Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System

Rajani Muraleedharan and Lisa Ann Osadciw
Department of Electrical Engineering and Computer Science
Syracuse University
Syracuse, NY 13244-1240
(315) 443-1319 (office)/(315) 443-2583 (fax)
rmuralee,laosadci@syr.edu

ABSTRACT

Sensors have varied constraints, which makes the network challenging for communicating with its peers. In this paper, an extension to the security of physical layer of a predictive sensor network model using the ant system is proposed. The Denial of Service (DoS) attack on sensor networks not only diminishes the network performance but also affects the reliability of the information making detection of a DoS threat is more crucial than recovering from the attack. Hence, in this paper, a novel approach in detecting the DoS attack is introduced and analyzed for a variety of scenarios. The DoS attack is dependent on the vulnerabilities in each layer, with the physical layer being the lowest layer and the first to be attacked by jammers. In this paper, the physical layer DoS attack is analyzed and a defense mechanism is proposed. Classification of the jammer under various attack scenarios is formulated to predict the genunity of the DoS attacks on the sensor nodes using receiver operating characteristics (ROC). This novel approach helps in achieving maximum reliability on DoS claims improving the Quality of Service (QoS) of WSN.

Keywords: Wireless Sensor Network, Security, Denial of Service(DoS), Jamming Attack, Detection Theory

1. INTRODUCTION

Sensor networks using distributed wireless technology are utilized in many applications, such as health monitoring system, building or infrastructure access systems, disaster relief and tsunami warning systems. Some of these applications lack security due to resource constraints, thus, resulting in reduced Quality of Service (QoS). In resource constrained network such as WSN, traditional security schemes cannot be applied. Hence, need for new security measures to maintain network functionality without sacrificing performance becomes a necessity. In this paper, different jamming attack on WSN is considered, and a defense mechanism is proposed.

In WSN, a multitude of wireless sensors are interconnected by means of RF communication links. The functionality of the nodes in this application include sensing, collecting and distributing dynamic information within the network. Energy usage is a key issue as the sensors are typically tiny and wireless with limited memory and functionality given the fact that the batteries(y) have a limited power supply. Hence, difficulties arise during computation[2]. A network or node can be affected by many kinds of DoS attacks including those, forcing nodes to be in idle or stand-by mode. This affects the performance of the node and the network. In worst cases, the attacked node continues to communicate to its neighbors and finally depletes all its power and declares itself dead, which reduces the networks coverage area. Hence, WSN need to be adaptable with minimal wait period (network set up need to be modified). The communication links in such an unpredictable environment (node failures) are kept functional by applying a robust routing algorithm. In this paper a novel approach is proposed. The agents use the sensor node's information to predict or anticipate jamming attacks by using key performance parameters.

One problem that all evolutionary algorithm suffer is finding a local solution instead of global. Optimality[3], finding the solution with the best performance, and reachability[3], the global optimal instead of local optimal, are two important factors in choosing an appropriate algorithm. The focus of this paper, is to detect a node under DoS attack and upon detection to re-direct the message to its appropriate destination node. In Section 2 justification for using an ant system and its impact on the sensor network is discussed. Section 3 discusses the different DoS attack in brief and a detail analysis on the different kinds of jammer attack. In Section 4 detection of the jammer attack using an ant system and its performance parameters is explained with mathematical illustrations and simulations described in Section 5 . The paper concludes with the Section 6 discussing the conclusion and future work.

2. SWARM INTELLIGENCE AND ANT SYSTEM

An algorithm is selected based on the design constraint and the performance expected from the application. As each approach possesses trade off, the main criteria in selecting an algorithm is the time and probability of obtaining an optimal solution. For example, an evolutionary algorithm may not always provide the global solution.

Swarm Intelligence, is an algorithm that models the collective behavior of social insects, namely the ants, bees, birds, slime mould, etc. Ant system is one such evolution from the swarm intelligence forming an evolutionary algorithm with unique characteristics such as robustness, distributed problem solving, versatility and de-centralization approach. The ant system solves any complex convex optimization problem. It also adapts to the network with environmental changes. The agents in the system communicate interactively either directly or indirectly in a distributed problem-solving manner. The agents move towards the optimal solution and communicate directly by sharing knowledge with their neighbors.

The initial set of agents traverse through the nodes in a random manner, and once they reach their destinations, they deposit pheromone on trails as a means of communicating indirectly with the other ants. The amount of pheromone left by the previous ant agents increases the probability that the same route is taken during the current iteration. Other performance factors discussed in Section 3 also affect the probability of selecting a specific path or solution. Pheromone evaporation over time plays an important role in preventing suboptimal solutions from dominating in the beginning.

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. Initially, the computational cost and time is high but this drops drastically once the agents learn the network and environment.

A Tabu-list serves as memory tool listing the set of nodes that a single ant agent has visited. The ant's goal is to visit nodes in the network depending on the number of hops assigned by the user. Thus traversing all the nodes and depleting all the energy at every node is avoided. In a given tour, a node is never re-visited. The pheromones on all the paths are updated at the end of a tour. The pheromone deposition, tabu-list, and energy monitoring help this novel ant system (AS) to obtain an optimal solution and adapt it as nodes degrade.

2.1 Mathematical Approach Of the Ant System

The sensor network in this paper is assumed to have no cluster heads. Thus the sensor nodes need no authorization to communicate with its peers. Eliminating cluster heads reduces the complex process of changing cluster heads as well as additional functionality such as fusing the different member messages at the cluster head. The performance of the AS is determined by the node spacing and 4 parameters: Q, , an arbitrary parameter, ρ , trail memory, α , power applied to the pheromones in probability function, and β , power of the distance in probability function. These AS parameters control the performance of the ant system on a specified set of nodes. 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 pheromone is initialized and assigned value of 10. The pheromone is updated following each complete tour by, (AS - see [4, 5, 6, 8])

$$\psi_{ij}(t) = \rho(\psi_{ij}(t-1)) + \frac{Q}{D_t \cdot E_t} \tag{1}$$

where D_t is the total distance travelled by ant agents during the current tour, i is the index for the source node with coordinates (X_i,Y_i), and j is the index for the destination node with coordinates (X_j,Y_j). The transition probability between nodes for a wireless network is computed from with its neighbors (agents) by means of pheromone deposition and tabu list using

$$.P_{ij} = \frac{(\Psi_{ij})^{\alpha} \cdot \left(\frac{1}{D_{ij}}\right)^{2\beta} \cdot (E_{ij})^{\alpha}}{\sum_k \left((\Psi_{ik})^{\alpha} \cdot \left(\frac{1}{D_{ik}}\right)^{2\beta} \cdot (E_{ik})^{\alpha}\right)} \tag{2}$$

The energy is dissipated from the sensor node after each ant passes through that node. Assumption is made that the wireless nodes consumes more energy than of a wired network. Thus the distance is squared and the energy dissipated for a wireless sensor node is given by,

$$\Delta E_{ij} = \frac{K}{(D_{ij})^2} \tag{3}$$

The link budget k, is calculated with respect to the bluetooth protocol (i.e., where P_{tx} is the transmitted power, G_{tx} and G_{rx} are the antenna transmit and receiver gain, L_{fs} is the propagation loss and P_{rx} is the receiver sensitivity**.** or

$$P_{tx} = P_{rx} - G_{tx} + L_{fs} + Fadem\arg in \ ) \tag{4}$$

The node's remaining energy is computed by

$$E_i(t) = E_i(t-1) - \sum_j \Delta E_{ij} \tag{5}$$

The agents avoid visiting nodes with depleted energy by determining alternative routes in the sensor network. Thus the network remains partially functional even if some of the individual sensors fail. The tabu list supports energy usage prediction and decisions concerning situation assessment. Transition probabilities assist in optimizing route selections. The above features of the ant system coupled with application-specific performance parameters enhances the predictive nature of sensor network as discussed in the future sections.

3. DENIAL OF SERVICE IN SENSOR NETWORK USING ANT SYSTEM

A Denial of Service (DoS) attack on a network is typically used by illegitimate users to reduce the capacity of the network. Similarly, when the sensor network is encountered by a Denial of Service (DoS) attack, it reduces both the functionality and the overall performance of the network. In crucial applications such as disaster relief, health monitoring etc., reduced performance due to DoS will only make the network unfit for the application. Hence, detecting DoS attacks and defending the network by taking the necessary countermeasures helps in maintaining or improving the performance of the application.

3.1 Previous Work - Denial Of Service

Interception or compromise of the secure information by an enemy is an act that cannot be neglected. Hence, appropriate security measures need to be taken at every layer of a protocol design. Many attacks are caused by intruders who have seldom or complete knowledge of the protocol. There has been research on the different kinds of possible DoS attacks on sensor network. Wood et al in [9] had summarized different DoS attack and its effect on the sensor network. Though no defense mechanism is proposed in this survey but different possibilities to reduce the attacks are given. In the physical layer, using spread spectrum is often used to reduce jammer attacks. This paper concludes that due to the limited resources code spread as used in mobile networks cannot be used in WSN.

In [13], mapping protocol for nodes that surround a jammer is proposed. Using this approach, the protocol creates awareness in the neighboring nodes to detect a jamming attack using message diffusion. Also, in this paper single-channel wireless communication is assumed. It is simulated using GloMoSim simulator with different range of jamming attack and neighboring nodes. The protocol was robust (message re-routed and only loses data in inactive nodes) to failure rates of 20-25% of mapping nodes from twelve neighboring nodes within communication range.

In [10], sybil attack on a network and routing layer of WSN is analyzed. Here it is assumed that a sensor node communicates with its neighbors using half-duplex and single radio with various channels. The process of identifying sybil attacks is based on radio resource testing. Legitimate neighboring nodes are allotted a single channel for identity. This process of identifying a sybil attack cannot function if the spectrum is jammed. Hence, would lead to a false identification of a sybil attack.

In [11], routing security in sensor network is analyzed and a countermeasure is proposed. Defense mechanism for different DoS attacks such as spoofing, wormhole, sybil, selective forwarding etc., is given based on the assumption that using radio frequencies alterations can be made to the data. Radio jamming using traditional methods in military environments is summarized in [12].

In most of the previous work in DoS attack the transmission is either assumed secure or intruded only for injecting wrong data. One of the major disadvantage of any network is becoming non functional or unable to communicate. This is the most adverse attack a sensor network can encounter. This attack can account towards node's inability to communicate inspite of enough resources. In this paper, an evolutionary algorithm helps in maintaining the performance of the network by finding an alternative solution when a node is jammed by an intruder.

3.2 DoS attack on Physical Layer

Figure 1 gives a pictorial idea of the different types of attack that occur in every sensor network layer[9]. The blocks that are shaded in stripes can be eliminated, as it primarily depends on the kind of protocol that is used for sensor network. The hypothesis formulated in this paper can be extended to other layers too, which helps in optimizing cross-layer Denial of Service attack[16]. Depending on the modulation scheme opted for the physical layer, jamming the node from its peers varies.

For example, in [17] the modulation scheme for sensor network uses adaptive modulation technique in a rayleigh fading channel. Thus jamming this network that uses DS/FH spread spectrum is not trivial. The characteristics of different types of jammer has varied effects on the network performance, which is discussed in the following section.

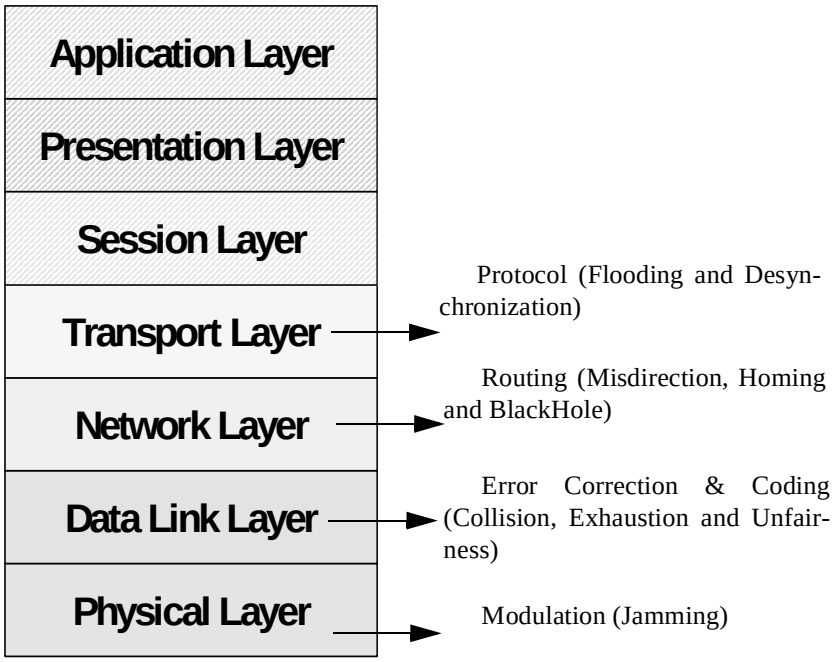

Fig. 1.Denial of Service Attack on Sensor Network Layer

4. JAMMER ATTACKS AND ITS CHARACTERISTICS

A jammer is a device which can partially or entirely disrupt a node's signal, by increasing its power spectral density (PSD). Jammer can never re-produce a signal nor can it pretend like a receiver node. The parameters such as signal strength of a jammer, the location and the type influences the performance of the network and each jammer has different effect on the node.

The application of spread spectrum (SS) techniques developed by the end of World War II. Using SS technique the data is spread across the frequency spectrum making the signal resilient to jamming, noise and eavesdropping. There are different types of SS such as Direct Sequence (DS), Frequency hopping (FH), Time hopping (TH) and hybrid. There are both advantages and disadvantages associated with using SS in sensor networks. The advantages are 1. Ability to alleviate multi-path interference, 2. Jamming attacks reduced, and 3. Less power spectral density. The disadvantages are, 1. Bandwidth inefficiency, 2. Comples implementation, and 3. Computational cost.

Bluetooth[22] uses FHSS, which consumes more power as frequency hops needs to be synchronized. Whereas, Zigbee[23] uses IEEE802.15.4 standard where DSSS with CSMA-CA is used. Of late Zigbee is being considered as a wireless technology for wireless sensor networks as it consumes less power.

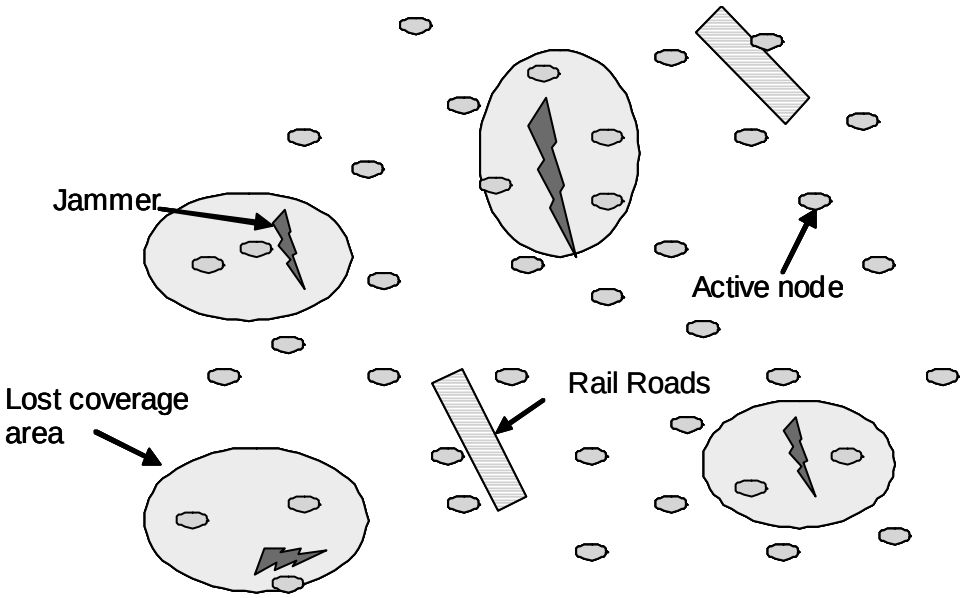

Fig. 2.Jammer Attack on Sensor Network

Figure 3 pictorially describes the jammer attack on sensor network. The network is not only disrupted by adversary attacks but also the environment. Differentiating the attack from nature needs knowledge of the various attacks that can be caused by an illegitimate user. Since an attack can completely eliminate a coverage area, and in applications where network cannot be immediately updated, the network performance will be poor. Hence, study of different characteristics of an attack keeps the attack attempts minimal as knowledge of the types of jammer helps in taking the appropriate countermeasure. In this paper, its assumed that there are four different types of jammer[18], namely: single-tone jammer, multiple tone jammer, pulsed-noise jammer and ELINT.

4.1 Single-Tone Jammer[19]

A single-tone jammer's frequency lies within the specified bandwidth of the signal being jammed. It targets any narrowband communication. Since traditional wireless sensor network use narrowband technology[20]. This kind of jammer tries to continuously jam the node within specified bandwidth, which might result in a dead link and diminishes the node's coverage.

4.2 Multiple-Tone Jammer

A jammer that can disrupt the signal of some or entire channel of a multiple channel receiver. This type of jamming leads to a complete node failure, if the entire channel is compromised. The only time the node can recover is when the jammer is turned off. Typically, an intruder plays it safe while jamming a node by occasionally turning off its radio. Thus, make the neighboring node assume the node is not under attack but rather lost its energy and needs recuperation. Hence, detections of a jammed node is very important.

4.3 Pulsed-Noise Jammer [19]

A pulsed-noise jammer is a wideband jamming, which behaves like a pulsed signal by turning on and off perodically. The primary goal of this jammer, is to disrupt the spread spectrum communication by spreading the peak jamming power during the "on" time. Two types of pulsed-noise jammers are considered, namely, slowly switching and fast switching jammers.

4.4 ELINT

ELINT is typically a passive system that tries to break down or analyze radar or communicatin TCF signals. They may be integrated. In the following section, mathematical formulation based on the different types of jamming is described with simulations.

5. DETAILED APPROACH - MATHEMATICAL FORMULATION

The sensor network is built based on the following assumptions, such as, (1) All nodes are initialized with varied energy level, thus giving each different capacity to transmit messages (2) Each node has varied threshold, therefore the probability of all node 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 is set for every packet loss and successful packet delivery, beyond which, a node is penalized for it's behavior and (6) Sensor mobility is not considered, the links are heterogeneous, i.e., wireless or wired. The probabilistic approach of the ant system depends on the energy depletion and the percentage of false decision. The two factors need to be minimal.

The IEEE 802.11b standard has a Clear Channel Assessment (CCA) in DSSS protocol which checks whether WLAN channel is free for transmitting. Using the same protocol in IEEE 802.14.5 will only jeopardize the performance of the network. Hence detection of any attack is important while trying to secure the link from intruders. Hence a hypothesis is formulated that helps in detecting whether the DoS claim is authentic.

The jamming attack can be classified into four possible decisions namely,

1. Sensor out of resources - is accepted,
2. Sensor encounters a resource outage but falsely calls it a Jammer attack,
3. DoS-Jammer attack is accepted. and
4. DoS-Jammer attack is rejected and claimed as resource outage.

The accuracy of the decision is specified in terms of the rate with which the system makes decision 2 and 3, which are erroneous. The error described in 2 is referred to as False Rejection Rate (FRR). The error in 3 is the False Acceptance Rate (FAR). Genuine acceptance rate (GAR) is one other performance measure, where GAR = 1-FAR. These quantities are specified in terms of conditional probabilities. In detection theory[25], FAR, FRR and GAR are commonly known as the false alarm rate, miss rate and detection rate.

The problem of Denial of Service using 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. This will be further explored in future work, the sensor nodes under different jamming attack and the countermeasure is analyzed in this paper.

Figure 3 provides a pictorial description of the algorithm used in sensor network. The network layer is given as input to the algorithm, the location of the sensor and initial parameters for the ant system. The number of agents is proportional to the number of sensors in the network. The ant agents are randomly placed on the sensors; not all sensor nodes are assigned an agent.

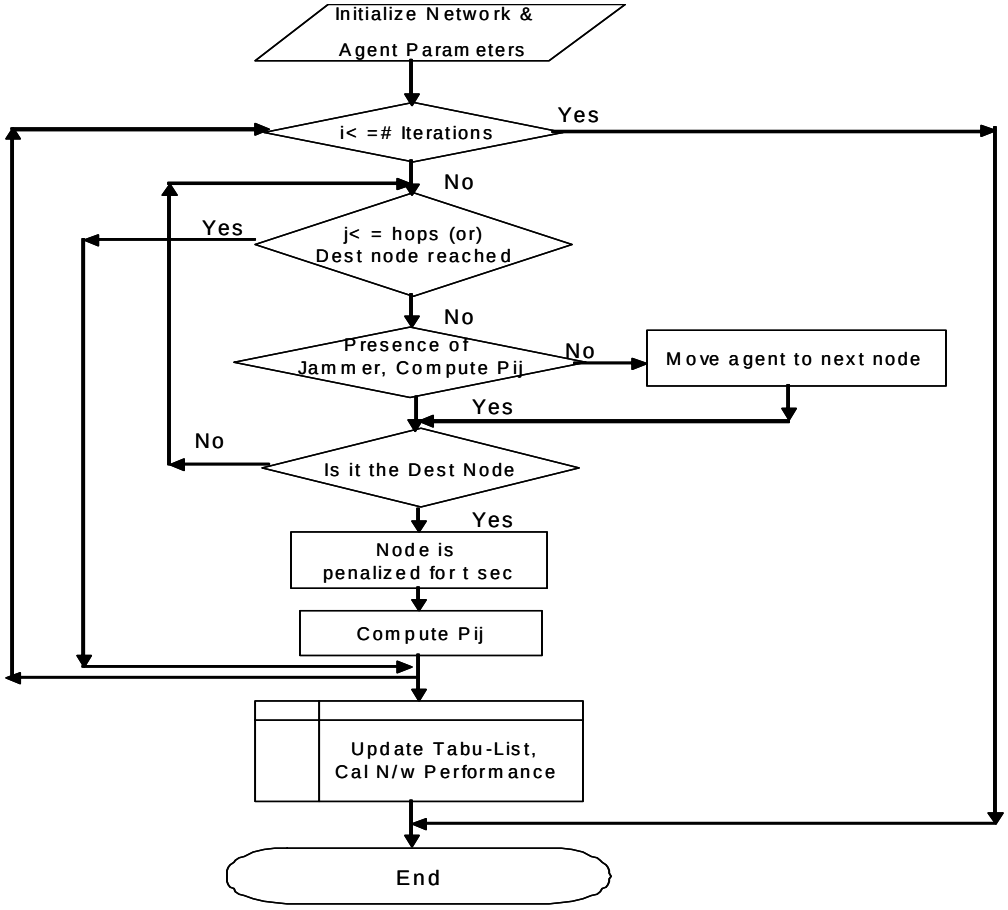

Fig. 3.Flowchart - Predictive Sensor Network

As discussed in the second section, 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 affects the movement of the ant agent in the network. Link factor is incorporated into the ant system. The transition probability is given as

$$P_{ij} = \frac{(\psi_{ij})^{\alpha} \cdot (\eta_{ij})^{\alpha} \cdot \left(\frac{1}{D_{ij}}\right)^{2\beta}}{\sum_{k} (\psi_{ik})^{\alpha} \cdot (\eta_{ik})^{\alpha} \cdot \left(\frac{1}{D_{ik}}\right)^{2\beta}} \tag{6}$$

where η_{ij} is the 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 [7].

$$\eta_{ij} = H_{ij} \cdot E_{ij} \cdot B_{ij} \cdot SNR_{ij} \cdot Pd_{ij} \cdot Pl_{ij}$$

(7)

The normalized value is given by the difference between total and actual value of the performance parameters, which helps in either minimizing or maximizing the output. This performance value helps in computing the transition probabilities in a route while traversing the data set formed by the agents. The link being active or dead in a tour taken by an agent is incorporated in the pheromone (8). Thus the trails formed by the ant agent is now dependent on the link factor. The pheromone deposition is defined as

$$\psi_{ij}(t) = \rho(\psi_{ij}(t-1)) + \frac{Q}{D_t \cdot \eta_t} \tag{8}$$

The tabu list now consists of updated values of the energy available in the nodes for the particular sub-optimal route with high reachability.

5.1 Result

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 table below illustrates scenarios using different types of jammer and the effectiveness of evolutionary algorithm in assessing the performance of the network. The proposed detection and defense mechanism is simulated using Matlab 6.5 and Simulink R14. The performance of the network can be evaluated based on varied Jamming to signal ratio (J/S), energy to jamming density ratio, energy to noise density ratio, multi-path interference,

The parameters of ant system are assumed to be a = 4, b = 7, r= .7, Q = 9 and initial pheromone value, y as 10. The number of agents employed in the network is 16, and the source and destination nodes were assumed constant. The stability of the algorithm is analyzed by iterating all scenarios for 100 runs. The actual hops is user defined which varies depending on the problem assigned. The normalized value of hops is given as $Hops_{Norm}$. The predicted energy and distance helps in making a decision whether the nodes in the current route is still capable of communicating with its peers in the next iteration.

Table 1 shows the performance of the sensor network where single tone jammer is applied. Initially, the number of jammed node in a period t seconds is 3. Hence, the number of nodes jammed is 3 out of 16 in the network. Similarly in each case nodes are jammed for t seconds. Since single tone jammer affects only one carrier, and the modulation used here is DS/FH, therefore the probability of finding the PN sequence by the jammer is low. The performance of the network, based on the distance, energy depleted, percentage of packet loss and packet delivery for the worst case, when 12 nodes is 92.373, 50.0292, 0.3792 and 78.7423. Only 78% message delivery is due to the fact that in some of the iteration its the destination node, which was jammed and hence it triggered increased packet loss rate.

Table 1. Performance of Sensor Network -Single Tone Jammer

# node jammed	Average Distance	Average Energy	Average Packet Loss	Average Packet Delivery
3	9.756	15.2038	0.038	97.349
6	24.205	23.3931	0.095	95.2798
9	35.3302	30.4269	0.3257	69.3568
12	92.373	50.0292	0.3792	78.7423

Table 2 shows the performance of the network when multiple tone jammer is applied. In this type of jammer, all the carrier is jammed in a single node if its under attack. The node recovers from the attack only after t seconds, so the chances of assuming the node has depleted its energy is a possibility. Since, ant agents uses memory tool the jamming attack can be differentiated with sensor energy depletion. Tracking SNR and energy conserved from previous routes,

helps in detecting jamming attack. The number of node attacked by multiple tone jammer is 9 but the average distance taken is only 20.203 with energy depletion of 42.482.

Table 2. Performance of Sensor Network -Multiple Tone Jammer

# node jammed	Average Distance	Average Energy	Average Packet Loss	Average Packet Delivery
3	4.937	3.329	0.013	99.230
6	5.920	7.2372	0.021	98.410
9	20.203	42.482	0.105	92.938
12	94.297	97.392	0.4128	60.239

In Table 3 performance of the network when attacked by pulsed-noise jammer is shown. In this case, the number of nodes under attack did not affect the network's performance. As the duty cycle of this jammer increases it's signal strength only during the "on" duration. Since the DS/FH modulation rarely falls in the duty cycle, even when 12 nodes where under attack the network performance was fairly good as the average packet loss is 0.1307 with energy depletion of only 31.92. As shown, the pulsed-noise jammer does not influence the performance of the network.

Table 3. Performance of Sensor Network -Pulsed-Noise Jammer

# node jammed	Average Distance	Average Energy	Average Packet Loss	Average Packet Delivery
3	1.202	0.2569	0.0023	99.008
6	2.45	1.3981	0.0015	99.129
9	8.2093	7.4903	0.0293	98.2108
12	28.2928	31.920	0.1307	78.9812

Table 4 shows the network performance when ELINT jamming attacks the sensor network. Since ELINT can disrupt the network based on the node's signal detection. This type of jammer affects the network performance very poorly. When 12 nodes are attacked by ELINT jammer, the packet loss is 92% whereas the successful packet delivery is a low value of 0.34% when compared to the other jammers.

Table 4. Performance of Sensor Network -ELINT Jammer

# node jammed	Average Distance	Average Energy	Average Packet Loss	Average Packet Delivery
3	10.2921	20.948	0.173	82.1823
6	17.185	40.0862	0.298	73.976
9	40.4931	59.3495	0.5529	40.209
12	70.0383	90.893	0.9236	0.0034

The influence of a jammer attack is primarily based on the type of jammer, which can be avoided by knowing the characteristic and by predicting the attack.

6. Conclusion and Future work

This paper proposed a novel method of avoiding sensor network under jamming attack by using evolutionary algorithm, the ant system. The performance parameters such as hops, energy, distance, packet loss, SNR, BER and packet delivery influences the decision taken in anti-jamming techniques. The network under 75% ELINT jammer attack is shown to be functional indicating the robustness of the Ant system. The four scenarios presented in the result section re-emphasize the fact that a sensor network remains functional and assesses the situation under all critical conditions.

The sensor network considered in this paper is made simple with 16 nodes and ant agents. In future work, the data collected by the sensor nodes is made as a dataset from which both an assessment and suggesting a plan based on the situation could be predicted. Predicting the jammer attack such as ELINT could increase the network performance by decreasing the packet loss. The formulation of DoS attack based on each layer can be combined to optimize the attacks by using a simple optimization algorithm. A sensor network with predictive nature could be applied to many applications where decision plays an important role such as medical controller, military applications, traffic monitoring and others.

References

1. Kennedy J, Shi Y. and Eberhart R.C., " Swarm Intelligence " , Morgan Kaufmann Publishers, San Francisco, 2001.

2. Rajani Muraleedharan and Lisa Ann Osadciw, " Balancing The Performance of a Sensor Network Using an Ant System ", 37th Annual Conference on Information Sciences and Systems, John Hopkins Unversity, 2003.

3. Rajani Muraleedharan and Lisa Osadciw, "Sensor Communication Networks Using Swarming Intelligence", IEEE Upstate New York Networking Workshop, Syracuse University, Syracuse, NY, October 10, 2003.

4. Luca Maria Gambardella and Marco Dorigo, " Solving Symmetric and Assymetric TSPs by Ant Colonies", IEEE Conference on Evolutinary Computation(ICEC'96), May20-22,1996, Nagoya, Japan.

5. Marco Doringo, "The Ant System: Optimization by a Colony of Cooperating Agents", IEEE Transactions on Systems, Man and Cybernetics-Part B, Vol-26, No. 1, Sept1996, pp 1-13.

6. Dorigo and L.M. Gambardella, " Ant colony system: a co operative learning approach to the travelling salesman problem" , IEEE Transations on Evolutionary Computation, Vol 1, no.1, 1997, pp.53-66, JOURNAL.

7. Yun-Chia Liang and Alice E. Smith, " An Ant system approach to redundancy allocation," Proceedings of the 1999 Congress on Evolutionary Computation, Washington D.C., IEEE, 1999, 1478-1484.8]

8. H. Van Dyke Parunak, Sven Brueckner, " Ant like Missionaries and Cannibals : Synthetic Pheromones for Distributed Motion Control ", Proc of the 4th International Conference on Autonomous Agents(Agents 2000), pp. 467-474.

9. A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks", IEEE Computer, Vol 35, Issue: 10, Oct 2002.

10. J. Newsome, E. Shi, D. Song and A.Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses", Third International Symposium on Information Processing in Sensor Networks (IPSN), 2004.

11. C. Karlof and D.Wagner, “Secure Routing in Sensor Networks: Attacks and Countermeasures“, First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

12. R. Anderson, “ Security Engineering: A Guide to Building Dependable Distributed Systems”, pages 326{331. Wiley Computer Publishing, 2001.

13. A.D. Wood, J.A. Stankovic and S.H. Son “JAM: A Jammed-Area Mapping Service for Sensor Networks“, In Real-Time Systems Symposium (RTSS), Cancun, Mexico, 2003.

14. Bernard Sklar, “Digital Communications: Fundamentals and Applications“, Chapter 12. Spread Spectrum Techniques, Englewood Cliffs, NJ: Prentice Hall, 1988.

15. Lisa Ann Osadciw and John F. Slocum “Clutter Processing Using K-Distribution for Digital Radars with Increased Senstivity“, International Radar Conference. 2002.

16. Rajani Muraleedharan and Lisa Ann Osadciw, “Cross Layer Denial of Service attacks in Wireless Sensor Network Using Swarm Intelligence “, 40th Annual Conference on Information Sciences and Systems, Princeton University, 2006.

17. Rajani Muraleedharan and Lisa Ann Osadciw, “Robustness of Predictive Sensor Routing in Fading Channels “, In Proc of SPIE Defense and Security Symposium, Orlando, 2005

18. Poisel Richard, “Modern communications jamming principles and techniques“.

19. F.C.M. Lau and C.K. Tse, " Study of Anti-Jamming Capabilities of Chaotic Digital Communication Systems," Proceedings, 2002 International Symposium on Nonlinear Theory and Its Applications, (NOLTA'2002), October 2002, Xian, China, pp.65-68.

20. K.D.Wong, “Physical Layer considerations for Wireless Sensor Networks“, IEEE Int’l Conference Net, Sensing and Control, Mar 2004, pp 1201-1206.

21. Bernard Sklar, “Digital Communications: Fundamentals and Applications“, Chapter 12. Spread Spectrum Techniques, Englewood Cliffs, NJ: Prentice Hall, 1988.

22. Technical Information of Bluetooth: Official website www.bluetooth.com.

23. Technical Information of Zigbee: official website www.zigbee.org

24. Don J. Torrieri, “Principles of Secure Communication Systems“, Artech House, Boston, London, 1992.

25. Steven M. Kay, “Fundamentals of Statistical Signal Processing: Detection Thory“, Vol II, Prentice-Hall Inc, 1998