eliminate the impacts of jamming attacks through various mechanisms, such as path switching, Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), etc.

In [16], the author considered four types of jamming such as interrupt jamming, activity jamming, scan jamming and pulse jamming. The solutions proposed in this work are as follows: Frame Masking is a method to defend against interrupt jamming, where the sender and the receiver node agree with a secret pseudorandom sequence for the SFD in each packet. Frequency hopping is a method proposed for activity jamming. The author suggests packet fragmentation for scan jamming. Redundant encoding is the proposed method for pulse jamming. The limitation of the proposed work is increased computational and energy cost. The proposed solution against interrupt jamming cannot defend against constant jammer.

In [5], JAM algorithm aids in detecting and mapping of jammed regions. Data is then simply routed around the jammed regions. The function of jamming detection module is to transmit jammed or unjammed message to its neighbor nodes. The

jammed node will not be able to send any messages, if MAC protocols require a carrier sense to indicate a clear channel in order to have clearance for transmission. To cope with this problem, MAC must provide a way to override carrier-sense to allow broadcasting a brief, high-priority, unacknowledged message. The drawback of the proposed method is it will fail if the attacker JAMs the entire WSN or a significant percentage of nodes.

In [17], Query-based jamming detection algorithm QUJDA is an anomaly-based approach used. The network parameters considered for jamming detection are PDR, bad packet ratio (BPR), and energy consumption amount (ECA). The threshold values are determined to separate network from abnormal condition. Due to many parameters, processing overhead has become the main drawback. Maximum

Methodology

BAT Algorithm

Intelligent optimization techniques are computationally fast and converges quickly to optimal or near optimal solutions in many practical optimization problems. Most of the algorithms are population-based, relying on initial randomization associated with logical patterns. Different constraint handling methods were suggested and those are known as intelligent techniques/Heuristic Methods.

BAT algorithm (BA) is a meta-heuristic algorithm, based on the echolocation behaviour of bats. The Bat calculation is an algorithm based on the echolocation performance of bats used for optimization problems. The ability of echolocation of bats is attractive, as these bats can discover their prey and identify the insects even in complete darkness. The advanced capability of echolocation of bats has been used to solve different optimization problems. Echolocation of bats works as a type of sonar, it produces a loud and small beat of sound, waits as it hits into an object, after a few seconds the sound turn back to their ears. Therefore, bats can calculate how far they are from an object. With the reference of the bats' behaviour, a new metaheuristic type technique called Bat Algorithm was developed by yang [18]. Such optimization technique has been developed on the basis of the ability of echolocation of the utilization of bats.

Bat algorithm idealized rules:

1. All bats custom echolocation to intellect distance, and they likewise know the difference between sustenance/prey and circumstantial barriers in particular magical approach.
2. Bats fly arbitrarily with velocity v_i at point x_i with a fixed frequency z_{low} changing wavelength λ and volume A_0 to search for sustenance. They can spontaneously modify the wavelength (or frequency) of their emitted beats r $\in$ [0, 1] and change the rate of beat based on the closeness of their target.

3. Despite the fact that the volume may vary from various perspectives [18], it is assumed that the volume varies from a large (positive) A_0 to a smallest constant value $A_{\min}$.

The points χ_i and velocities v_i in a dimensional search space are updated using the following equations 2, 3 and 4. The new solutions χ_i^t and velocities v_i^t at time step t are given by,

$$z_i^t = (z_{high} - z_{low})\alpha + z_{low} \tag{1}$$

$$V_i^t = V_{i-1}^t + (X_i^t - optimal)z_i \tag{2}$$

$$X_i^t = X_{i-1}^t + V_i^t \tag{3}$$

Where, α is an arbitrarily generated number in the interval [0, 1] is a random vector drawn from a uniform distribution. For the local search part, once a solution is nominated among the current best solutions, a new solution for each bat is made locally using random walk:

$$X_{new} = optimal + \varepsilon A^t \tag{4}$$

Where, $\varepsilon \in [-1, 1]$ is a random number, while $A_t = < A_i^t >$ is the average loudness of all the bats at this time step [18]. Figure.1 shows the flowchart of Bat algorithm [18].

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 [13] are established for an experimental environment. Different values of the following parameters are selected to adjust the attacking strength of those jammers: jamming range and number of jammers. The proposed detection and defense mechanism are simulated with the help of gr Theory toolbox in MATLAB. The performance of the network could be analyzed by considering varied Jamming to signal ratio (J/S), energy to jamming density ratio, energy to noise density ratio, multi-path interference. The radio-propagation model and the antenna model are taken for this system is Omni-antenna and Two Ray Ground model [19]. A classical reactive routing protocol called Ad hoc On-Demand Distance Vector (AODV) is considered for this work. A square grid of 100 immobile nodes (numbered from node 0 to node 99 column by column) is found in the simulated network. Node 0 as the source node and node 100 that spots at the opposite to node 0 as the destination node, where data flow that starts at simulation time of 20s.

The source node originates User Datagram Protocol (UDP)/constant bit rate (CBR) flows with a packet size of 1024 bytes and a transmission rate of 0.02 mbps to its intended destination and for jammer the packet size and transmission rate are varied.

More simulation parameters are listed as follows: Frequency, wavelength and antenna gain are set to 864.536 MHz, 0.424 m and 1.5 dB, respectively. The MAC protocol used in this proposed method is BMAC. The transmitted power for sensor network is 8.56 × 10-4 W and for jammer its varied. The receiver sensitivity and path loss are 3.652 × 10-4 W and 1.5 dB. Initially, the number of jammed node in a period t seconds is 12. Hence, the number of nodes jammed is 12 out of 100 in the network. Similarly in each case nodes are jammed for t seconds.

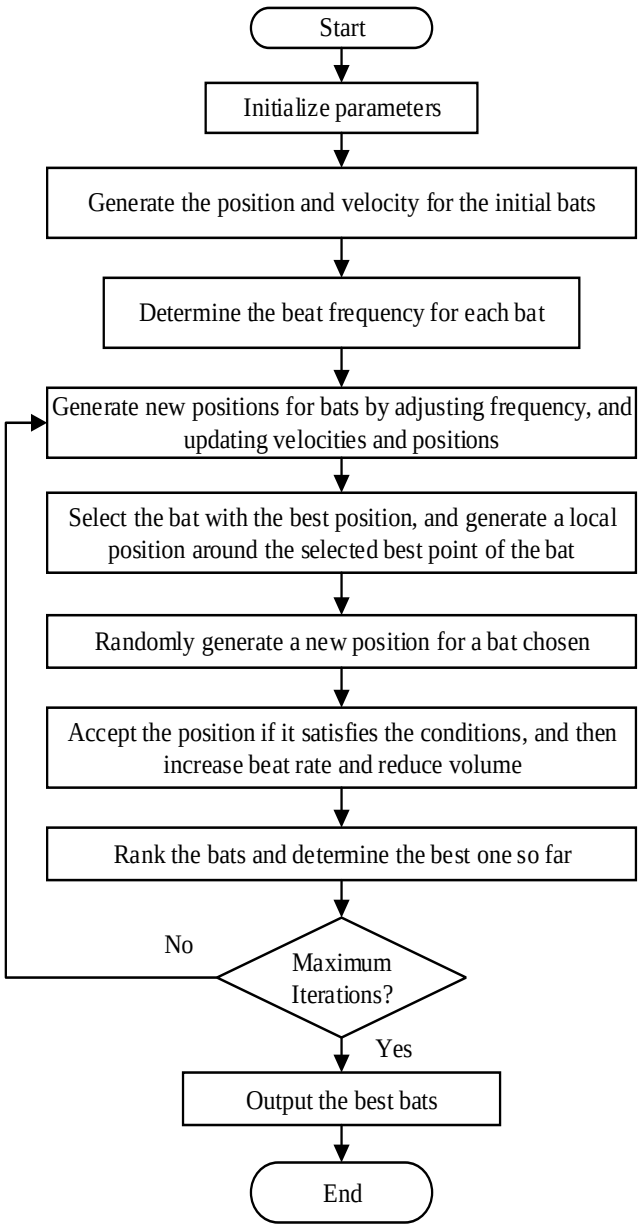

Figure 1: Flowchart representation of Bat algorithm

The jammer was programmed to transmit at the same power level as the node which is power level 1. Figure 2 shows the square grid 100 node wireless sensor network topology and the jammer's various position for testing the protocol. Depending on the

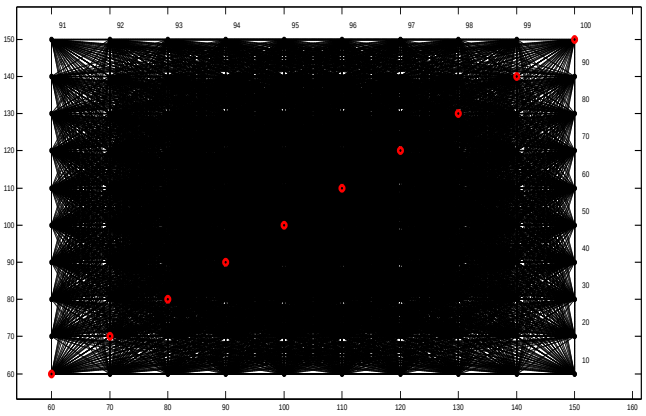

Figure 2: Proposed Square grid 100 node WSN network

position of a node in the network, the number of neighbours for a node varied from 6 to 14 nodes. Though the nodes were not time synchronized, they were all running at the same intervals of time. Nodes which lie on the edge of the network were having less number of neighbours and nodes which lie inside the network were having more number of neighbours. Tests were carried out to record the detection time, detection rate, and the false alarm rate of the protocol.

Simulation Results

The Figure 3 illustrates scenarios using different types of jammer and the performance of the network based on the energy depleted, distance, and packet loss and packet delivery ratio. The proposed BAT technique is evaluated with the results of ABC and Ant System. From the result, the proposed method detects jamming attacks by checking the energy, distance, Packet loss and packet delivery ratio, investigating the abnormal behaviors of neighbors radio signals. Then, the proposed method recovers the network from jamming attacks using path switching. Thus, the proposed method is effective to protect the network from attacks launched by different jammers. Comparative results were presented in Fig.3-6. From the figure the superiority of BAT technique for jamming attack has been proved

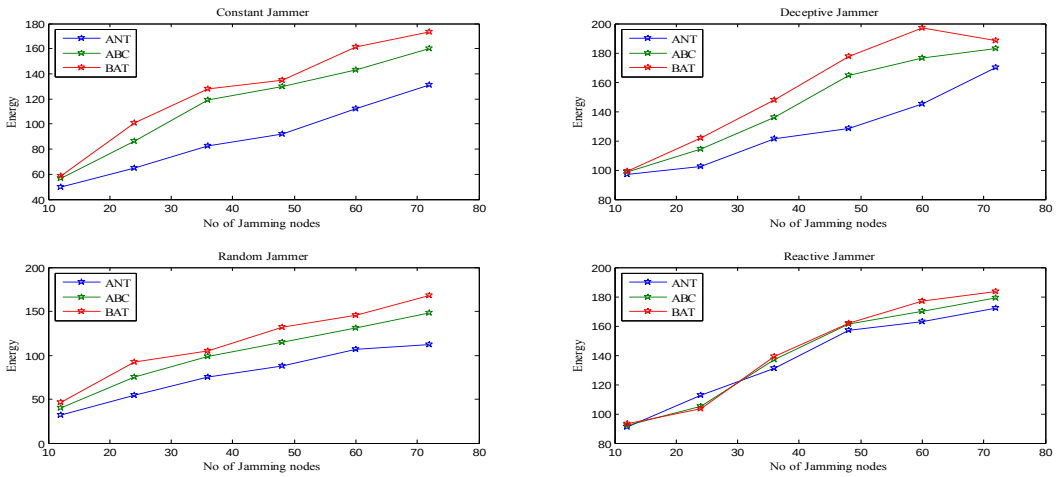

Figure 3: Comparison of BAT with Ant & ABC System by means of Energy

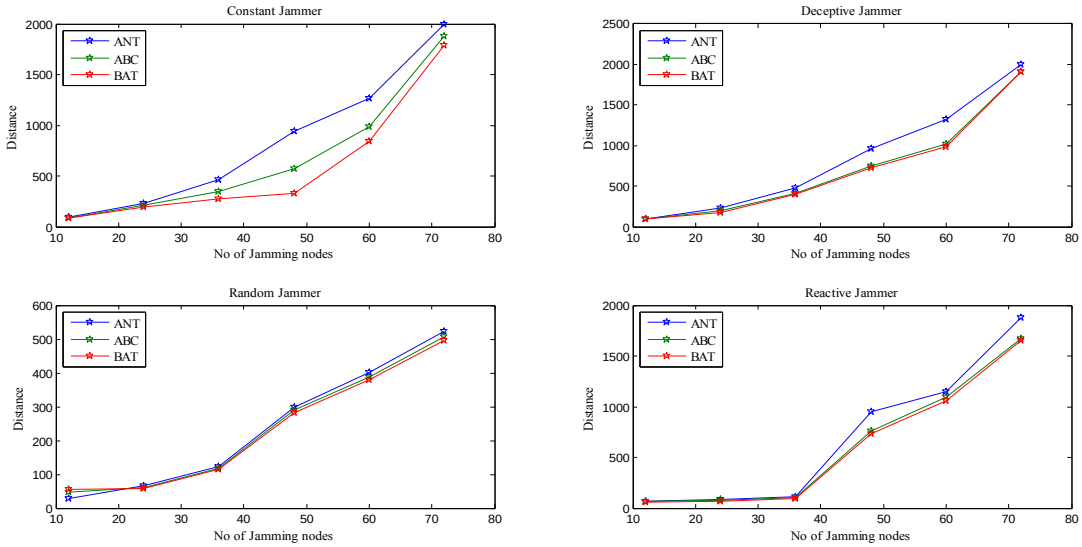

Figure 4: Comparison of BAT with Ant & ABC System by means of Distance

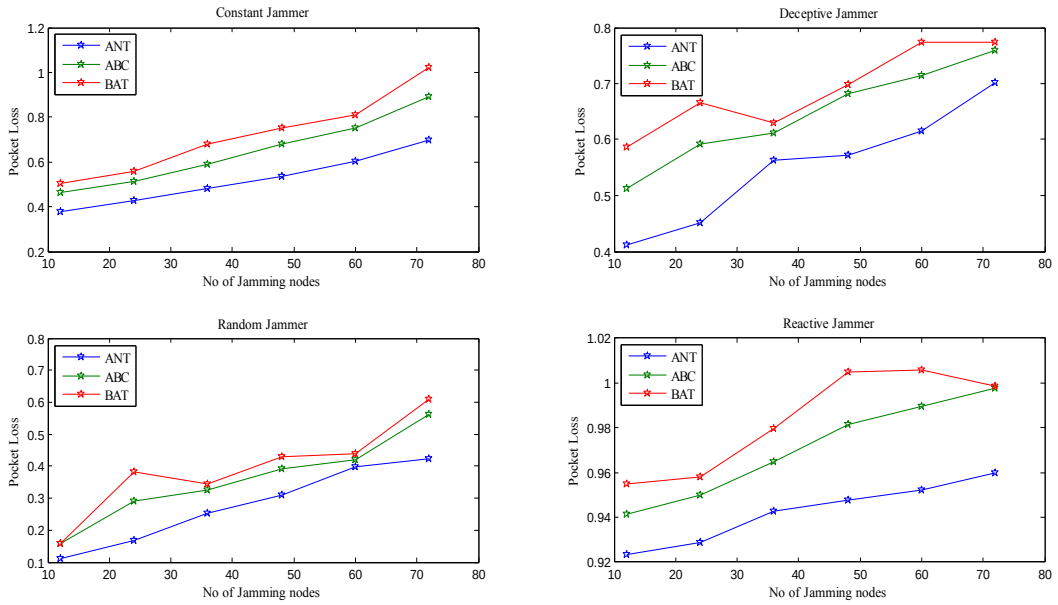

Figure 5: Comparison of BAT with Ant & ABC System by means of Packet Loss

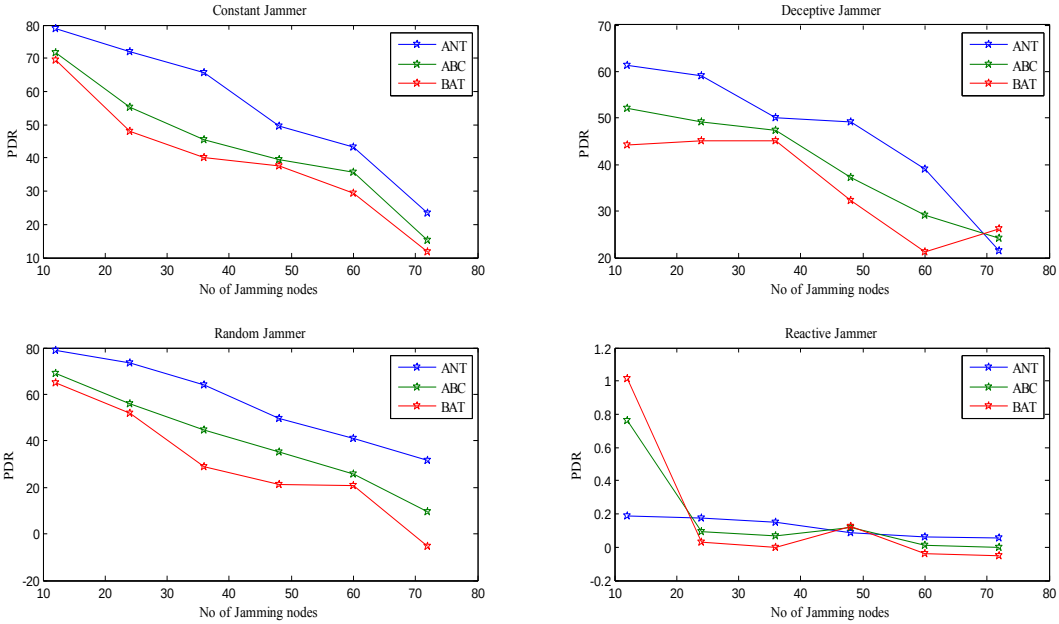

Figure 6: Comparison of BAT with Ant & ABC System by means of Packet Delivery Ratio

Conclusion

This paper proposes a novel method to detect jamming attack using BAT a meta-heuristic algorithm and compares its performance with ABC and ANT algorithms. The performance parameter such as energy, distance, packet loss, and packet delivery influences the decision taken in anti-jamming techniques. The formulation of DoS attack based on each layer can be combined to optimize the attacks by using a simple optimization algorithm. The proposed algorithms can separate network conditions caused by various types of jammers or caused by natural sources from each other along with high detection rate and low false positive rate. Another advantage is that no additional hardware is required to implement the algorithms on existing wireless sensor nodes. In future, the algorithms will be implemented on real wireless sensor nodes and, thus, the performance achievement of the algorithms in a real environment will be elaborated.

References

[1]. A. Mainwaring et al.," Wireless Sensor Networks for Habitat Monitoring", In Proceedings of the ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, USA, 2002, pp. 88–97

[2]. I.F Akyildiz et al., "Wireless sensor networks: A survey", Computer. Networks, 38, 2002, pp. 393–422.

[3]. D. L. Adamy and D. Adamy, "EW 102: A Second Course in Electronic Warfare", Artech House Publishers, 2004.

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

[5]. 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.

[6]. W. Xu et al., "The feasibility of launching and detecting jamming attacks in wireless networks", In Proceedings of the Sixth ACM International Symposium on Mobile ad hoc Networking and Computing, Alexandria, VA, USA, 2005, pp. 46-57.

[7]. M. Li, I. Koutsopoulos, and R. Poovendran., "Optimal jamming attacks and network defense policies in wireless sensor networks", In IEEE International Conference on Computer Communications (INFOCOM), May 2007, pp. 1307–1315.

[8]. A. Wood, J. Stankovic, and S. Son., "JAM: A jammed-area mapping service for sensor networks", In Proceedings of IEEE Real-Time Systems Symposium, 2003, pp.286–297.

[9]. W. Xu, W. Trappe, and Y. Zhang., "Anti-jamming timing channels for wireless networks", In WiSec '08: Proceedings of the first ACM conference on Wireless network security, 2008, pp. 203–213.

[10]. M. Cagalj, S. Capkun, and J.P. Hubaux., "Wormhole-based anti-jamming techniques in sensor networks", IEEE Transactions on Mobile Computing (TMC), 6, Jan 2007.

[11]. G. Alnie and R. Simon., "A multi-channel defense against jamming attacks in wireless sensor networks", In ACM International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, 2007, pp.95–104.

[12]. W. Xu, W. Trappe, Y. Zhang, and T. Wood., "The feasibility of launching and detecting jamming attacks in wireless networks", In Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2005.

[13]. M. Rajani and A.O Lisa, "Jamming attack detection and countermeasures in wireless sensor network using ant system", Available online: http://www.cognitiveintelligence.com/ documents /SPIE 2006.

[14]. Sudip Misra et al.,"Information Warfare-Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks Using a Fuzzy Inference System", Sensors, Vol.10, 2010, pp. 3444-3479.

[15]. Qiang Liu et al., "A Bio-inspired Jamming Detection and Restoration for WMNs: In View of Adaptive Immunology", Springer International Publishing Switzerland, 2013, pp. 243–257.

[16]. D.W Anthony et al., "DEEJAM: defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks", SECON 2007, San Diego, CA, USA, 2007.

[17]. M. Çakiroğ lu and A.T Özcerit,"Design and evaluation of a query-based jamming detection algorithm for wireless sensor networks", Turkey Journal Elec Eng & Comp Sci, Vol.19, No.1, 2011, pp. 1-19.

[18]. 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.

[19]. C. Perkins et al., "Ad hoc on-demand distance vector (AODV) routing", 2003.