Cross Layer Security Protocol Using Swarm Intelligence

Rajani Muraleedharan and Dr. Lisa Ann Osadciw

Department of Electrical Engineering and Computer Science

Syracuse University, Syracuse, NY- 13244-1240

Phone: 315-443-3366/Fax: 315-443-2583

rmuralee/laosadci@syr.edu

Abstract - **Security and privacy plays a vital role in wireless applications such as health monitoring, military and biometric identification systems. Due to the limited resource constraints in wireless sensor network, security in protocols is sacrificed or kept minimal. In this paper, a cross layer protocol is designed to detect denial of service attack imposed on the network by malicious nodes. The Denial of Service attack on sensor networks not only diminishes the network performance but also affects the reliability of the information. Swarm intelligence, an evolutionary algorithm is used in predicting the traffic patterns and detecting malicious nodes. This novel approach helps in keeping the network functional and self sustaining by re-routing the information. The sybil, worm-hole and jamming attacks are overcome using this protocol design with minimal resource exploitation. The performance of the network is evaluated based on the successful packet delivery, energy consumption and average percentage of threat detection.**

Index Terms: Wireless Sensor Networks, Swarm Intelligence, Denial of Service attack,

I. INTRODUCTION

The wireless sensor nodes are made of low power electronic devices deployed in remote area, where battery cannot be recharged. The power scavenging schemes would only increase the complexity of the network, hence efficient usage of energy becomes a priority. Recently, the demand of WSN is extended to many real world applications such as health monitoring, emergency evacuations security, soldiers in battlefield, biometric application in airport, etc.,

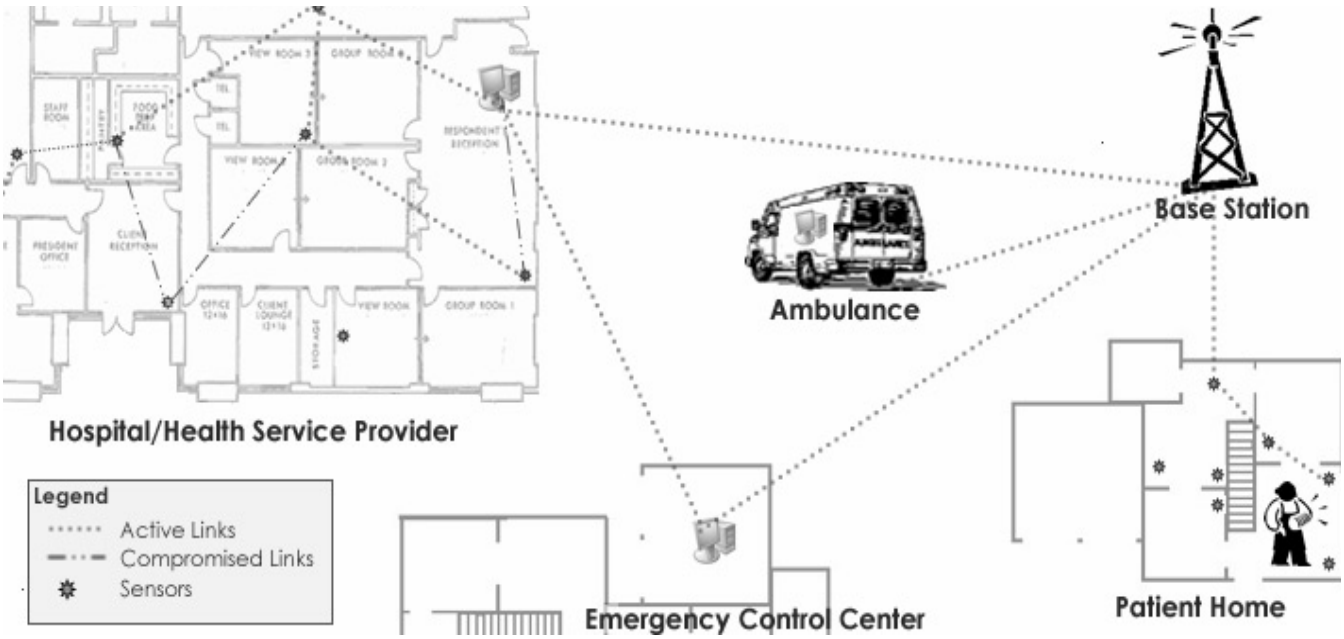

Fig. 1.Smart Home Environment Using Swarm Intelligence

where image co-efficients need to be communicated to the sink and security becomes a necessity. Since WSN are susceptible to DoS attacks, securing the links is an primary task in designing a sensor network.

Figure1 illustrates a smart tele-health environment. The nodes are spread in three forms, wired, wireless and mobile forming a heterogeneous network. A wireless node is embedded on a patient to monitor his/her biological readings. Another set of mobile nodes are placed on ambulances, where the vehicles can either receive or send data to the nearest hospital or patient. The wired and wireless nodes are placed in the hospital where continued monitoring of outgoing and incoming patients with added functionality such as security of the building is also maintained. The dash lines show the communication between the active nodes in the network. The dash-dot lines show the compromised nodes, the route taken is bi-directional and thus it excludes the compromised links making the route robust to any malicious attack.

The primary functionality of a sensor node is to sense, collect and communicate the message to its neighboring (relay) nodes in the network. The limited resource constraints of multi-hop sensor nodes prohibit traditional security schemes. Other factors, such as computation time and communication delays should be minimized to increase response time of the system and maintain network performance.

Hence, the primary goal of this paper is to find an optimal route to avoid nodes under DoS attack, which is performed by first finding if the DoS claim is genuine, next to find routes with increased QoS. Section III describes the importance of detecting the DoS attacks and Section IV gives an detailed analysis of the previous research work in this area. Section IV defines the problem statement and the restricted network functionalities. The evolutionary algorithm and its unique characteristics with mathematical illustrations is explained in Section V and Section VI. The simulation results is given in Section VII which provides evidence on the performance of the system. The conclusion and future work is given in Section VIII.

II. Denial Of Service Attacks

The impact of a single DoS attack is phenomenal, neglecting a single attack could compromise the entire network and applications relying on it. Hence combining different DoS attack into a single optimization problem will reduce attacks on the network.

The different DoS attack addressed in this paper are Jamming, Collision, Exhaustion, Misdirection, Sybil and Worm-Hole attacks. Jamming attack occurs in the physical layer of the network. This attack disrupts any communication from the attacked node. It is one of the most crucial attack, as it blocks all communications in such a way that the node is put to sleep mode thus denying it from its functionality. The effects of a jamming attack depends on the type, location and noise power of the jammer.

The collision attack takes place in the data link layer, where the probability of losing packets are very high affecting the reliability of the application. In addition, exhaustion incinerates the resource availability at the node making it cumbersome for future communication.

In the network layer, depending on the routing protocol used misdirection occurs, which re-directs the message to an illegitimate node upon false broadcasting of its resource availability. Whereas, in a Sybil attack[5] an illegitimate node presents multiple identity thus deceiving its neighboring nodes. In a worm-hole attack, the packets are tunneled to another location and re-sent to bombard the network with communication overhead, thus reducing the QoS. The above attacks primarily depend on the layer, incorporating performance parameters that contribute toward increasing the QoS in a network are used to obtain an optimal and secure route. Cross-layer security issues could be minimized using the ant system (AS) algorithm.

In the design phase of a sensor node, security in protocols is sacrificed or kept minimal. Hence a trade-off between security and resource constraints still remains a dilemma to researchers. The Denial of Service (DoS) attack on sensor network not only diminishes the network performance but also reliability of the information is lost. As security could possibly be ignored in any or every layer, there are different types of DoS attacks that can occur. For e.g., in routing and network layer, due to “misdirection” attack the messages are flooded over the network. This information could also happen by looking at the routing table or negative advertising by the adversary to flood either sender, receiver or any arbitrary node.

III. Previous Work

Wood et al in [2] has summarized different DoS attack and its effect on the sensor network. The attacks in each layer is listed in a tabular format while emphasizing the importance of security features in sensor nodes. In [secure countermeasures] two new attacks sinkhole and Hello flood are proposed and link layer encryption and authentication as the possible solution to protect nodes against these attacks. Sleep deprivation attack is proposed by T.Martin et al in [4] for battery powered mobile computers. The nodes are deprived of communicating with its neighbors using three types of power draining attacks. The defense mechanism employed against such attack is multilevel authentication and energy signatures.

In [7] mapping protocol for nodes that surrounds 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 to failure rates of 20-25% of mapping nodes from twelve neighboring nodes within communication range.

In [3] sybil attack on 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. The other approach used is key distribution which seem to be a better option of detecting sybil attacked node.

In [5] 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. To avoid radio jamming using traditional methods in military environments is summarized in [6]. In most of the previous work in DoS attack the radio transmission is either assumed secure or intruded only for injecting wrong data. One of the major disadvantage of any network is being 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.

IV. Problem Statement

Sensor network distributes dynamic information, consisting of a multitude RF links and sensor nodes, which include sense and collect this information. The wireless sensor network is limited to power, bandwidth and memory, hence applying complex and traditional security schemes would decrease the lifetime of the sensor node. Time constraint in the system's response plays an major role in choosing an algorithm which best suits the application.

There are basic assumptions made in the datalink layer of a sensor network. First, not all the nodes are compromised by a 'sybil' attack i.e., k nodes compromised out of N sensor nodes. Second, the communication between the nodes is full duplex and uses hand shake as a means of confirming the delivery of messages to the destination node. Third, a trade-off between resource availability and DoS attack needs to be considered during communication. Fourth, there are four different types of jammer[24], namely: single-tone jammer, multiple tone jammer, pulsed-noise jammer and ELINT. Fifth, the whole spectrum is not affected by the jammer attack at the physical layer. Sixth, the sensor nodes are tamper resistant, though not acceptable in reality.

The dilemma is to agree whether a node is attacked or has exhausted its resource during communication. Process of authenticating the DoS attack claim helps the node to identify if the neighboring node is malicious and is injecting wrong claims. This kind of wrong claims could lead to misdirection of message route or selective forwarding attack. When a neighboring/ targeted node is compromised by a malicious node, any information stored can also be obtained by the attacker.

V. Swarm Intelligence & Optimization

Selecting a path that satisfies multiple QoS constraint is Nondeterministic Polynomial (NP) Complete problem, on the other hand, optimizing load balancing based on resource priorities is a Nondeterministic Polynomial (NP) hard problem. Ant system[17] is best suited for solving this problem to obtain an optimal, reliable and efficient path among all feasible paths.

Conventional wireless network algorithm used for internet cannot be applied to WSN due to its resource constraints. In this paper, load balancing[16], energy efficiency and maintain QoS traffic are prioritized by using Partially ordered sets (POSets). The Ant system is a learning algorithm which compares local with global optimization information giving it robustness and versatility to solve NP hard problems[9].

Sensor nodes are deployed in a random manner over the area of interest. Self-organizing techniques are applied in a sensor network to suit remote deployment. The ant agents are randomly placed along the network. The agents communicate with its neighbors to attain an optimal solution using the current status of the node and information gained through previous routes. The decision on validity of the route is obtained from pheromone deposition by the agents accumulated over time. The type of modulation scheme, coding scheme, queuing delay, number of re-transmissions, QoS issues impact the energy exploited for communication. Measures to reduce the amount of time taken for recovering from any data loss or re-routing information during link failure is a tedious task.

Unlike other routing algorithms, swarm agents react immediately upon sensing changes in the environment. This feature of the swarm agents truly make it an cognitive algorithm. The only data lost is the one that was prepared by the most recently visited node. Using the updated link status and the performance parameters, the agents exert a random movement towards its destination. Hence the probability of tampering the data packet depending on the route taken is very less unless the node itself is compromised.

VI. Mathematical Approach

In smart network, the agents are spread at random to speed up the search process. Monte Carlo simulations were performed for sensor node scattered across a 2D space with euclidean distance D_{ij}. In this paper, load balancing, energy

efficiency and maintain QoS traffic are prioritized by using Partially ordered sets (POSets). The Ant system is a learning algorithm which compares local with global optimization information giving it robustness and versatility. Self-organizing techniques are applied in a sensor network to suit remote deployment.

The performance parameters (between source i and destination j), such as Packet loss P_l, successful packet delivery to destination P_d, Signal to Noise Ratio (SNR), Bit Error Rate (BER), Number of hops H, Energy consumption E and the Distance D, are influenced by the DoS attack. These parameters will primarily decide if a route is efficient and reliable for secure transmission of messages.

(1)

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

Distance travelled by the agents is one of the critical parameter's that needs to be considered while depositing the trails. The pheromone is updated upon completing a tour by every agent and is given by

(2)

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

where D_t and is the total distance and total performance of the current agent in a tour, respectively. Q is an arbitrary parameter, controls the memory.

Partially ordered sets (POSets) has been used in queuing theory, networking, and lately sensor management [20, 21] . POSets provides a graphical mathematical framework for representing relationships between a finite number of elements. In the last 3 decades, POSets have been applied in a variety of computer science, engineering, and social science areas [22]. POSets began in the early nineteenth century with De Morgan.

POSets formulate weights at each graphical level to flow down the importance of a communication goal to the performance parameter measuring the success of achieving that goal. The POSet provides a weighting scheme to guide the creation of a single global performance parameter so that sensor parameter decisions can be made by the sensor manager agents. For example, distance and the number of hops need to be emphasized if the sensor network needs to quickly send messages if intruders are expected. Saving energy to prolong the life of the sensors is less important at that particular point in the system's lifetime. The weights[19] are then computed from

.

(3)

$$W_k = Y_i y_k, k = 1, 2, 3, i = 1, 2$$

The total performance is recomputed by

(4)

$$P_{global} = \sum_{i=1}^{N} W_i \left[\frac{\left(\psi_{actual_i} - \psi_{required_i} \right)}{\psi_{required_i}} \right]$$

where are global performance parameters (hops, distance, and energy) and W_i is the weighting from the POSets structure in (4). The operator may make new decisions at this point as to the weighting applied in the POSet.

Another key factor involved is the energy, which is weighted in the global performance. Using pheromones in (5), the transition probability is calculated from

(5)

$$P_{xy} = \frac{(\Psi_{xy})^{\alpha} \cdot (\eta_{xy})^{\beta}}{\sum_k (\Psi_{xk})^{\alpha} \cdot (\eta_{xk})^{\beta}}$$

where Q is an arbitrary parameter, ρ controls the memory, α is the power and weights the pheromone in probability function versus the global performance, β is the power applied to the global performance in the probability function and η is the global performance from the swarm agents.

Unlike other routing algorithms, swarm agents react immediately upon sensing changes in the environment. This feature of the swarm agents truly make it an cognitive algorithm. The only data lost is the one that was prepared by the most recently visited node. Using the updated link status and the performance parameters, the agents exert a random movement towards its destination. Hence the probability of tampering the data packet depending on the route taken is very less unless the node itself is compromised. Measures to reduce the amount of time taken for recovering from any data loss or re-routing information during link failure is a tedious task.

VII. Simulation

A sensor network with 25 sensor nodes with 6 nodes influenced by DoS attack is considered in scenario I. Under a sybil attack, the node (1,2) pretends dual personality as (2,1) and (3,4) with some mobility. In the first route the SI algorithm is tricked in believing that (1,2) is a reliable node since there is a communication delay in detecting the DoS attack. Whereas in the next subplot the algorithm responds immediately to the attack and excludes the compromised node from its route. Thus maintaing the efficiency of the network. Since the algorithm uses Posets, which helps in weighing the parameters. The packet delivery has a direct impact in indentifying if the node is under worm-hole attack, ie., if any node shows a good energy level and attracts its neighboring nodes to send more package to itself. By using the negative packet

delivery weight the malicious node can be removed from the route.

In case of a sybil attack, distance approximation[23] and energy depletion are tracked. When a node communicates it burns energy and using this concept the attack is detected. The routing table, that is stored temporarily, is used by the ant agent to track nodes that emit energy. If a sybil node assumes multiple identities though it does not appear in the route it can be easily identified to have high energy depletion at the end of the route. Upon identification the malicious node will be ignored for the future routes.

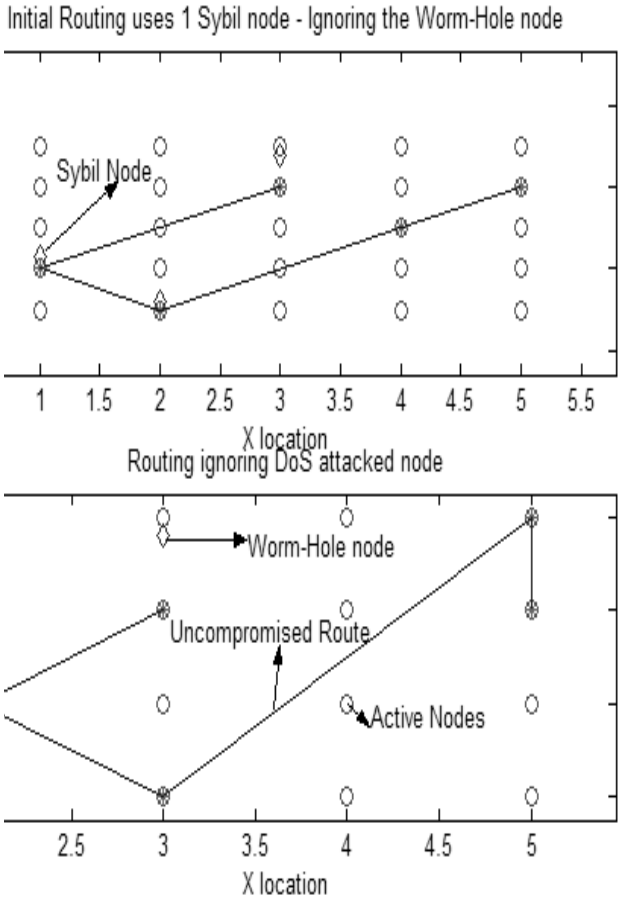

Fig. 2. Routing using Swarm Intelligence under DoS attack

In scenario II, a network with 16 sensor nodes with 6 nodes influenced by DoS attack is considered in this simulation. ELINT is typically a passive system that tries to break down or analyze radar signals. The results in Table I show the average performance of the AS with 2.9% packet-loss and 40% energy consumption under ELINT attack. These simulations were performed based on reduced learning rate of the AS. Weights on parameters need to be balanced based on the application's performance criteria. [23]

TABLE I. PERFORMANCE OF CROSS LAYER PROTOCOL: DOS ATTACK

Attacks	Average Packet Loss	Average Packet Delivery	Average Energy
ELINT [24]	0.0298	73.976	40.0862
Collision	0.0010	89.5713	16.7913
Sybil [23]	0.0087	80.7951	46.8922
Worm-Hole	0.0682	94.004	29.7067

VIII. CONCLUSION AND FUTURE WORK

In this paper, the worm hole, sybil and jamming attacks were analyzed using swarm intelligence algorithm. The performance of a system can be improved by adding an inference algorithm such as Bayesian Network (BN). The scenarios simulated above where assumed to have either affected by sybil or worm hole attack, in the future a combination of attacks will be imposed on the application. Since the sensor nodes uses RF links the probability of having a jamming DoS attack is highly predictable and will be researched in our future work.

IX. REFERENCES

[1] 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.

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

[3] 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.

[4] T.Martin, M.Hsiao, D.Ha, J.Krishnaswami, "Denial-Of-Service attack on Battery operated Mobile computers", Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications (PerCom'04), pg 309, 2004.

[5] 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.

[6] R. Anderson, " Security Engineering: A Guide to Building Dependable Distributed Systems", pages 326{331. Wiley Computer Publishing, 2001.

[7] 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.

[8] Percy P.C. Yip and Yoh-Han Pao, " Combinatorial Optimization with Use of Guided Evolutinary Simulated Annealing ", IEEE Transactions on Neural Network, Vol. 6, May 1999, pp. 968-972.

[9] B. R. Secrest, " Traveling Salesman Problem for Surveillance Mission using Particle Swarm Optimization ", Thesis , School of Engineering and Management of the Air Force Institue of Technology, Air University , 2001

[10] Shi Y. and Eberhart R.C., " Empirical Study of Particle Swarm Optimization ", Proc of the 1999 IEEE International Conference on Evolutionary Computation, Vol 3, 1999 IEEE Press, pp 1945-1950.

[11] Shi Y. and Eberhart R.C., " Parameter Selection in Particle Swarm Optimization ", Proc of the 1999 IEEE International Conference on Evolutionary Computation, Vol 7, 1998 IEE Press, pp. 591-600.

[12] Don J. Torrieri, "Principles of Secure Communication Systems", Artech House, Boston, London, 1992.

[13] Steven M. Kay, "Fundamentals of Statistical Signal Processing: Detection Thory", Vol II, Prentice-Hall Inc, 1998.

[14] Lisa Ann Osadciw, Edward L. Titlebaum and Mark Hahm, "Mainlobe characteristics of Ambuiguity Function for Linear Congruential Codes", Proc of Baltimore 1997 CISS Conference, Baltimore, MD, March 1997, pp 898-994.

[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, "Robustness of Predictive Sensor Routing in Fading Channels", In Proc of SPIE Defense and Security Symposium, Orlando, 2005.

[17] E. Bonabeau, M. Dorigo, and G. Théraulaz, " Swarm intelligence: from natural to artificial systems", Oxford University Press, 1999.

[18] Joseph Neggers and Hee Sik Kim, "Basic Posets", World Scientific Publishers, 1999.

[19] Rajani Muraleedharan and Lisa Ann Osadciw, "Decision Making In a Building Access System Using Swarm Intelligence & POSets", In Proc of 38th Annual Conference on Information Science and Systems, Princeton, NJ, March 2004.

[20] Kenneth J. Hintz and Greg McIntyre, "Goal Lattices for Sensor Management", Proceedings of Signal Processing, Sensor Fusion, and Target Recognition VII, 1999 SPIE International Symposium on Aerospace/Defense Sensing & Control, vol. 3720, Orlando FL, 1999, pp. 249-255.

[21] Varshney, P.K., Distributed Detection and Data Fusion, Springer-Verlag, 1997.

[22] Woodward, P. M., Probability and Information Theory, with Applications to Radar, Pergamon Press, Inc., NY 1953

[23] Rajani Muraleedharan and Lisa Ann Osadciw,"Security: Cross Layer Protocol in WSN", INFOCOM 2006, Spain.

[24] Rajani Muraleedharan, Lisa Ann Osadciw, "Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System", SPIE Defence and Security, Orlando, 2006.