DEALING WITH JAMMING IN WIRELESS SENSOR NETWORK

Md. Shanawas Babu
ID:-09221141
Md. Fahmidur Hossen
ID:-09221103

Department of Computer Science and Engineering
June 2005

BRAC University, Dhaka, Bangladesh

DECLARATION

I hereby declare that this thesis is based on the results found by myself. Materials of work found by other researcher are mentioned by reference. This theis, neither in whole nor in part, has been previously submitted for any degree.

for Md. Khalilur Rhaman

Signature of
Supervisor
(Dr. Al-Sakib Khan Pathan)

Signature of
Author

ACKNOWLEDGMENTS

Special thanks to Al-Sakib Khan Pathan who give us all kind of material that we need for our thesis. He also help us about how to think and proceed forward. We give our admiration to our co-supervisor Khalilur Rhaman who has always stayed beside us, encouraged and uphold us whenever we felt exhausted and confused.

TABLE OF CONTENTS

Page

TABLE OF CONTENTS

Page

LIST OF FIGURES

Abstract:

Wireless sensor networks (WSNs) have emerged as an important application area resulting from the advancement of efficient short-range radio communication and miniaturization of computing devices .As these networks (WSNs) are built upon a shared medium that makes it easy for adversaries to conduct radio interference, or jamming, attacks that effectively cause a denial of service of either transmission or reception functionalities. In this paper we survey different jamming attacks that may be employed against a sensor network, as well as different types of defense strategies in order to cope with the problem of jamming attacks.

A jamming attack can be launched in data-link layer or physical layer. Link layer jamming attacks disturb the communication between sensor nodes around the jammer. Physical layer jamming attacks let the radios frequency interfere with the open wireless environment. In WSN architecture, Base Stations (BSs) are the prime target for jamming attack because of their importance in aggregating sensor readings, and for playing a role in security protocols. Our objective is to find a defense strategy against BS jamming attack in WSNs.

Introduction:

Wireless Sensor Network, or WSN, is a network of RF transceivers, sensors, machine controllers, microcontrollers, and user interface devices with at least two nodes communicating by means of wireless transmissions. The development of wireless sensor network (WSNs) was originally motivated by military applications such as battlefield monitoring [5]. However, wireless sensor networks are now used in many industrial and civilian application areas, including machine health monitoring, environment and habitat monitoring [2], indoor sensor networks with sensor enabled user interfaces [1], home automation, and traffic control. As the applications of WSNs are increasing, providing security and trustworthiness is an important issue. In WSN, sensor nodes have limited resources such as energy, computation power and storage available. The broadcast nature of communication in WSN significantly increases the capabilities of adversary to initiate Denial of Service (DoS) attacks. In a DoS attack, an adversary can deny to follow medium access protocol. In this manner, it can continuously transmit on the wireless channel, and prevent the legitimate user to perform MAC operations, or introduce packet collision that force repeated back offs, or even jam transmission [3].

Jamming attacks are representative energy consumption DoS attacks in WSN. Jamming is a well known DoS attack, which interferes with the radio frequencies used by sensor nodes for communication. Anti-jamming techniques such as spread-spectrum and lower duty cycle are not widely applicable for low cost sensor networks [4].

In a WSN, the Base Station (BS) aggregates sensor readings and conducts command and control tasks. So it is a central point of failure and is an attractive target for jamming attack, because failing of it can render the whole WSN out-of-service during attack [6].

Basic Sensor Network Operation:

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors nodes to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. Each node in a sensor network consists of a transceiver unit, a processing unit, a power unit, a small microcontroller and a battery which is used as the energy source. The transceiver unit connects the node to the network. Power unit [7] is an important component of a node and it may be supported by power generator such as solar cells. Sensor nodes are equipped with very limited computational power and energy resource. The WSN consists of hundreds or thousands of nodes that are scattered in an area called sensor field. The nodes sense data and forward the same to the outside world via the sink node or the base station. The base station or the sink node is responsible for receiving data from the nodes present in the network and processing them for sending data to the outside world. [8]

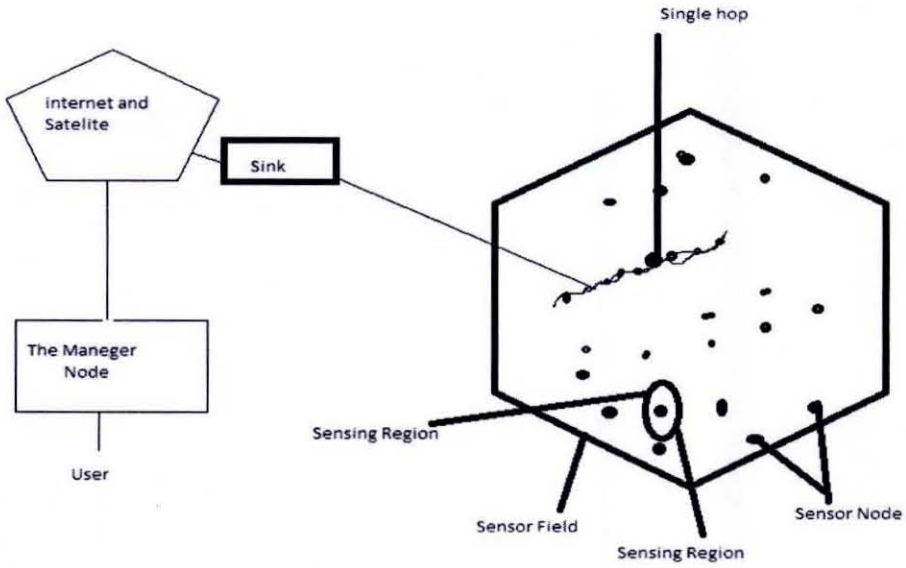


Figure 1: Basic Sensor Network Operation

Figure .1 shows the operation of a sensor network [9]. The data ultimately reaches the user via the internet or satellite. Nodes in a WSN are deployed in an open field and thereby they remain unattended and are prone to attack [10] by adversaries. One of the attacks is jamming attack where the adversary blocks the radio communication of one or more nodes which are within the sensing range of the adversary by capturing a particular frequency.

Jamming Attacks:

There are many different attack strategies an adversary can use to jam wireless communications [11]. Some commonly known attack strategies discuss bellow

Constant jammer:

The constant jammer continually emits a radio signal, and can be implemented using either a waveform generator that continuously sends a radio signal [12] or a normal wireless device that continuously sends out random bits to the channel without following any MAC-layer etiquette [13].

Deceptive jammer:

Instead of sending out random bits, the deceptive jammer constantly injects regular packets to the Channel without any gap between subsequent packet transmissions. As a result, a normal communicator will be deceived into believing there is a legitimate packet and be duped to remain in the receive state. For example, in TinyOS, if a preamble is detected, a node remains in the receive mode, regardless of whether that node has a packet to send or not. Even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected.

Random jammer:

Instead of continuously sending out a radio signal, a random jammer alternates between sleeping and jamming. Specifically, after jamming for a while, it turns off its radio and enters a "sleeping" mode.During its jamming phase, it can behave like either a constant jammer or a deceptive jammer. This jammer model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply.

Reactive jammer:

An alternative approach to jamming wireless communication is to employ a reactive strategy. The reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. One advantage of a reactive jammer is that it is harder to detect.

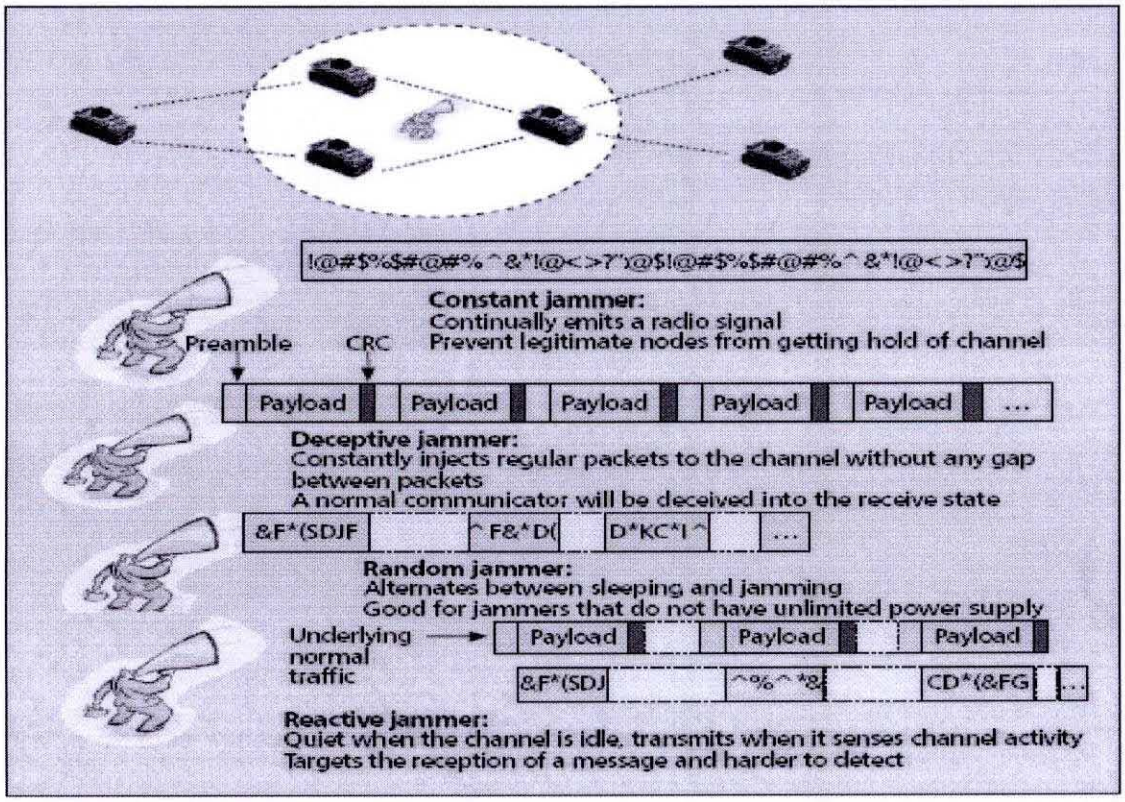


Figure 2: Jamming attacks target a sensor's ability to transmit or receive packets. Different jamming models accomplish the objective of blocking communications through different strategies. [0]XU et. al.

Different types of defense strategies:

A number of works towards defending WSN from attacks have reported so far. Some of those are not that effective and some of those have advanced detection strategies. A brief description about some of these techniques is given bellow.

Signal Strength:

One natural measurement that can be employed to detect jamming is signal strength. The rationale behind using this measurement is that the signal strength [11] distribution may be affected by the presence of a jammer. Two natural approaches to detecting jamming using signal strength involve comparing average signal magnitude vs. a threshold calculated from the ambient noise levels, and classifying the *shape* of a window of signal samples.

Packet Delivery Ratio:

PDR may be used to detect the presence of jamming, as the jammer can effectively corrupt transmissions, leading to a much lower PDR. Since a jamming attack will degrade the channel quality surrounding a node, the detection of radio interference attack essentially boils down to determining whether the communication node can send or receive packets in the way it should have had the jammer not been present. More formally, let us consider the PDR between a sender and a receiver who are within radio range of each other, assuming that the network only contains these two nodes and that they are static. As noted earlier, an effective jammer results in a very poor PDR, close to 0, which indicates that PDR may be a good candidate in detecting jamming attacks. We

would like to point out that a non aggressive jammer, which only marginally affects the PDR, does not cause noticeable damage to network quality and does not need to be detected or defended against.

Carrier Sensing Time:

A jammer can prevent a legitimate source from sending out packets because the channel might appear constantly busy to the source, and hence it might seem possible to use carrier sensing time as a means to determine whether a device is jammed. In [] the authors explored this possibility. We observed that using carrier sensing time is suitable when the following two conditions are true: the jammer is non-reactive or non random, and the underlying MAC protocol determines whether a channel is idle by comparing the noise level with a fixed threshold. If these two conditions are true, carrier sensing time is an efficient way to discriminate a jammed scenario from a normal ill-functioning scenario, such as congestion, because the sensing time will be bounded, although large, in a congested situation, but unbounded in a jammed situation. Overall, carrier sensing time alone cannot be used to detect all the jamming scenarios.

Our Recommended Solution:

In this paper, we propose a hybrid model of defense for mitigating BS jamming attacks in WSNs. The hybrid model is a combination of three defense techniques: the first technique is mapping jammed area, so that Network services can use this knowledge to influence routing, power management, and higher-layer planning. Our second technique BS replication, so in a jamming condition, there may be some unjammed replicated BSs, which can provide service to the network.. The second defense technique is multipath routing, so there may be some alternate paths available for communication with BS in case of jamming one or more paths by jammers. In this work, we enhance DYMO routing protocol [9] to support multiple path data delivery.

Problem Overview:

A jamming attack can be launched in data-link layer or physical layer. Link layer jamming attacks disturb the communication between sensor nodes around the jammer. Physical layer jamming attacks let the radios frequency interfere with the open wireless environment. In WSN architecture, BSs are the prime target for jamming attack because of their importance in aggregating sensor readings, and for playing a role in security protocols. We propose a hybrid model of defense against BS jamming attack in WSNs. The hybrid model contains a combination of three defense techniques. A brief description about these techniques is given below

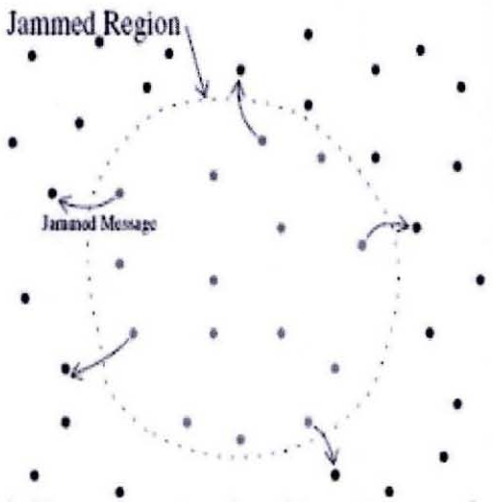
Mapping Jammed Areas:

Following the detection of whether a node is jammed, it is desirable for the network to map out regions of the sensor network that are jammed. By having a map of jammed areas, network services can use this knowledge to influence routing, power management, and higher-layer planning. A protocol for mapping out the jammed regions of a sensor network was presented in []. In this article jamming detection is performed by monitoring channel utilization. Once the sensors observe that their channel utility is below a preset threshold, they conclude that they are jammed. Following detection, the jammed nodes bypass their MAC-layer temporarily and broadcast JAMMED messages, announcing the fact that they are jammed. These JAMMED messages will not be able to be received by other jammed neighbors. However, those neighbors on the boundary of the jammed region, but are not themselves jammed themselves, will be able to hear the JAMMED messages, though potentially at a higher error rate. Once non-jammed sensors receive JAMMED messages, they initiate the mapping procedure. These non jammed nodes exchange and merge information describing which nodes they have witnessed as jammed, where those jammed

sensors are located, along with neighbor information. By continuing the exchange of information regarding witnessed jammed nodes, the network will eventually be able to map out the boundary of a jammed area. We describe there idea bellow.

How To Map Jammed Area:

Two primary components form the basis of the mapping service, a jamming detection module, and a mapping module. Both operate on every node in the network. The jamming detection module is responsible for monitoring the radio and medium access control (MAC) layers and applying heuristics to determine whether the node is jammed. When it determines that the local node is most likely jammed, it sends a message to its neighbors by overriding the carrier-sense multiple access (CSMA) limitation usually enforced by the MAC, shown in Figure 3(a).it alerts the application layer, which can apply power management strategies to help the node outlast the jamming.



(a) Upon detecting local jamming, nodes blindly report it to their neighbors.

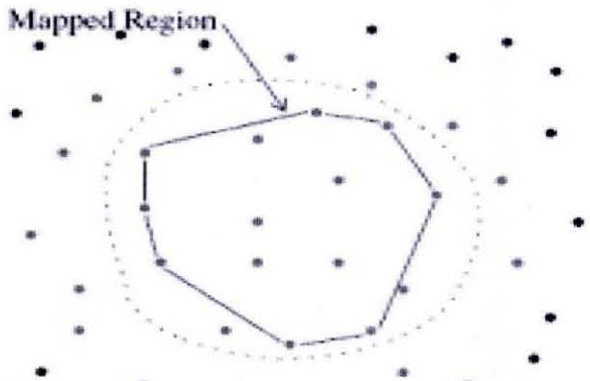
Figure 3(a)

Mapping is initiated by the neighbors of jammed nodes who receive the jamming notifications. Each receiver forms a group, explicitly adding nearby jammed nodes as jammed members; the receiver itself becomes a mapping member. Figure 3(b) shows mapping messages, which contain information about the local group, being exchanged between neighbors.

(b) Receivers outside the jamming form groups and exchange mapping messages.

Figure 3(b):

Neighboring groups are coalesced and eventually most or all of the mapping members know about the jammed region, as shown in Figure 3(c). Details of the mapping protocol are in Section 2.2. When the jammer(s) move or simply stop the attack, the jammed nodes recover and send notifications to their neighbors informing them of this change. The mapping members change the status of the formerly jammed nodes and send messages to update the group. When a mapping member knows of no neighboring nodes that remain jammed, it retires from the group.



(c) Groups are coalesced to yield a mapped region.

Figure 3(c):

BS Replication:

According to this technique, there should be multiple replicated BS in WSN, so that in case of a jamming attack, if one or more BSs are not jammed, these can serve the whole WSN, and the WSN can continue delivering data for alonger time during such a jamming attack. When jammed BS becomes unjamed, they may request for the sensor readings from unjammed BSs.

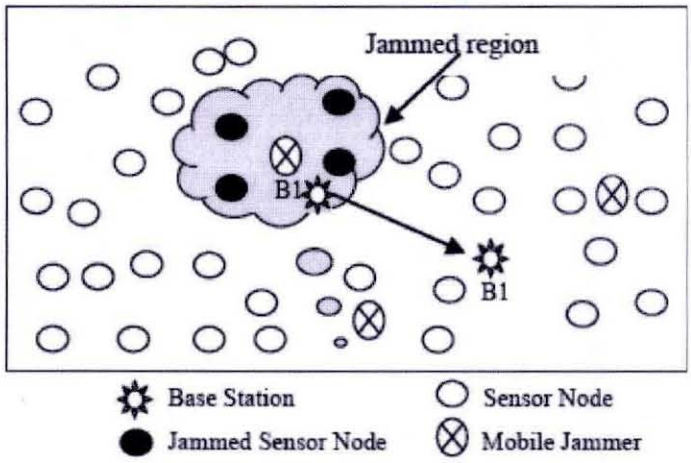


Figure 4: BS Replication

Multipath Routing:

Our third defense technique is multipath routing. According to this technique, there should be multiple paths between sensor nodes and BS, so that in case of jamming attack, if atleast one path between sensor node and BS is not jammed, the BS can get sensor readings through this path and the sensor network can continue working. Through multipath routing, traffic dispersion can be used to prevent eavesdropping, to do load balancing or to minimize the energy consumption by nodes. Traffic dispersion means that, for a same source

destination pair, communication simultaneously uses different paths (i.e. multiple paths) instead of a single one [].

Figure 3 shows a WSN consisting of 5 BSs and 3 mobile jammers, one of which successfully jams a BS. There are two paths from sensor node S1 to BS B1 (path P1 and path P2). As one sensor node under path P2 is jammed, sensor readings are delivered by path P1. Thus there is no effect of jamming on un-jammed BSs for reading the sensor information from un-jammed sensor nodes.

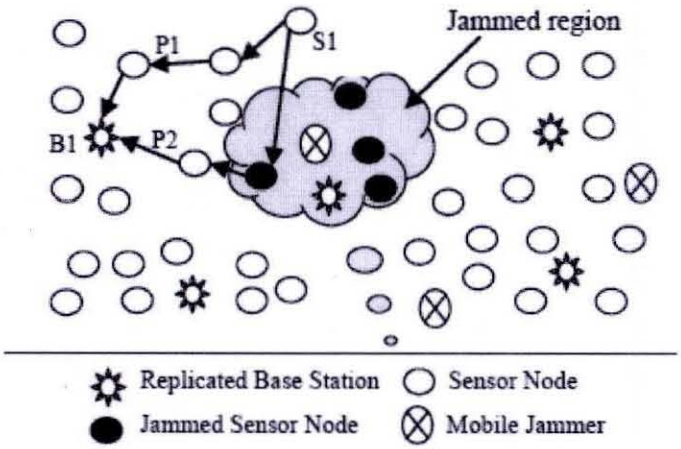


Figure 5: Multipath Routing

Network Framework and Attack Model:

Our WSN is organized in a tree-like structure, where BS works as a root node of the tree. Sensor nodes sense around, and report the sensing result to the BS. Sensing results contain the normal sensing data or alarm event messages. The sensor nodes under the jammed area are called jammed sensor nodes. These jammed sensor nodes cannot transmit data to the BS. According to a pro-active defense strategy, the BS roam among collection points using a pseudo-random schedule, pre-loaded off-line. It may be possible that the unjammed BS have to change location, while jammed BS may remain at their location. Multipath extension of DYMO routing protocol proposed in [15] introduces the advertised hop count to prevent loops and a header extension (the last hop field) to identify the path. Last hop is the destination neighbour. The path is identified with the pair nexthop/ last-hop.

The following are the modifications made by [15] in DYMO routing protocol for extending it to a multipath routing protocol:

1. During the request phase, every intermediate node has to save the path to the request the packet's originator in order to send the corresponding reply message to it. Therefore, every intermediate node registers all the paths with different last hops though they may arrive through the same neighbour (next hop in the path register).

2. During the reply phase, when the destination node receives a Route Request, it sends the reply back through the neighbour node from which it received the packet; the last-hop value is the same one contained in the request packet. The first path used by each intermediate node with this last hop is the valid path and determines its next hop; the node removes the other paths with the same next hop although with a different last hop.

3. After the route discovery process, every node will have one or more routes for every possible destination.

Simulation results of [15] show that by introducing multipath routing, reduction in the throughput of both UDP and TCP connections is under 20%. It shows that multipath extension of the routing protocol decreases the throughput only by a little amount.

Limitation of Our Model:

We assume the following capabilities of jamming attackers:

1. An attacker can compromise a sensor node, and can obtain all its information.

2. Jammers can move, so that jammed locations can be changed by the mobile jammers.

3. The mobile jammers are uncoordinated and unsynchronized. They follow an off-line schedule to determine when, where, and which jammers to move. So it may happen that successfully jamming attackers have to move, while unsuccessful ones remain still.

4. Jammers continuously emit RF signals to fill the wireless channel, so that legitimate traffic may be blocked. A jammer can do this by either preventing sensor nodes to send sensor readings, or by preventing the reception of legitimate traffic at the BSs.

5. A jammer does not have information about the whole network, and it cannot jam the entire network.

6. Jammers can flood the BS with illegitimate packets, so that it cannot receive legitimate packets from sensor nodes

7. We assume that the attacker cannot be

DYMO Multipath Routing Protocol:

Our multipath routing protocol is an extension of DYMO (Dynamic MANET On-demand) routing protocol, which is based on []. DYMO [] is basically an enhancement of the AODV protocol [3]. In the multipath route discovery process, if several Route Replies arrive at the source, through different neighbor nodes and different path identifiers, the DYMO agent keeps these nodes as next hops in the destination entry of its route table, which enables extending the path selection algorithm to make traffic dispersion. For traffic dispersion, multiple paths between source-destination pair will be link disjoint routes, so that nodes can be common for two or more paths.

Conclusion and Future plan:

In this paper, we propose a hybrid model of defense for mitigating BS jamming attacks in WSNs. The hybrid model is a combination of three defense techniques: the first technique is BS replication, so in a jamming condition, there may be some unjammed replicated BSs,In wireless sensor networks the nodes are subjected to various types of attacks including jamming attack.

In our next semester we will show the result by simulation analysis. In order to simulate the proposed techniques, we used a discrete
event simulator named QualNet [14],

Reference:

[1] . James Carlson, Richard Han, Shandong Lao, Chaitanya Narayan, and Sagar Sanghani, "Rapid prototyping of mobile input devices using wireless sensor nodes", In *WMCSA'03*, Monterey, California, USA, October 2003.

[2]. A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless sensor networks for habitat monitoring", In *WSNA'02*, 2002.

[3]. W. Xu, T. Wood, W. Trappe, and Y. Zhang. "Channel surfing and spatial retreats: defenses against wireless denial of service", In Proceedings of the 2004 ACM Workshop on Wireless security, 2004, pp. 80 - 89.

[4]. A. Wood and J. Stankovic, "Denial of service in sensor networks", IEEE *Computer*, Oct. 2002, pp. 54–62.

[5] U. A. F. ARGUS, "Advanced Remote Ground Unattended Sensor Systems", Department of Defense Argus, http://www.globalsecurity. org/intell/systems/arguss.htm

[6]. Sherif Khattab, Daniel Mosse, and Rami Melhem, "Honeybees: Combining Replication and Evasion for Mitigating Base station Jamming in Sensor Networks", Parallel and Distributed Processing Symposium, April 2006, pp. 25-29

.

[7]. S.dasbit, R. Ragupathy ,"Routing in Manet and Sensor Network –A 3D position based approach", international journal of foundation of computing and decision Science,2008.

[8]. Amirita Ghosal, Subir Halder "Estimating Delay in a data forwarding schem for defending Jamming attack in wireless Sensor Network "

[9]. I.F. akyildiz, W. su, Y. Sankerasubramaniam, E.Cayirci, "A survey on sensor network",IEEE Communication 2002

[10] A.Wood , J. Stankovic , "Denial of service in sensor networks",IEEE Computer 2002

[11]Wenyuan Xu et. Al. "Jamming Sensor Network: Attack And Defense Strategies"

[12]. J. Polastre, J. Hill, and D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks," *SenSys '04: Proc. 2nd Int'l. Conf. Embedded Networked Sensor Sys.*, 2004, ACM Press, pp. 95–107.

[13] W. Xu *et al.*, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," *MobiHoc '05: Proc. 6th ACM Int'l. Symp. Mobile Ad Hoc Net. and Comp.*, 2005, pp. 46–57.

[14] A. Wood, J. Stankovic, and S. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks," *24th IEEE Real-Time Sys. Symp.*, 2003, pp. 286–97.

[15] Marga Nacher, Carlos T. Calafate, and Pietro Manzoni, "Multipath extensions to the DYMO routing protocol", Mobile Wireless Communications Networks, 9th IFIP International Conference, Sept. 2007, pp. 1 – 5.

[16] I. Chakeres, and C. Perkins, "Dynamic manet on-demand (dymo) routing", http://www.ietf.org/internetdrafts/ draft-ietf-manet-dymo-17.txt, March 2009