A Swarm Based Defense Technique for Jamming Attacks in Wireless Sensor Networks

S. Periyanayagi and V. Sumathy

Abstract—**Jamming can interrupt wireless transmission and occur by mistake in form of interference, noise or as collision at the receiver or in the circumstance of an attack. In this paper, we propose 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 which channel there is prevalence of attacker 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.**

Index Terms—**Jamming attacks, Swarm Based Defense Technique (SBDT), Swarm Intelligence (SI), Wireless Sensor Networks (WSN).**

I. Introduction

A. Wireless Sensor Networks (WSN)

A wireless sensor network (WSN) constitutes a set of light-weight devices called sensor nodes. It has least energy resources for carrying out the process such as environment sensing, information processing, and communication [1]. A sensor network consists of wireless ad hoc network which means that each sensor supports a multi-hop routing algorithm (quite a few nodes forwards data packets to a base station). Each node in the sensor network is equipped with a radio transceiver or wireless communication device, microcontroller and an energy source (battery) in addition to one or more sensors [2].The wireless sensor network field provides prosperous, multi-disciplinary area of research where a various tools and concepts are engaged for addressing diverse set of application. The moving intruders in battle field are detected using wireless sensor networks. However, now wireless sensor network is used in civilian application field, which includes environment and habitat monitoring, health care applications, home automation, and traffic control [3].

B. Attacks on WSN

There are two types of attacks, namely invasive and non-invasive attacks in WSN.

Invasive Attack

Invasive attacks are those attacks that most commonly take place. They are as follows.

- Sybil Attack
- Denial of Service Attack
- Denial of Sleep attack
- Node-replication Attack
- Sinkhole Attack / Black holes
- Wormhole Attack

Non-Invasive Attack

The non-invasive attack occurs at the link layer. If the WSNs have vulnerability at the link layer, attack is expected at the MAC protocol and hence security is major issue for the network engineers [4].

C. Attack

WSNs are vulnerable to various forms of intrusions. It needs a solution in distributed and cheap manner in terms of communication, energy and memory requirements. For certain anomalies and applications, typical threats models must be known. The way by which cooperative adversaries might attack the system should be understood by researchers and practitioners. For decentralized intrusion detection, the promising technique is to utilize secure groups. A new automated defense against DoS is obtained by networked nature of sensor networks. The jamming-resistant network could overcome the attack by detecting the jamming, mapping the affected region and routing the jammed area when jamming affects a part of the network [5].

D. Problem Identification and Solution

Among the above discussed different attacks, we consider the jamming attack in this paper and develop a novel detection and defense technique for this attack.

Jamming can interrupt wireless transmission and occur by mistake in the form of interference, noise or as collision at the receiver or in the circumstance of an attack. Jamming attack is efficient from an attacker's point of view as

1) An opponent doesn't need special hardware to launch it.
2) An attack can be implemented by listening to an open medium and distributing in the similar frequency band same as network.
3) It can lead to significant benefits with small incurred cost

Manuscript received October 30, 2011; revised November 30, 2011.

S. Periyanayagi is with Department of ECE, Angel College of Engineering and Technology, Tirupur (e-mail: periyanayagiphd@gmail.com)

V. Sumathy is with Department of ECE Government College of Technology

for the attacker when launched in a wise manner.

With respect to machinery and impact of jamming attacks, they usually plan for the physical layer so that they are realized by means of a high transmission power signal that corrupts a communication link or entire area [6].

We assume that there are four types of jamming attacks as follows

1) Single-Tone Jammer
2) Multiple-Tone Jammer
3) Pulsed-Noise Jammer
4) ELINT

The network activity becomes poorer as attack can completely remove a coverage area, and in some application network cannot be immediately updated. Therefore, the study of different characteristics of attacks, keep attack minimum since the idea of types of jammer is helpful in taking suitable countermeasure. Link layer jamming using MAC layer semantics is a complex type of reactive jamming attacks. A link layer jammer switches between the sleeping and active modes and also adjusts its operation to the MAC layer rules of the participants in the communication. Hence the jammer uses total energy in an effective manner.[4]

The work by Rajani Muraleedharan and Lisa Ann Osadciw [7] doesn't consider jammer detection in effective way and this leads to major problem.

DEEJAM [8] provides four defensive mechanisms for hiding communication from jammer, evading its search and reducing its impact. But the technique is complex involving complicated calculation and results in more overhead.

In this work, the same scenario of jamming attack is considered and a robust solution for this attack with minimum overhead is proposed. The solution depends on swarm intelligence technique which updates the sensor details more efficiently and successfully. In our proposed work, DEEJAM is combined with swarm technique such that swarm's forward and backward agents scan through all the channels in a fast way and detects effectively the jamming activity by informing the legitimate node. Then legitimate node swaps the channel by avoiding the affected channel. This will improve the detection of a jammer quickly with less complication.

Swarm Intelligence (SI) is all about designing intelligent multi-agent systems inspired by collective activities of social insects such as ants, bees and wasps. The agents in the SI system interact directly or indirectly in a distributed troubleshooting way. The agents move towards for the optimal results and interact directly by sharing facts with their neighbors. These agents are very helpful in finding the minimum path to the concerned destination in a short time required.

Swarm intelligence has the following advantages

- The proximity principle – it carry out simple space and time computation.
- The quality principle – it responds to quality factors.
- The principle of diverse response – it doesn't commit activities along excessively narrow channels
- The principle of stability – does not change its behavior every time as the environment changes.
- The principle of adaptability – it change behavior mote when it is worth the computational price. [9]

II. Related Work

A. Attack Detection Techniques in WSN

Waldir Ribeiro Pires Junior et al [10] have proposed protocols for detecting suspicious transmissions and the consequent identification of malicious nodes and for disseminating this information in the network. They evaluated the detection rate and the efficiency of their solution along a number of parameters. They provided a solution to identify malicious nodes in wireless sensor networks through detection of malicious message transmissions in a network. A message transmission is considered suspicious if its signal strength is incompatible with its originator's geographical position.

Devesh C. Jinwala et al [11] have proposed a novel design of link layer security architecture for WSNs. The principal characteristic of the design is the flexible and configurable architecture, with respect to the actual security attributes demanded by the application. Their design is based on the premise that when the link layer architecture is implemented in software, flexibility and seamless integration of the application code become the prime advantages.

Wenyuan Xu et al [12] have proposed two enhanced detection protocols that employ consistency Checking. The first scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, while the second scheme employs location information to serve as the consistency check. They examine the feasibility and effectiveness of jamming attacks and detection schemes using the MICA2 Mote platform.

B. Defense Techniques in WSN

Mingyan Li et al [6] have considered a scenario where a sophisticated jammer jams an area in which a single-channel random-access-based wireless sensor network operates. The jammer controls the probability of jamming and the transmission range in order to cause maximal damage to the network in terms of corrupted communication links. The jammer action ceases when it is detected by the network (namely by a monitoring node), and a notification message is transferred out of the jammed region. The jammer is detected by employing an optimal detection test based on the percentage of incurred collisions. On the other hand, the network defends itself by computing the channel access probability to minimize the jamming detection plus notification time.

Anthony D. Wood et al [8] have presented DEEJAM, a novel MAC-layer protocol for defeating stealthy jammers with IEEE 802.15.4-based hardware, to address this problematic area. It layers four defensive mechanisms to hide communication from a jammer, evade its search, and reduce its impact.

Rajani Muraleedharan and Lisa Ann Osadciw [7] have proposed an extension to the security of physical layer of a predictive sensor network model using the ant system. 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.

III. Swarm Based Defense Technique

A. Swarm Intelligence (SI)

Swarm intelligence (SI) is the interaction of simple agents in order to achieve a universal goal. Using social insect metaphor for solving various problems is the main basis of swarm intelligence. Ants, bees, and termites are the insects which live in colonies. Every insect in colony have their own plans. The combination of their activities does not have any supervisor. A worker in insect colony does not execute all tasks but rather specializes in particular task. Thus working in this manner is more efficient than performed by unspecialized individuals. SI is emerged as combined intelligence of groups of simple agents. An alternative means of designing intelligent system is offered by SI, so that autonomy, emergence and distributed functioning are replaced control, preprogramming and centralization. This technique focuses on distributed ness, flexibility, strength, and direct or indirect communication among fairly simple agents [13].

Interactions among insects for acquiring self organization can be of direct or indirect form. Direct interactions are with food or liquid exchange. Indirect interaction are delicate in which when two individuals are interacting, one modifies the environment and other answers new environment at a later time. This interaction is an example of stigmergy which is a mechanism of indirect coordination between agents or actions [13].

The agents are autonomous entities which are reactive and proactive and have potential to adapt, collaborate and travel from one location to the other in a communication network.

The complex interaction of thousands of autonomous swarm members results in intellectual behavior of SI. The individual ant during food searching process randomly selects the path to proceed. When ants start moving they leave behind a chemical substance called pheromone. Other ants smell and recognize that an ant has visited there before. When the pheromone level is more concentrate, the ant will proceed with that route. Later, the concentration of pheromone keeps decreasing over time. The interaction of individuals gives complex group activities.

The numerous applications of ant agents in the real world are industry, design, vehicle routing, network and gaming.

B. General Characteristics of SI

- SI offers characteristics such as adapting network and generating multipath for routing. SI algorithm is proficient enough to adapt change in network topology and traffic and further gives equivalent performance.
- It depends on both passive and active information for collective monitoring. They gather non-local information regarding the traits of solution set, like every potential paths.
- It utilizes stochastic component like pheromone table for user agents. User agents are autonomous and can interact through stigmergy.
- It sets the way in favor of load balancing than pure shortest path. The algorithm also supports multiple paths in order to achieve load balancing.

C. Principle of SI

There are four principles based on which ants will self organize. They are positive feedback, negative feedback, randomness and multiple interactions.

- Positive feedback- This is helpful in enhancing the good result. The pheromone concentration increases when the ant changes the path from one node to another. This is helpful for other ants to move in this path.
- Negative feedback- This is mainly used to devastate bad results. It is done by decomposing pheromone concentration with respect to time. The rate of decay is trouble specific.
- Randomness - The path selected by ant is in a random manner and thus there is a possibility to generate new results.
- Multiple interactions- By interaction of many agents, the solution is obtained. During food searching process, one ant cannot find the food since pheromone decays. However more ants can find food sooner.

D. Proposed Detection Algorithm

Step 1

The sender and receiver change channels in order to stay away from the jammer, in channel hoping technique.

Step 2

The pair-wise shared key KS is used for creating a channel key $KCh = EKS(1)$, which generates a pseudorandom channel sequence

$$Ch_S = \{E_{KS}(i) \bmod Ch\}, i \geq 0,$$

where, Ch is the number of channels available in the band, message mi is transmitted on channel Chi, (unknown to any but the two parties involved.)

Step 3

Using packet fragmentation technique, the packets are break into fragments to be transmitted separately on different channels and with different SFD (start of frame delimeter). The last fragment contains a frame check sequence FCS for the entire payload.

Step 4

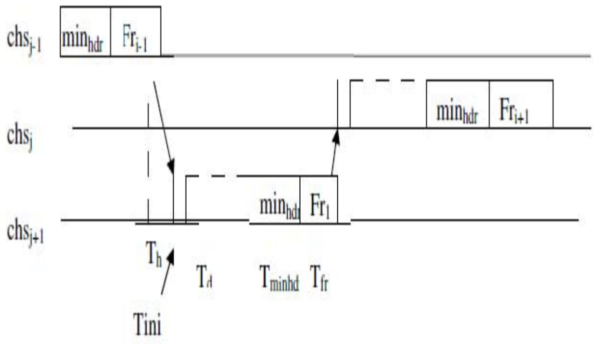

Fig. 1. Packet fragmentation technique

The above figure shows the way in which fragments are transmitted.

To transmit fragment Fri, the sender hops to Chi, fills the transmit FIFO with Fri, sets SFD to Si , and issues the transmit command.

Step 5

The time to transmit the fragment is

$$T_{frag} = T_h + T_{ini} + T_d + T_{minhdr} + T_{fr}$$

Step 6

If the fragments are short, the attacker's jamming message does not start till the sender has finished transmitting and hopped to another channel.

Step 7

In the Pulse Jamming attack, the jammer remains on a single channel, hoping to disrupt any fragment that may be transmitted. As packets cannot be detected quickly enough for selective jamming, the attacker transmits blindly in short pulses. The jamming pulses must occur no less frequently than $T_{minhdr} + T_{fr}$ to prevent any fragments from slipping through.

Step 8

The forward ants (FA) explore the network to collect the jammer's information on each channel. It keeps collecting the attackers' data if any and moves forward though channels. When the FA reaches the end of the channel, it is deallocated and the backward ant (BA) inherits the stack contained in the FA.

Step 9

The BA is sent out on high priority queue. The backward ants retrace the path of the FA and utilize this information to update the data structures periodically.

Step 10

As it reaches the source, the data collected is verified which channel there is prevalence of attacker long time, and those are omitted. Simultaneously the forward ants are sent through other channels which are not detected before for attacks.

Step 11

The FAs either unicast or broadcast at each node depending on the availability of the channel information for end of the channel.

Step 12

If the channel information is available, the ants randomly choose the next hop. This scheme helps limit the channel maintenance overhead. If the pheromone information is available at the channel i , then the channel probability P $(Ch^{i,j,d})$ of choosing neighbor channel j as the next hop for last

$$P(Ch_{i,j,d}) = \frac{[\sigma_{i,j,d}]^{\alpha}[\lambda_{i,j}]^{\beta}}{\sum_{l \in N_i}[\sigma_{i,l,d}]^{\alpha}[\lambda_{i,l}]^{\beta}}$$

where α and β are the relative weights for pheromone trail $\sigma_{i,j,d}$ and the heuristic value $\lambda_{i,j}$. For optimal performance, normally α is set to 1 and β is set to 2. Ni is the neighbors of channel i

Step 13

The heuristic value λ_i is calculated depending listening time of various users and number of pulses generated by each users, which is as follows,

$$\lambda_i = LT_i + NP_i$$

where LTi = listening time of various user at channel i

NPi = number of pulses generated by each users in channel i

Step 14

$$\text{If } LT_i > LT_{th} \text{ and } NP_i > NP_{th}$$

Then FA receives negative reinforcement, whose probability is given as,

$$P_{nl} = P_{nl} + r^{-}$$

where P_{nl} is the probability values assigned to neighbors' n of the current channel for last channel d and r^{-} is negative reinforcement. LTth and NPth are threshold values of listening time of various users and number of pulses generated by each user.

At the same time warning message about the channel i is sent to the sender. On receiving the warning message, the sender omits the channel i and sends the fragment message through another channel.

Step 15

If $LT_i < LT_{th}$ and $NP_i < NP_{th}$

Then FA receives positive reinforcement, whose probability is given as,

$$P_{fl} = P_{fl} + r^{+}$$

where P_{fl} is the probability values assigned to neighbors' f of the current channel for last channel d and r^{+} is the positive reinforcement.

IV. Simulation Results

A. Simulation Model and Parameters

The Network Simulator (NS2) [14], is used to simulate the proposed architecture. The IEEE 802.15.4 MAC layer is used for communication among the devices, providing access to the physical channel for all types of transmissions and appropriate security mechanisms. IEEE 802.15.4 provisions 16 channels separated by 5 MHz, and the Chipcon CC2420 allows dynamic selection of the same [8]. The IEEE 802.15.4 specification supports two PHY options based on direct sequence spread spectrum (DSSS), which allows the use of low-cost digital IC realizations. The PHY adopts the same basic frame structure for low-duty-cycle low-power operation, except that the two PHYs adopt different frequency bands: low-band (868/915 MHz) and high band (2.4 GHz). The PHY layer uses a common frame structure, containing a 32-bit preamble, a frame length.

In the simulation, 50 mobile nodes move in a 750 meter x 750 meter region for 50 seconds of simulation time. All nodes have the same transmission range of 40 meters. The simulated traffic is Constant Bit Rate (CBR). In our simulation, 4 source nodes send their sensor data to the sink. We have two jamming attack nodes along the same channel.

The simulation settings and parameters are summarized in table.

No. of Nodes	50
Area Size	750 X 750
Mac	IEEE 802.15.4
Transmission Range	40m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Sources	4
Attackers	2
Rate	50kb to 250kb

B. Performance Metrics

The proposed Swarm Based Defense Technique (SBDT) is compared with the DEEJAM detection technique [8]. The performance is evaluated mainly, according to the following metrics.

- **Aggregated Throughput**: We measure aggregated throughput in terms of packets received.
- **Packet Delivery Ratio:** It is the ratio between the number of packets received and the number of packets sent.
- **Packet Drop:** It refers the average number of packets dropped during the transmission

C. Results

1) Based on Rate

In the initia05l experiment, we vary the traffic rate as 50,100,150,200 and 250kb.

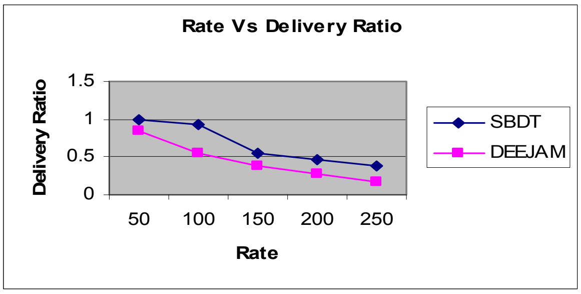

Fig. 2. Rate Vs packet delivery ratio

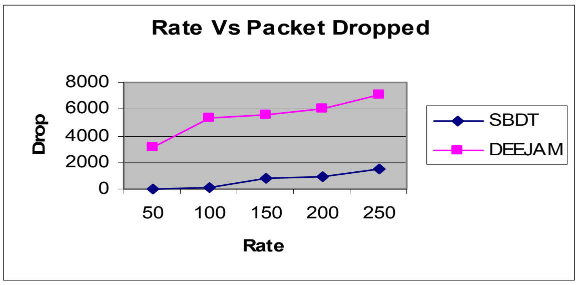

Fig. 3. Rate Vs packet dropped

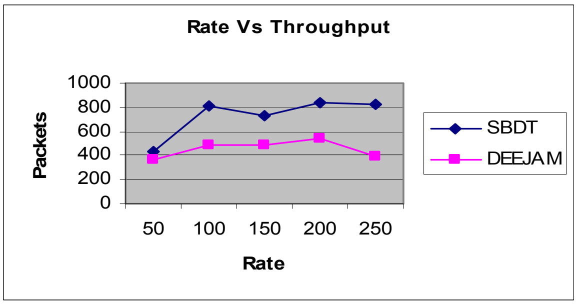

Fig. 4. Rate Vs throughput

Since the proposed SBDT technique efficiently detects and eliminates the jamming attacks, the packet drop due to jamming attack is reduced to a great extent. Hence the throughput and packet delivery ratio are also increased.

Fig. 3, 2 and 4 illustrates the packet drop, delivery ratio and throughput for SBDT and DEEJAM respectively, when the sending rate is increased from 250 to 450kb. From the figures, we can see that the throughput and delivery ratio are more for SBDT when compared with DEEJAM.

2) Based on Time

In this experiment, we measure performance in various time intervals from 10 to 50 seconds of simulation time with rate as 250kb.

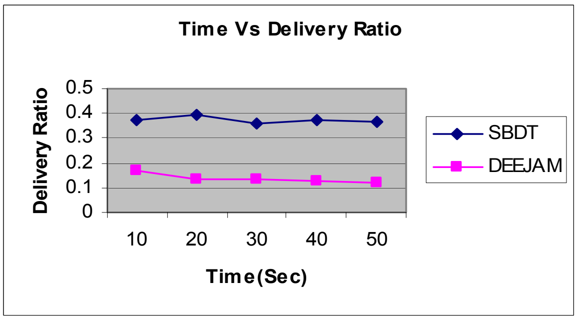

Fig. 5. Time Vs packet delivery ratio

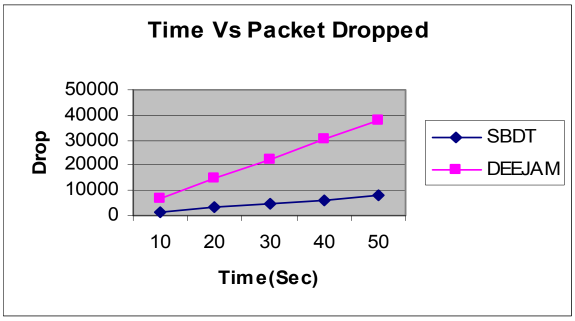

Fig. 6. Time Vs packet dropped

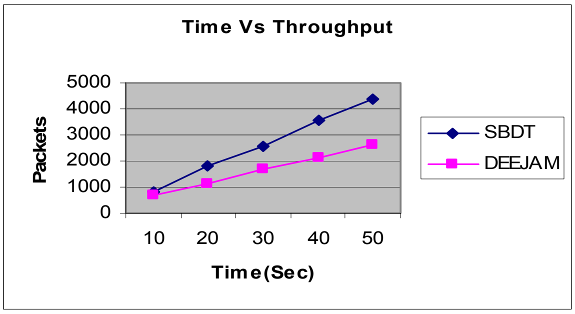

Fig. 7. Time Vs throughput

Fig. 6, 5 and 7 illustrates the packet drop, delivery ratio and throughput for SBDT and DEEJAM respectively, when the time interval is increased from 10 to 50 seconds. Similar to the previous case, from the figures, we can see that the throughput and delivery ratio are more for SBDT when compared with DEEJAM

V. Conclusion

In this paper, we propose 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 which channel there is prevalence of attacker 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 concluded that this swarm based defense technique for jamming attack is most effective.

References

[1] Z. A. Baig and S. A. Khan "Fuzzy Logic-based Decision Making for Detecting Distributed Node-Exhaustion Attacks in Wireless Sensor Networks," *Second International Conference on Future Networks*, 2010.

[2] from http://en.wikipedia.org/wiki/Wireless_sensor_network

[3] Mukesh Tiwari, Karm Veer Arya, Rahul Choudhari and Kumar Sidharth Choudhary "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information," *Fourth International Conference on Computer Sciences and Convergence Information Technology*, 2009

[4] Y. W. Law, P. Hartel, J. den Hartog and P. Havinga, "Link-layer jamming attacks on S-MAC," *in Proceedings of IEEE WSN'05*, 2005, pp.217-225.

[5] Adrian perrig, John stankovic, and David wagner "Security In Wireless Sensor Networks," *Communications of the ACM*, June, Vol. 47, 2004.

[6] M. Y. Li, Iordanis Koutsopoulos and Radha Poovendran "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks," *IEEE Trans. Mobile Computing*, Vol. 9, No. 8, August 2010.

[7] Rajani Muraleedharan and Lisa Ann Osadciw "Jamming Attack Detection and Countermeasures in Wireless Sensor Network Using Ant System," *in Wireless Sensing and Processing, proceedings of the SPIE*, volume 6248, pp. 62480G, 2006.

[8] A. D. Wood, J. A. Stankovic, and G. Zhou. "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks,". *In Proc. of SECON '07*, 2007

[9] Swagatam Das, Ajith Abraham and Amit Konar, "Swarm Intelligence Algorithms in Bioinformatics," *Computational Intelligence in Bioinformatics*, Arpad Kelemen et al. (Eds.), Springer Verlag, Germany, 2007.

[10] Waldir Ribeiro Pires Junior Thiago H. de Paula Figueiredo Hao Chi Wong "*Malicious Node Detection in Wireless Sensor Networks,*" Society for Computer Simulation International San Diego, CA, USA, 2008.

[11] C. D. Jinwala, R. D. Patel and S. D. Kankar "Configurable Link Layer Security Architecture for Wireless Sensor Networks," *Proceedings of the World Congress on Engineering* 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.

[12] W. Y. Xu, W. Trappe, Y. Y. Zhang and Timothy Wood "The feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," *MobiHoc'05*, May 25–27, 2005, UrbanaChampaign, Illinois, USA

[13] N. K. Cauvery, and K. V. Viswanatha, "Enhanced Ant Colony based Algorithm for Routing in Adhoc Network," *World Academy of Science, Engineering and Technology* 46 2008.

[14] Network Simulator, http://www.isi.edu/nsnam/ns

S. Periyanayagi has completed her B.E (ECE) in Kumaraguru College Of Technology from Bharathiyar University and M.E(Communication Systems) in Kumaraguru College of Technology from Anna University and pursing her Ph.D in Anna University of Technology ,Coimbatore from july 2007.she is working as Assistant Professor in Department of ECE at Angel College of Engineering and Technology, Tirupur. Her areas of interest are wireless sensor networks, Digital communication.

Dr. V. Sumathy has B.E.(ECE) in Government College of Technology, Coimbatore and her M.E in Computer Science in Government College of Technology, Coimbatore .She had completed her Ph.D in the area of Wireless Adhoc Networks from Anna University Chennai in the year 2006. She has more than twenty years of teaching experience and currently working as a Assistant Professor in the Department of ECE at Government College of Technology. Her areas of interest are Wireless networks, Wireless Adhoc Networks, Wireless Sensor Networks etc. She is Guiding More than 10 Research scholars in various domains of Wireless Networks.