Effective Network Defense Strategies to Maximize System Survivability of Wireless Mesh Networks under Malicious and Jamming Attacks

Frank Yeong-Sung Lin
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
yslin@im.ntu.edu.tw

Yu-Shun Wang
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
d98002@im.ntu.edu.tw

Jing-Wei Wang
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
r98045@im.ntu.edu.tw

Chi-Hsiang Chan
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
r99049@im.ntu.edu.tw

***Abstract*—Continuity of wireless networks is a critical issue for wireless networks. Unfortunately, there is a category of attacks that seriously threatens the continuity of wireless networks: the jamming attack. The open nature of wireless mediums makes them vulnerable to any wireless capable devices.**

However, there have not been any studies that address the issue of how the service providers should deploy its topology or allocate its resources to minimize the impact of jamming attacks launched by malicious attackers.

In this paper, a mathematical model formulating an attack-defense scenario of the problem is proposed. The results show when deploying defense resources, considering hops from the core node is more useful than link degrees. With the advantage of simulations, the concept of incomplete information can be taken into account which, while increasing the difficulty of the problem, makes the problem closer to reality.

Keywords: Network Attack and Defense, Wireless Mesh Networks, Jamming Attack, Network Survivability, Resource Allocation, Mathematical Programming, Honeypots, Incomplete Information

I. INTRODUCTION

Owing to the convenience and increasing importance of wireless networks, service providers have to deal with a variety of wireless threats. Unfortunately, there is a category of attacks that seriously threatens the continuity of wireless network, which is called a jamming attack. Currently, although there are several approaches to ease the impact of jamming, their effectiveness is limited by several constraints. Previous studies [1] have classified the countermeasures of jamming attacks into attack mitigation and attack prevention, and most of them involve mitigation techniques.

It is clear that there are two major difficulties for jamming prevention. First, the open nature of the medium makes it vulnerable to any wireless capable devices which are able to access the medium once they are located in each other's transmission range. Second, the channel has already been jammed by the time the defender is aware of the presence of a jamming attack. As such, since there is no indication before a jamming attack is launched, attack prevention is not an easy task.

Since the impact of a jamming attack cannot be intuitively avoided, why don't we remove the jammers? The localization of wireless devices is not a brand new idea. There have been many studies on localization, such as using trilateration and trigonometric measurement, but the idea of jammer localization has not been addressed until recent years. There are two main categories of localization techniques. As will be mentioned in [2-4], signal processing localization techniques require special, additional hardware to achieve their goal, such as ultrasound, infrared or laser infrastructures. The other category of received signal strength (RSS) based techniques require measurement of the RSS and have to deliver the information out of the jammed area. The techniques of both categories thus have some limitations.

However, till now there has not been any research addressing the issue of how service providers should deploy nodes or allocate defense resources to minimize the impact of jamming attacks from malicious and jamming attackers.

Thus, we consider an attack-defense scenario in a wireless mesh network in which the defender attempts to maintain the level of quality of service when attackers try to launch malicious attacks and jamming attacks to maximize service disruption. Both defender and attackers have budget constraints and various strategies to choose from.

In this paper, we proposed a mathematical model to formulate the scenario and solve the problem using heuristics and then evaluate the processes as well as suggest a policy enhancement procedure. Our objective is to formulate effective topology planning and defending strategies to maximize system survivability, so as to provide a guideline for service providers.

II. RELATED WORKS

A. *Survivability*

Demands for metrics to describe the ability of a system to provide services in abnormal conditions arose with the growing dependence on a certain kind of application system. The issue of survivability was first studied in the military since the failure of its systems could result in lethal consequences. Though survivability has been applied to a variety of fields, such as computer, network, ecological and biological systems, the definition of survivability has not been unified and remains unstandardized.

In contrast to the formulation mentioned above,

978-1-4673-4794-5/12/$31.00 ©2012 IEEE

there is another method to measure survivability, which is called the "Contest Success Function" (CSF) [5-7]. The idea of CSF originates in economic theory and describes a function-based model in which the winning probability of the participants in a contest is a function of all the players' efforts [7]. In [6, 8], the concept of vulnerability, which is the success probability of the attacker, is determined by the ratio form of the CSF. Generally, the attackers which allocate more resources on the object have a higher probability of success.

B. Deception Based Mechanisms

A computer system designed to deceive malicious attackers to improve the current network system's security can be called a deception-based mechanism. The objective may be learning the behavior of attackers [9-12], acting as a false target [1, 9-13], or wasting the resources of the attackers [1, 13].

Generally, the function of deception-based mechanisms in wireless networks is no difference to those in wired networks. Yet, Misra *et al.* proposed a novel technique which uses deception-based resources to prevent wireless communication channels from being jammed, which offers a new way to enhance the robustness of wireless networks.

C. Jamming Attacks

Generally speaking, a jamming attack can be viewed as a special case or subclass of denial of service (DoS) attacks [1, 14]. The objective of such attacks focuses on the interdiction of any communication on the targeted channels or a range of frequency. Most of the network types of previous research which address the problem of jamming attack are wireless sensor networks (WSNs). The probable reason is that WSNs have been used in many safe-critical systems, such as the monitoring of patients or children [14]. Therefore, the survivability requirement of these systems increases because "*in such systems even a temporal disruption of the proper data stream may lead to disastrous results*" (A. Mpitziopoulos, *et al.*[14]). However, as jamming attacks may happen in any category of wireless network, regardless of the category of wireless network, the threat of jamming attacks should not be ignored. W. Xu*, et al.* had reviewed a wide range of jammers cases and provided a summary [15] which listed four types of jammers that have proven to be effective.

D. Jamming Countermeasures

The general approach of jamming countermeasures includes three steps: attack detection, attack prevention and attack mitigation [1]. It has been pointed out, however, that existing attack mitigation techniques have a number of limitations (S. Misra*, et al.* [1]). Spatial Retreat [16], for example, requires jammed nodes to physically move away from the jammed region; in Jammed-Area Mapping [17], as jammed-area will be mapped out, part of the network will be inoperable. As for; channel Surfing [1], on the other hand, while being able to provide service with minimal service disruption and additional requirements compared to the former techniques, is unlike Spread Spectrum techniques in that it does not have to consume a large amount of bandwidth. In addition, it can be applied to both wireless infrastructure and wireless infrastructure-less (ad–hoc) networks.

S. Misra*, et al.* proposed an attack prevention technique in [1]. "*We define honeynodes as secondary interfaces present on base-stations which guard the frequency of operation of the actual communicating nodes by sending out a fake signal on a nearby frequency to prevent the attack by deceiving the attacking entity to attack the honeynode.*" Though the technique does prevent jamming attacks in some cases, the effectiveness greatly depends on the behavior of jammers and the number of jammers in the network.

E. Jammer Localization

The localization of jammers provides some additional strategies for network operators. As described in [4], the effect of jamming can be neutralized through human intervention, or by providing information for routing protocols to redesign a route that avoids jammed areas. Generally, there are two restrictions of jammer localization: First, the requirement of extra hardware [2-4]; and second, disturbed network communications makes it impossible to transmit a signal out of jammed areas.

To address these difficulties, K. Pelechrinis*, et al.* proposed a lightweight jammer localization technique in [2], which is based on the idea that "*Packet Delivery Ratio* (*PDR) has lower values as we move closer to the jammer*". But this approach only seeks out the locations of nodes which reside on the boundary of the jammed range, and is unable to precisely indicate the location of the jammers. On the other hand, range-free approaches, such as Centroid Localization (CL) and Weighted Centroid Localization (WCL), do not rely on the property of received signals. The positions of jammers are derived from the position of jammed nodes. However, this makes them extremely sensitive to node density [4]. H. Liu*, et al.* proposed a novel approach, Virtual Force Iterative Localization (VFIF), which is less sensitive to node density. In this approach, another category of nodes is recognized as being useful in jammers' localization, called boundary nodes. Here, "*A boundary node is not jammed, but part of its neighbor is jammed*."[4].

This idea is further extended in [3]. The proposed algorithm uses a least-squares approach (LSQ) to localize the jammer by exploiting the hearing ranges of the jammed nodes based on a free space propagation model. In their simulation results, the mean error of the jammers' locations falls between 1 meter and 3 meters, which is far more accurate than VFIF.

III. Problem Formulation

A. Problem Description

For service providers, it is extremely important to ensure the quality of service received by its customers. Thus, in this work, the problem of a jamming attack in a

wireless mesh network will be addressed. There are two roles in this problem: the defenders and the attackers. As defenders, the service provider deploys an infrastructure based wireless mesh network to provide service.

Since the attackers' objective is to gather the topology information of the network and launch a jamming attack to disrupt service provision, the defenders have to reasonably allocate their resources, including both non-deception-based resources and deception-based resources, to maintain the level of QoS. In addition, the attackers have different attacking strategies according to their goals.

Attackers will be able to maximize the effect of the jamming attack if they have complete information of the network. However, this is not possible in the real world. Consequently, they may try to gather information of the network by compromising devices. In general, the actions of attackers can be classified into two stages: a "Preparing Phase" and an "Attacking Phase". The Preparing Phase is the stage in which attackers try to collect information from the network, whereas the Attacking Phase is when attackers launch the jamming attack.

Similarly, the defenders will try to deploy their resources to minimize the effect of the jamming attacks launched by the attackers. In the "Planning Phase", the defender deploys its resources. In most cases, when the defenders are aware of the presence of jamming attacks, the QoS level has already declined. As a consequence, the defenders must deploy defense resources before jamming attacks occur. Therefore, the defenders will deal with node compromising attempts and the impact caused by jamming attacks in the "Defending Phase". The time sequence of the phases is illustrated in Figure 1. In order to clearly detail this problem, the perspectives of the defenders and attackers will be discussed in following sections.

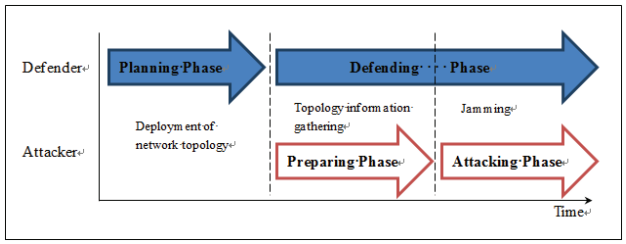

Figure 1 Period of the Defenders and Attackers

B. Problem Formulation

We model the attack and defense scenario as a mathematical formulation. The given parameters and decision variables are shown in table 1 and 2.

Table 1 Given Parameters

Given Parameter	
Notation	Description
N	The index set of all nodes
C	The index set of all base stations
H	The index set of all honeynodes
Q	The index set of the nodes equipped with locators
R	The index set of the nodes equipped with a population re-allocation function
B	The defender's total budget
Z	All possible attack configurations, including attackers' attributes and corresponding strategies
E	All possible defense configurations, including defense resource allocation and defending strategies
F	Total attacking times of all attackers
$\overline{A_i}$	An attack configuration, including the attributes and corresponding strategies, where $1 \le i \le F$
$a(\varphi_i)$	The cost of constructing static locators with the density φ_i, where $i \in N$
$h(\varepsilon_i)$	The cost of constructing a honeynode with the interactive capability ε_i, where $i \in H$
$t(\rho_i)$	The maximum traffic of node i with quality ρ_i, where $i \in N$
o	The cost of constructing one base station
p	The cost of constructing one mesh router
b	The cost of constructing a population re-allocation function to one node

Table 2 Decision Variables

Decision Variable	
Notation	Description
$\overline{D}$	The information regarding resources allocation and defending strategies
w_i	1 if node i is equipped with a honeynode function, and 0 otherwise, where $i \in N$
x_i	1 if node i is equipped with a localization function, and 0 otherwise, where $i \in N$
y_i	1 if node i is equipped with a population re-allocation function, and 0 otherwise, where $i \in N$
n_i	The non-deception-based defense resources allocated to node i, where $i \in N$
e	The total number of mesh routers
ε_i	The interactive capability of honeynode i, where $i \in H$
φ_i	The density of locator near node i, where $i \in N$
ρ_i	The quality of node i, where $i \in N$
$B_{defending}$	The budget of the defending phase
B_{node}	The budget of constructing nodes
$B_{proactive}$	The budget of allocating proactive defense resources
$B_{reactive}$	The budget of allocating reactive defense resources
$B_{honeynode}$	The budget of constructing honeynodes
$B_{locator}$	The budget of constructing locators
$B_{population}$	The budget of constructing a population re-allocation function
$T_i(\overline{D}, \overline{A_i})$	1 if the attacker can achieve his goal successfully, and 0 otherwise, where $1 \le i \le F$

Objective function:

$$\min_{\overline{D}} \frac{\sum_{i=1}^{F} T_i(\overline{D}, \overline{A_i})}{F} \qquad \text{(IP 1)}$$

Subject to:

$$\overline{D} \in E \qquad \text{(IP 1.1)}$$

$$\overline{A_i} \in Z \qquad 1 \le i \le F \qquad \text{(IP 1.2)}$$

Budget constraints:

$$B_{node} + B_{proactive} + B_{reactive} + B_{defending} \le B \quad \text{(IP 1.3)}$$

$$B_{honeynode} + B_{locator} + B_{population} \le B_{reactive} \quad \text{(IP 1.4)}$$

$$p \times e + o \times \|C\| \le B_{node} \quad \text{(IP 1.5)}$$

$$\sum_{i=1}^{N} n_i \le B_{proactive} \quad \text{(IP 1.6)}$$

$$\sum_{i=1}^{H} w_i \times h(\varepsilon_i) \le B_{honeynode} \quad \text{(IP 1.7)}$$

$$\sum_{i=1}^{Q} x_i \times a(\varphi_i) \le B_{locator} \quad \text{(IP 1.8)}$$

$$\sum_{i=1}^{R} y_i \times b \le B_{population} \quad \text{(IP 1.9)}$$

$$p \times e \ge 0 \quad \text{(IP 1.10)}$$

$$n_i \ge 0 \qquad \forall i \in N \quad \text{(IP1 11)}$$

$$h(\varepsilon_i) \ge 0 \qquad \forall i \in H \quad \text{(IP 1.12)}$$

$$a(\varphi_i) \ge 0 \qquad \forall i \in N \quad \text{(IP 1.13)}$$

$$t(\rho_i) \ge 0 \qquad \forall i \in N \quad \text{(IP 1.14)}$$

$$b \ge 0 \quad \text{(IP 1.15)}$$

Integer constraints:

$$w_i = 0 \text{ or } 1 \qquad \forall i \in N \quad \text{(IP 1.16)}$$

$$x_i = 0 \text{ or } 1 \qquad \forall i \in N \quad \text{(IP 1.17)}$$

$$y_i = 0 \text{ or } 1 \qquad \forall i \in N \quad \text{(IP 1.18)}$$

Explanation of the objective function:

We formulate the problem as the following minimization problem. IP 1 is our objective function, which is a function of probability. The probability is modeled as the total success times of the attackers divided by the total attack times. Our objective is to obtain a configuration which effectively reduces the probability of the attackers.

IV. Solution Approach

A. Monte Carlo Simulation

The problem discussed in this paper is hard to be solved purely by mathematics since there are too many factors which are not deterministic, such as the probability of using a certain category of strategies to compromise nodes, the probability of being deceived by false target, and the probability of compromising nodes. Therefore, in order to obtain an effective solution, we adopt an evaluation process to measure the effectiveness of defense configurations.

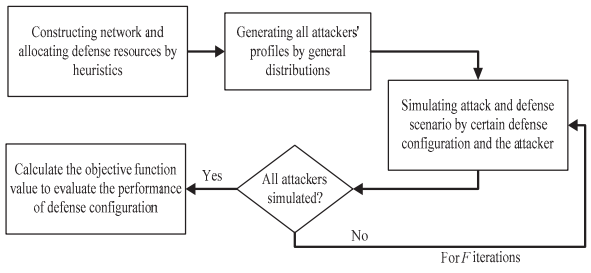

Figure 2 Monte Carlo Simulation Process

At the beginning of the process, a defense configuration is generated by heuristics and the attackers' profiles are derived by general distributions. Then the performance of the initial configuration is evaluated for F times, which allows the defender to obtain the compromise probability of a certain configuration. The total attack times F, which is sufficient for the probability to converge, is derived by the subsequent experiments. The process is represented in Figure 2.

B. Initial Allocation Scheme

Clearly, different resource allocation schemes will lead to diverse evaluation results. In this section, we will illustrate our initial allocation heuristics. For wireless service providers, the distribution of users is of the greatest importance. However, since we may not be able to acquire this information in advance, we consider two other important factors which can be derived instantly from the topology: the number of hops from core nodes and the link degree.

- **Number of hops from core nodes**

The number of hops to core nodes is an important factor when considering security issues. The risk level of core nodes increases when attackers are approaching since the chance to reach the core nodes becomes higher.

- **Link degree**

The attackers gain direct information from the nodes which contain a larger amount of traffic and sources since they provide clues to important targets. Generally, the nodes with the most traffic and sources are BSs which are already protected by the factor of hops from core nodes. Consequently, we take the nodes with a high link degree into consideration since they have higher probability to contain more information about the topology.

V. Computational Experiments

In this section, we will illustrate the details and an analysis of our computational simulations, including the simulation environment, initial resource allocation, and simulation results.

A. Simulation Environment

The source code is written in C language, and the program was executed on several virtual machines with Intel quad-core CPUs. There are three categories of topology applied in our simulation, consisting of grid, scale-free and random network types. Along with the scale of topology, the defenders have a different number of nodes, BSs, and budget. Other topology and defender related information is illustrated in Table 3.

Table 3 Parameters for Defenders

Parameters	Value		
Topology Type	Grid		
	Scale-Free		
	Random		
Topology Scale	1	2	3
Number of Nodes	9	25	49
Number of Services	1	1	1
Number of Core Nodes	2	4	9
Defense Budget	500,000	1,000,000	1,700,000

Node Distance	60~150 meter
SNR Threshold	1.5

To address the property of all possible categories of attackers, the attackers' capability, aggressiveness and budget are determined by normal distributions, and their behavior are modeled by goals and corresponding strategies which have already been detailed in the problem description. The lower bound and upper bound of the normal distributions are listed in Table 4.

Table 4 Parameters for Attackers

Parameters	Value
Total Budget	300,000 ~ 1,500,000 (Normal Distribution)
Capability	0.00001 ~ 1 (Normal Distribution)
Aggressiveness	0.00001 ~ 1 (Normal Distribution)

B. Experiment Results

➢ **Convergence experiment**

Before starting the evaluation, we must gain knowledge of a sufficient number of attacking times for the process to converge. Figure 3 depicts an experiment result, with the vertical axis depicting the compromise probability of the service, and the horizontal axis illustrating chunk number. Each chunk contains 500 attacking times.

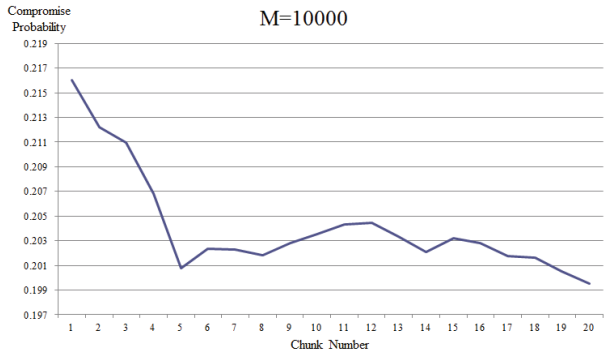

Figure 3 Convergence Experiment for 20 Chunks on a 9-Node Grid Network

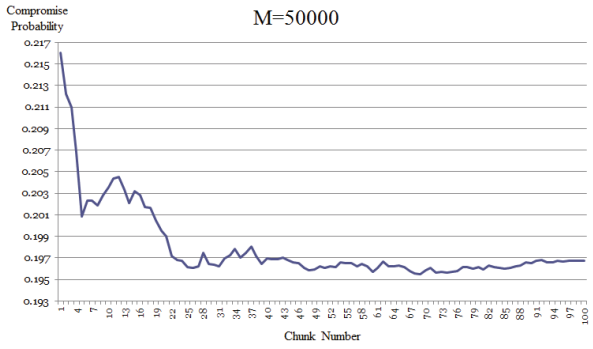

Figure 4 Convergence Experiment for 100 Chunks on a 25-Node Random Network

As it is not possible that the evaluation process converges in 20 chunks (10,000 times) due to the probability change being still greater than 0.2%, we then ran a second evaluation of 100 chunks (50,000 times) and noted that the evaluation process seemed to converge in 100 chunks as illustrated in Figure 4. Therefore, we set the convergence number M as 100 chunks (50,000 times).

➢ **Performance evaluation**

Simulations are conducted under scale-free topology to compare the performances of different ratios of initial allocation factors. Evaluation results are shown in Figure 5. Value 0.1 on the horizontal axis means the initial allocation ratio of hops from core node factor is 0.1, and ratio of link degree factor is 0.9. Every single point on the figures is an evaluation result of 100 chunks. Figure 5 illustrates the results for the scale-free topology.

As we can see, the compromise probability decreases with the ratio of link degree. This indicates that, for the defender, the factor of hops from core nodes is more important than link degree factor.

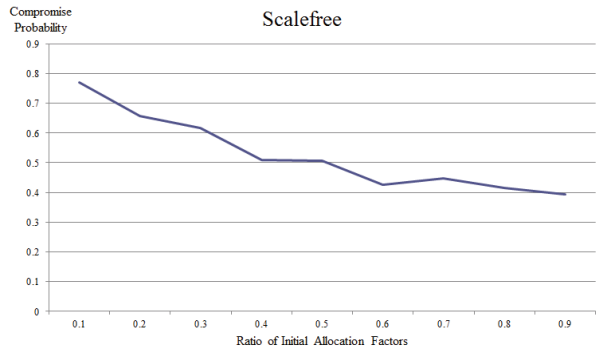

Figure 5 Performances of Different Initial Allocations in a 25-Node Scale-Free Network

C. Discussion of the results

According to the simulation results, it can be concluded that: the factor of hops from core nodes is more effective on defense resource allocating.

In the attack and defense scenario considered in this paper, the attackers can arbitrarily choose a node as the starting point. Therefore, the key to success for attackers depends on how many hops they have to make.

For high link degree nodes, targeting them does not guarantee high service compromise probability since those nodes may only connect to core nodes. Therefore, for the defender, it is much more effective to allocate defense resources according to number of hops from core nodes rather than by link degree.

VI. Conclusions and Future Work

In this paper, an attack defense scenario with a non-deterministic characteristic is modeled into mathematical formulation. Corresponding solutions are derived from a Monte Carlo Simulation. Further, meaningful defense strategy is proposed.

For defenders, the factor of hops from core nodes is more effective than the link degree factor. For future work, different types of defense resource allocation can be taken into consideration and other types of reactive defense mechanisms can be involved in the scenario.

References

[1] S. Misra, *et al.*, "Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks," *Computers & Electrical Engineering,* vol. 36, pp. 367-382, 2010.

[2] K. Pelechrinis, *et al.*, "Lightweight Jammer Localization in Wireless Networks: System Design and Implementation," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 2009, pp. 1-6.

[3] Z. Liu, *et al.*, "Wireless Jamming Localization by Exploiting Nodes' Hearing Ranges," in *Distributed Computing in Sensor Systems*. vol. 6131, R. Rajaraman, *et al.*, Eds., ed: Springer Berlin / Heidelberg, 2010, pp. 348-361.

[4] H. Liu, *et al.*, "Localizing jammers in wireless networks," in *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*, 2009, pp. 1-6.

[5] K. Hausken and G. Levitin, "Protection vs. false targets in series systems," *Reliability Engineering & System Safety,* vol. 94, pp. 973-981, 2009.

[6] G. Levitin and K. Hausken, "False targets efficiency in defense strategy," *European Journal of Operational Research,* vol. 194, pp. 155-162, 2009.

[7] S. Skaperdas, "Contest success functions," *Economic Theory,* vol. 7, pp. 283-290, 1996.

[8] P. E. Heegaard and K. S. Trivedi, "Network survivability modeling," *Computer Networks,* vol. 53, pp. 1215-1234, 2009.

[9] S. Xing, *et al.*, "Honeypot Protection Detection Response Recovery Model for Information Security Management Policy," *Asian Social Science,* vol. 6, December 2010.

[10] C. K. Dimitriadis, "Improving Mobile Core Network Security with Honeynets," *IEEE Security and Privacy,* vol. 5, pp. 40-47, 2007.

[11] M. Sink. *The Use of Honeypots and packet Sniffers for Intrusion Detection*. Available: http://www.lib.iup.edu/comscisec/SANSpapers/msink.htm

[12] H. Debar, *et al.*, "White Paper: "Honeypot, Honeynet, Honeytoken: Terminological issues"," Institut Eurécom Research Report RR-03-081September 2003.

[13] L. Spitzner, *Honeypot: Tracking Hackers*: Addison-Wesley.

[14] A. Mpitziopoulos, *et al.*, "A survey on jamming attacks and countermeasures in WSNs," *Communications Surveys & Tutorials, IEEE,* vol. 11, pp. 42-56, 2009.

[15] W. Xu, *et al.*, "Jamming sensor networks: attack and defense strategies," *Network, IEEE,* vol. 20, pp. 41-47, 2006.

[16] W. Xu, *et al.*, "Channel surfing and spatial retreats: defenses against wireless denial of service," presented at the Proceedings of the 3rd ACM workshop on Wireless security, Philadelphia, PA, USA, 2004.

[17] A. D. Wood, *et al.*, "JAM: a jammed-area mapping service for sensor networks," in *Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE*, 2003, pp. 286-297.