AN OVERVIEW OF JAMMING ATTACKS AND COUNTERMEASURES IN WSN

[1]Saylee Gharge, [2]Yash Desai, [3]Akshata More, [4]Bhakti Parab, [5]Saharsh Mindewar

[1]Associate Professor, [2]B.E. Student, [3]B.E. Student, [4]B.E. Student, [5]B.E. Student
Department of Electronics and Telecommunication
Vivekanand Education Society's Institute of Technology, Mumbai, India

Abstract: Wireless sensor networks provide a platform to collect and monitor data about a particular physical quantity. When Sensor nodes are deployed over a large area, they collect sensor data and transmit it to the sink node through wireless media. With large-scale deployments, security is becoming a vital concern in the WSN. Jamming attacks are a subgroup of Denial of service (DoS) attacks wherein the malicious nodes interfere with the network communication. The main contribution of this article is to discuss the types of jammers and jamming techniques. This paper describes the optimal placement of jammers and different existing technologies for localizing jammers in the network. Jamming detection techniques can remarkably enhance jamming protection only when used together with other countermeasures by providing valuable data. Some countermeasures of jamming include use of directional antennas instead of Omni-directional antennas and the application of high-transmission power on jammed channels providing less jamming.

***IndexTerms* - Wireless Sensor Networks, Jamming, Denial of Service, Placement of jammers, Countermeasures.**

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a spatially dispersed network of sensor nodes that record and monitor a particular physical quantity in the environment. A wireless sensor network's principal purpose is to serve as an interface to the real world, providing physical information to a computer system. The data can be observed and analyzed. It plays a crucial role in monitoring and recording sensitive information. A dense wireless network is formed, and the information gathered can be relayed through a network of nodes and be delivered to the destination. The data is transmitted to other nodes via multiple hops until it reaches its destination, referred to as the sink node. Each node has the responsibility of gathering data and forwarding it to the sink node. The sink is a powerful node with high-speed processing, ample storage, long-distance transmission, low-power consumption, and low cost [1]. Each node consists of a microcontroller unit, radio transceiver, and sensors. Wireless sensor networks are becoming more affordable and are consequently being deployed in various applications. With large-scale deployments, security is becoming a significant concern in the wireless sensor network.

Jamming is defined as the act of intentionally directing electromagnetic energy towards a communication system to disrupt signal transmission [2]. Due to electromagnetic energy being focused on the channel, communication is affected**.** It can result in the attacker expanding its network's capacity or destroying the network such that no packet transmission will occur. Moreover, jamming can lead to delay in packet transmission. Jamming attacks can be considered as a particular case of Denial of service (DoS) attacks which can hinder a network from performing its function [3]. The jamming effect of a particular jammer is determined by the strength of its radio transmitter, its location, and its impact on the targeted node. To make jamming more effective, a jammer can jam a network in diverse ways [4].

This paper's main objective is to provide an overview of jamming in wireless sensor networks and discuss the relevant countermeasures in detail. The remainder of this paper is organized as follows: Section II describes the types of jamming techniques. Section III briefs about types of jammers. Section IV illustrates the optimal placement of jammers to achieve effective jamming. Further, in Section V we investigate existing technologies for localizing jammers in the network. Section VI deals with various countermeasures used in detecting jamming in wireless sensor networks. Section VII concludes the paper.

II. TYPES OF JAMMING TECHNIQUES [2]

A. SCAN JAMMING

Here, the attacker scans every channel as thoroughly as possible to check if any activity is present. If the jammer discovers any radioactivity, it immediately initiates jamming. It is very effective when frequency hopping is used as a countermeasure. However, the hopping rate of the attacker must be significantly higher than the victim. Scan jamming is most successful if the transmitted messages are long enough to be intercepted, giving the jammer more time to scan all the channels. An attacker's reactive jamming message does not commence until the sender has stopped transmitting and hopped to another channel if the fragments are short enough [2].

B. PULSE JAMMING

Here, the attacker blindly jams on a single channel in short pulses. Hence, the packet's fragments that are using the current channel will get corrupted, which is enough to cause the drop of the entire packet. Due to this, pulse jamming can achieve excellent results in WSNs with limited communication channels available for frequency hopping [2].

C. SPOT JAMMING

This is the most famous jamming method. Here, the attacker directs all its transmitting power on a single frequency that the target uses with the same modulation and enough power to rescind the original signal. The main drawback of this jamming technique is that since it jams a single frequency each time, spot jamming may easily counter it by changing to another frequency, known as frequency hopping.

D. SWEEP JAMMING

Here, a jammer shifts its full power rapidly from one frequency to another. This method can jam multiple frequencies intermittently, but it does not affect all of them simultaneously, which reduces its effectiveness. However, in a WSN environment, it can cause considerable packet loss and retransmissions and, hence, consume valuable energy resources [2].

E. BARRAGE JAMMING

In this method, a range of frequencies is jammed at the same time. It reduces the Signal-to-Noise Ratio of the receivers by jamming multiple frequencies simultaneously. However, the output power of the jamming is decreased proportionally as the range of the jammed frequencies increases.

F. DECEPTIVE JAMMING

When the jammer does not want to reveal its existence, deceptive jamming is used. Deceptive jamming can either be applied on a single frequency or a set of frequencies. It fills the network with fake data and hence tricks the defence mechanism involved in the network. Deceptive jamming can flood the entire network with useless or fake data, which misleads the WSN's operator and occupies the available bandwidth used by the legitimate nodes without being detected.

III. TYPES OF JAMMERS

Jammers are malicious wireless nodes planted by an attacker**,** which causes deliberate interference in a wireless network. The jamming effect of a jammer varies according to its radio transmitter power, location, and influence on the network or the targeted node. Depending upon its functionality, a jammer can be either elementary or advanced. The elementary jammers can be divided into two sub-groups: proactive and reactive jammers. Function-specific and smart-hybrid are advanced ones.

A. ELEMENTARY JAMMERS

1. Proactive Jammers

It jams the signal whether any data communication is taking place or not. It operates only on a single channel and functions till it contains energy [3]. One particular channel is targeted at a time and packets of random bits are sent on this channel, while all the other nodes are put on non-operating modes. It uses all its energy to jam only one channel. There are three basic types of proactive jammers: constant, deceptive, and random [4].

Constant Jammers: Constant jammer emits continuous, random bits without following the CSMA protocol. According to the CSMA mechanism, a legitimate node has to sense the status of the wireless medium before transmitting. Constant jammer emits continuous, random bits without following the CSMA protocol. According to the CSMA mechanism, a legitimate node has to sense the status of the wireless medium before transmitting. Only after a DCF (Distributed Coordination Function)Inter Frame Space (DIFS) period of inactivity is the medium intended to continue its transmission. If the channel is found transmitting or receiving during this DIFS interval, the station should delay its transmission. Hence, the nodes are prevented from communicating with each other as the channel is constantly busy. The radio signals emitted by the jammer are similar to the signals that are produced by sensor nodes so that interference can be produced which keeps the network busy and results in jamming [3].

Deceptive Jammers: Unlike a Constant jammer, which transmits random bits, this jammer continuously transmits regular packets. Other nodes are made to believe that a transmission is taking place and so they remain in the same receiving states till the jammer is turned off.

Random Jammers: Random Jammers are capable of transmitting both packets as well as random bits. It focuses on energy saving, and hence it alternates between its two states, i.e., jamming and sleeping phase. It jams for a significant amount of time and then sleeps for a specific time before jamming again. It can behave like either a constant jammer or a deceptive jammer [5]. Different levels of effectiveness and power-saving can be achieved by changing the jamming time and sleeping of the jammer. We can alter the ratios between sleeping and jamming time to adjust the settlement between efficiency and effectiveness.

2. Reactive Jammers

The reactive jammer scans the channel, and once it senses any activity, it immediately sends out a random signal to corrupt the existing transmitting packets on the channel. They wait for transmission in the network, and once it senses any transmission, it starts producing interference in the network and focuses on energy efficiency. As it has to continuously monitor the network for any activity, it is less efficient as compared to a random jammer.

RTS/CTS Jammers: The RTS/CTS jammers star/t jamming as soon as it perceives a request-to-send (RTS). It starts interfering with the channel to a point where the receiver will not return the clear-to-send (CTS) because the RTS packet sent from the sender is distorted. Hence, the sender will not send any data because it thinks that the receiver is busy with some other transmission. The jammer can also jam the CTS after the RTS is received.Againthe sender will not send any data because it did not receive the CTS.

DATA/ACK Jammers: These jammers do not start jamming until a data transmission starts at the transmitter's end. They jam the network by corrupting acknowledgment packets or the transmitted information. Data/Acknowledge jammers can give rise to two scenarios: first, when the data packets are corrupted, the correct information is not received by the receiver, and second, being that the sender does not receive the acknowledgment message. In both cases, the information has to be retransmitted.

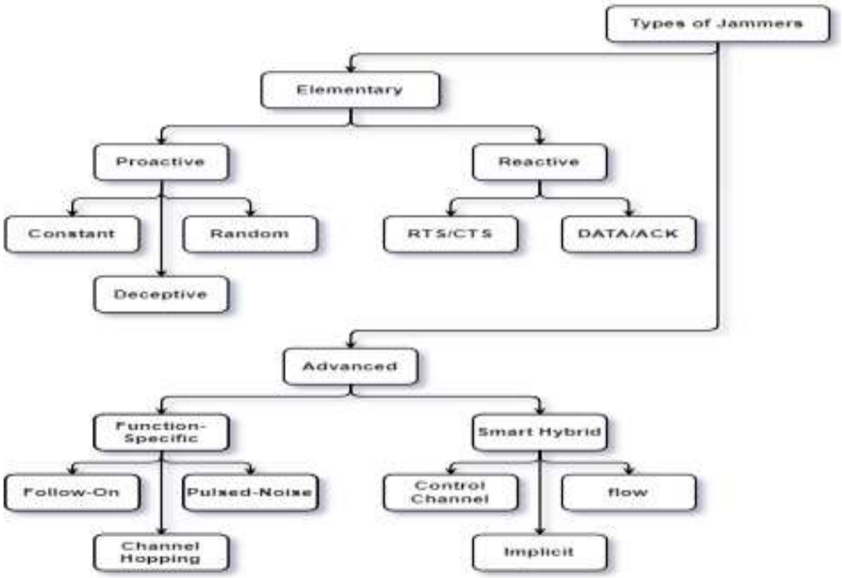

Figure 1: Types of Jammers

B. ADVANCED JAMMERS

1. Function Specific Jammers

As the name suggests, these jammers are made to perform a specific task. They can jam a single channel or cause the whole network's jamming depending upon their application. And in this way, Function Specific Jammers can be used to either provide maximum throughput or be energy efficient. They can change their targeted channel even when they are jamming a channel.

Follow-on Jammers: Jammers of this kind jam a single frequency at a time and then hop to various frequencies at different times. Assume a node hears jamming at onefrequency and jumps to a different one. In that case, these types of jammers will either scan the channel again and hop on the frequency used by the sensor nodes, causing interference, or they will spontaneously hop (thousands of times per second) and jam different frequencies. [3]

Channel Hopping Jammers: By countermanding the Carrier-Sense-Multiple-Access (CSMA) algorithm, it can directly access the channels. Apart from jamming more than one channel consequently, these jammers, as the name suggests, can hop from one channel to another dynamically following a pseudo-random sequence.

Pulse Noise Jammers: By swapping their target channels, Pulsed noise jammers will perform its jamming on different bandwidths at different times. These jammers can save energy when turned on and off by modifying the timing of their program. But unlike the random jammers, which jam only one channel at a time, pulsed-noise jammers can jam multiple channels.

2. Smart Hybrid Jammers

They are termed ‘smart' because they are powerand jamming effectiveand ‘hybrid' because they can be used as proactive as well as reactive. In vast networks, these jammers apply an accurate amount of energy at a specific node which obstructs the communication for the entire network [4].

Control Channel Jammers: In multi-channel networks, these jammers organise network operation by jamming the primary or control channel. When this control is targeted by a random jammer, it reduces the network functioning whereas, if it is targeted by a continuous jammer, the access to the whole network may be prevented.

Implicit Jammers: Implicit jamming attacks damage the functioning of the target node which causes a state of DoS at other nodes. Since the Access Point is forced to invest more time on the weaker node, rate adaptation is harmed. When a jammer jams a specific node, the rate adaptation effect causes the Access Point to concentrate on that node, causing other nodes to wait and slowing the entire operation.

Flow Jammers: These types of attacks are possible when multiple jammers are jamming the network. The jammer jams a packet in a centralised control attack by measuring the minimum power available to jam it. A non-centralized jammer model, on the other hand, allows each jammer to exchange data with its neighbour nodes in order to increase performance.

IV. Placement of Jammers

The placement of jammers plays a crucial role in jamming a particular network. Jammers can be placed randomly or placed in a location that is best suited to accomplish the attacker's desired objective. In this section, we will analyse various placements of jammers.

***Optimal jamming attacks**:* In [6], a scenario is being created where a jammer jams an area in a single channel WSN. The jammer controls the probability of jamming and transmission range to cause maximum destruction to the network. It is described that the chance of jamming is high if the attacker is aware of the network and transmission powers. Also, the jammer must know network channel access probabilities and the number of neighbours to the node. Suppose if a particular part of the network is jammed, the node is expected to send a jamming notification out of the area. It was proved by the authors using a probability of distribution and mathematical proof that this strategy can have long-term effects on the network.

Nanosize jammers: [4] Suggests the use of tiny, low-power jammers. They are challenging to detect as they are not visible to the naked eyes. The results show that they provide superior performance as compared to the traditional jammers. The number of jammers required in the network can be increased, leading to a reduction in jamming power and keeping the power consumption constant.

***Jamming under complete uncertainty**:* [7] considers the case where the attacker has no prior knowledge about the network. They assume a square-shaped area enclosing the network where the jammers are placed on the nodes of a uniform grid over an area of interest. Upper and lower bounds are derived for the optimal number of jamming devices and later convergence results are provided. It is also assumed that jamming devices have omnidirectional antennas which emit electromagnetic waves in all directions where jamming power decreases inversely to the squared distance from a device. This approach proves that it is more efficient than covering an area with circles.

***DSS for locating VHF/UHF Jammer**:* With the help of a decision support system, it is possible to determine a location where a jammer system should be placed so that it can jam the maximum area. The jammer should be placed at an optimum location to destroy the communication capability of the target system. It is assumed that there is line-of-sight between the jammer and target systems, and the signal power of the jamming system is higher than the signal power of the target system. The maximum covering model is used for this purpose and is solved with the LINGO-8 package. The locations for deploying jammers can be obtained by providing information on target points and jamming systems [8].

V. Jammer Localization

Centroid Localization: Centroid Localization uses placement information of all neighbouring nodes. These nodes are generally placed within the transmission range of the targeted node. It gathers all coordinates of jammed nodes and averages their coordinates to determine the estimated location of the jammer. Centroid Localization is robust against radio propagation uncertainties but is extremely sensitive to the distribution of jammed nodes. It will provide accurate results for a uniformly distributed network but seems inappropriate for the uneven distribution of nodes in a network [9].

***Weighted Centroid Localization**:* Weighted Centroid Localization is an enhanced version of Centroid Localization. It helps to estimate the location of the target node by calculating the weighted average. The weight value is added to the process of estimating the target node location. For example, we can consider the distance between a jammer and a jammed node. The idea is that a jammed node that is close to a jammer should impart more to the average location estimation than a jammed node far away. Weighted Centroid Localization shows a better estimation than Centroid Localization [9].

***Virtual Forces Iterative Localization (VFIL)**:* Centroid localization and Weighted Centroid Localization are extremely sensitive to the distribution of the jammed nodes and the network density. Hence, the VFIL approach is proposed to achieve better localization accuracy. The concept of virtual forces is used to estimate the jammer’s position based on the changes in the network topology. After each iteration, few nodes will fall inside jammed areas, while a few will fall outside. The jammed nodes located outside the estimated jammed region should pull the jammed region toward themselves. In contrast, the other nodes within the estimated jammed region should push the jammed region away from them [9].

***Exploiting Neighbour Changes**:* The paper suggests a Least-Squares (LSQ)-based localization algorithm that estimates the jammer’s location by utilizing the changes of neighbour defense nodes caused by jamming. The location is calculated based on the changes in a node’s hearing range. It is usually assumed that the initial hearing range of the node is acquainted with us before the jammer starts its operation. This approach does not measure signal strength inside the jammed area, nor does it require delivering information out of the jammed area. Hence, this algorithm works well in scenarios where network communication is intermittent [10].

VI. Detection and Countermeasures

A. Detection of a jamming attack: *[5]*

The first step towards building a dependable and secure wireless network is detecting jamming attacks. Jamming detection techniques can remarkably enhance jamming protection only when used together with other countermeasures by providing valuable data. A two-phase strategy includes the diagnosis of jamming attacks, followed by a defense strategy to deal with the jamming problem. The first strategy includes the jammer avoiding in either the spatial or spectral sense. This can be accomplished by changing allocations of channels by moving nodes away from the jammer. The second strategy competes with the jammer. It can be done by adjusting employing error correction and transmission power levels to have large flexibility against jamming.

1. Basic Statistics

Carrier Sensing Time: A jammer prevents a source from sending out packets. It is because the channel may appear busy constantly to the source. Hence carrier sensing time is used to determine whether a device is jammed.

Signal Strength: Jamming detection is also be done using Signal strength. Therefore, two natural approaches are used that include comparing average signal magnitude vs threshold which are calculated from noise levels and classifying a signal sample window shape.

Packet Delivery Ratio: This is used to detect the presence of jamming attacks because the transmissions can be effectively corrupted by the jammer. This leads to a much lesser PDR. It is a more powerful statistic than carrier sensing time and signal strength. It can be used to differentiate a jamming attack from a congested network scenario for different jammer models. The basic statistics are not enough for categorizing the presence of a jammer. Therefore, more advanced detection methods are required.

2. Advanced Detection Strategies

The signal strength is less than PDR, while the jammed case gives the signal strength, which should be high. This contradicts that the PDR is less. Because of this, a multimodal consistency check is defined.

Mapping Jammed Areas: Mapping out the regions of the jammed sensor network is advisable for the network. Network services can affect routing, higher-layer planning, and power management. The regions are jammed, as the channel utility observed by the sensors is below a preset threshold. After that, the jammed nodes temporarily bypass their MAC layer and broadcast JAMMED messages by announcing that those messages are jammed. Other jammed neighbours are not be able to receive these JAMMED messages. Non-jammed nodes exchange and merge information which describes nodes as jammed. The network is in the end map out the boundary of a jammed area by continuing the exchange of information regarding witnessed jammed nodes.

3. Evasion Defense Strategies

There are two strategies to protect against jamming attacks: channel surfing and spatial retreats. The idea behind each strategy is to avoid the interferer in either the physical or spectral sense.

Channel Surfing: It is inspired by frequency hopping modulation. Unlike frequency hopping, a PHY layer modulation method involves continuous changing of the carrier frequency. Due to this, the changing of frequencies in channel surfing is in demand. It operates at the link layer.

Spatial Retreats: In spatial retreats, jammed nodes try to move out from jammed regions. They are suitable for mobile sensor networks. Escaping from a jammed region is not enough. Large swaths are caused to relocate as a mobile adversary can move through the coverage area. Spatial retreat strategy has two phases:

a. The escape phase is when the nodes which are located within the jammed area move to "safe" regions. It stays connected with the rest of the network.

b. The reconstruction phase is the phase in which mobile nodes move about to accomplish uniform network coverage. It ends by preventing the jammer from partitioning the network.

Competition Strategies:(Code Throttling and Power Control). There is an alternative to have the sensors that try to compete in opposition to the jammer to perform evasion strategies. In this, the sensors improve the packets' reception reliability.

B. Countermeasures against Jamming:

1. ***Regulated Transmitted Power****:* Low transmission power reduces discovery probability from an attacker. High transmitted power implicit high resistance in opposition to jamming. Original signal has overcame by the stronger jamming signal [11].
2. ***Frequency-Hopping Spread Spectrum****:* It is a method of transmitting radio signals by quickly switching a carrier among numerous frequency channels, using a shared algorithm known both to the transmitter and the receiver [11]. FHSS reduces jamming of radio transmission and unauthorized interception between the nodes. The SNR of the carrier gets lower as a wider range of frequencies is used for transmission. It deals successfully with the multipath effect.
3. ***Direct Sequence Spread Spectrum****:* DSSS transmissions are carried out by multiplying the data which is being transmitted and a Pseudo-Noise (PN) digital signal. This causes RF signals to be replaced with wide bandwidth signals [12]. At the receiving end, PN can be filtered out to recover the original data. This can be done by multiplying the same PN modulated carrier with the incoming RF signal.
4. ***Hybrid FHSS/DSSS****:* This type of communication between WSN nodes represents an optimistic anti-jamming measure [12]. The direct-sequence systems accomplish their processing gains through interference attenuation by using a wider bandwidth for signal transmission but frequency hopping systems through interference avoidance.
5. ***Ultra Wide Band Technology***: It is a modulation technique based on simultaneously transmitting very short pulses on a wider frequency band. This gives the transmitted signal to be jammed. This provides resistance to multipath effects. In WSNs, UWB can provide more advantages.

6. ***Antenna Polarization***: The polarization of an antenna is the orientation of the electric field of the radio wave regarding the earth's surface. It is determined by the orientation of the antenna and its physical structure [13]. In jamming environments, the antenna polarization of nodes plays a significant role. This makes a remarkable difference in signal quality to have the transmitter and receiver using the same polarization for line-of-sight communications. But the jamming process gets disrupted by the change of nodes’ polarization of WSN. This is because it makes it necessary to use specialized jamming equipment to change its signal polarization during jamming quickly.
7. ***Directional Transmission***: Omnidirectional antennas are typically used by today’s sensor nodes. The directional antennas significantly improve jamming tolerance in WSNs. Directional antennas protect in opposition to detection, eavesdropping, and jamming than omnidirectional transmission [13][14]. A directional antenna transmits or receives radio waves only from one specific direction. On the other hand, an omnidirectional antenna transmits and receives radio waves from all directions simultaneously. It increases the transmission performance, receiving sensitivity, and reduces interference from unwanted sources compared to omnidirectional antennas.

VII. CONCLUSION

In this paper, a detailed introduction about Wireless Sensor Networks and the most harmful jamming attacks along with their countermeasures is given. This paper also studied the extensive details about the jamming techniques and different categories of attackers like proactive, reactive, and function-specific, which brief us about the technologies used in jamming and related research work.Different types of jammers attack wireless networks in several ways so that their jamming effects are significantly divergent. For instance, a constant jammer continuously jams the network, but it is easily detected. On the other hand, a reactive jammer attacks only when a certain condition is satisfied. In short, a powerful jammer will surely jam most of the networks but can be easily detected.

We also investigate the placement of jammers which is considered to help make jamming more effective. No matter which type of jammer is used, there is always an equivalent anti-jamming technique. Various countermeasures against jamming techniques have also been studied, like the use of spread spectrum technologies, the polarization of antennas, and the advantages of using directional antennas. Although accurately detecting jammers is the most important job of an anti-jamming system, energy efficiency should be considered for low-powered networks, for example - sensor networks.

While it is possible to detect a jammer, predicting the type of detected jammer is still a concern. Moreover, anti-jamming is extremely difficult in mobile networks and IEEE 802.11n networks due to the nodes' mobility. If these technologies are used appropriately, they can help develop a defense mechanism against the most sophisticated attacks.

REFERENCES

[1] Yang Lv, Yu Tian, “Design and application of sink nodes for Wireless Sensor Network”, 2010 2nd International Conference on Industrial and Information Systems, September 07, 2010.

[2] Aristides Mpitziopoulos, DamianosGavalas, Charalampos Konstantopoulos, GrammatiPantziou, “A Survey on Jamming Attacks and Countermeasures in WSNs”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 4, FOURTH QUARTER 2009, December 01, 2009.

[3] SunakshiJaitly, Harshit Malhotra, Bharat Bhushan, “Security Vulnerabilities and Countermeasures against Jamming Attacks in Wireless Sensor Networks: A Survey”, 2017 International Conference on Computer, Communications and Electronics (Comptelix) Manipal University Jaipur, Malaviya National Institute of Technology Jaipur & IRISWORLD, July 01-02, 2017.

[4] Kanika Grover, Alvin Lim, Qing Yang, “Jamming and anti-jamming techniques in wireless networks: a survey”, International Journal of Ad Hoc and Ubiquitous Computing, December 2014.

[5] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang, Rutgers University, “Jamming Sensor Networks: Attack and Defense Strategies”, IEEE Network, May/June 2006.

[6] M Li, I. Koutsopoulos, R. Poovendran, “Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks”, IEEE INFOCOM 2007 - 26th International Conference on Computer Communications, May 2007.

[7] Clayton W. Commander, Panos M. Pardalos, ValeriyRyabchenko, Oleg Shylo, Stan Uryasev, GrigoriyZrazhevsky, “Jamming communication networks under complete uncertainty”, Springer, January 2007.

[8] CevriyeGencer, EmelKizilkayaAydogan, Coskun Celik, “Decision support system for locating VHF/UHF radio jammer systems on the terrain”,Springer, September 6, 2007.

[9] Hongbo Liu, Wenyuan Xu, Yingying Chen, Zhenhua Liu, “Localizing Jammers in Wireless Networks”, IEEE International Conference on Pervasive Computing and Communications, 2009.

[10] Zhenhua Liu, Hongbo Liu, Wenyuan Xu, Yingying Chen, “Exploiting Jamming-Caused Neighbor Changes for Jammer Localization”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 3, MARCH 2012.

[11] Anthony. D. Wood and John. A. Stankovic, “Denial of service in sensor networks”, IEEE 2002.

[12] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, “Theory of spread spectrum communications-a tutorial”, IEEE Transaction on Communications, May 5, 1982.

[13] W. Stutzman, G. Thiele, “Antenna Theory and Design”, (2nd edition), John Wiley & Sons, 1997.

[14] Akis Spyropoulos, C.S. Raghavendra, “Energy-Efficient Communications in Ad Hoc Networks Using Directional Antennas”, IEEE INFOCOM 2002.