2013 IEEE 27th International Conference on Advanced Information Networking and Applications

Maximization of Wireless Mesh Networks Survivability to Assure Service Continuity under Intelligent Attacks

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

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

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

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

***Abstract*—Service continuity is a critical issue in wireless networks. Unfortunately, jamming attacks seriously threatens the continuity of wireless networks. The open nature of wireless mediums makes it vulnerable to any wireless capable devices.**

There are only few researches 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 core node is more useful than link degree. With the advantage of simulations, the concept of incomplete information can be taken into account which though raises the difficulty of the problem, but 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

As a result of the convenience and increasing importance of wireless network, service providers have to deal with a variety of wireless threats. There is a category of attacks that seriously jeopardies the continuity of wireless network, which are jamming attacks. Currently, there are several approaches to alleviate the impact of jamming although many constraints have to be fulfilled. Previous works [1] have classified the countermeasures of jamming attack into attack mitigation and attack prevention, most of them are mitigation techniques.

There are two major difficulties of jamming prevention. First, the open nature of the medium makes it vulnerable to any wireless capable devices. Second, the channel had already been jammed when the defender aware of the presence of jamming attack. There is not any symptom before jamming attack launched. As a result, attack prevention is not an easy task.

Since the impact of jamming attack cannot be avoided, intuitively, removing the jammers becomes a great option. Localization of wireless devices is not a brand new idea. There had been many works of localization, such as 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. In [2-4], signal processing localization techniques require special, additional hardware to achieve the goal, such as ultrasound, infrared or laser infrastructures. Received signal strength (RSS) based techniques require measurement of the RSS and have to deliver the information out of the jammed area. Therefore, the techniques of both categories have some limits.

However, there are only few works address the issue of how the service providers should deploy nodes or allocate resources to minimize the impact of jamming attacks launched by malicious attackers.

Thus, an attack and defense scenario in wireless mesh network which the defender attempt to maintain the level of quality of service when attackers try to launch malicious attacks and jamming attacks to maximize service disruption is considered. Both defender and attackers have budget constraint and various strategies to choose.

In this paper, a mathematical model formulating the scenario is proposed. The problem is solved by heuristics and Monte Carlo simulations in evaluation process procedure. The objective is to find an effective topology and defending strategies to maximize system survivability, so as to provide guidelines for service providers.

II. Literature Review

A. Network Survivability

Describing the degree of ability of a system providing services under an abnormal condition is an important criterion. Survivability is one of the pioneer studies in military since the failure of military systems could be fatal. Though this metric has been applied to a variety of fields, such as computer networks, ecological and biological systems, the definition of survivability has not been unified. In this paper, the definition of survivability is the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents [5].

Many other works studying survivability [6-8] adopt the concept of "Contest Success Function" (CSF) to determine the outcome of an attacker launching a malicious attack on the target node. The idea of CSF is

1550-445X/13 $26.00 © 2013 IEEE
DOI 10.1109/AINA.2013.31

originated from economy theory. It models the success probability of participants in a battle as a function of all players' efforts [8]. In [7, 9], the vulnerability which is the success probability of the attackers, is determined by $\frac{A^m}{A^m + D^m}$, where A means the efforts attackers invested and D stands for the resources deployed by the defender. The parameter m represents contest intensity. If $m<1$, the contest is under "fight to win or die" circumstance; while $1 \le m \le \infty$, the effectiveness of resources invested by both players is exponentially increasing; when $m \to \infty$, the contest is under "winner takes all" circumstance [6-8]. Generally, the attackers allocating more resources on the target have higher success probability.

B. Deception Based Defense Mechanisms

A computer system designed to deceive malicious attackers to improve the current network system survivability is one of deception mechanisms. Learning the behavior of attackers [10-13], act as a false target [1, 4], or waste the resources of attackers[1, 14] are possible objectives.

In wireless networks, generally, there is no difference of the function of deception mechanisms between wired and wireless networks. Yet, S. Misra*, et al.* [1] proposed a novel technique which applies deception based resources to prevent wireless communication channel from being jammed, this provides a new manner to enhance the robustness of wireless networks.

C. Malicious Jamming Attacks

Jamming attack can be viewed as a subclass of denial of service (DoS) attacks [1, 15]. The objective of such attacks focuses on interdiction of any communication on the targeted channels or a range of frequency. Most of the network types of previous researches which address the problem of jamming attack are wireless sensor networks (WSNs). The reason is probable that WSNs have been used in many safe-critical systems, such as monitoring of patients or children [15]. Therefore, the survivability requirement of these systems are raised since "*in such systems even a temporal disruption of the proper data stream may lead to disastrous results*" [15].

Nevertheless, jamming attacks may exist in any category of wireless networks. Thus, no matter what type of wireless network is, the threat of jamming attacks should not be ignored. W. Xu*, et al.* had reviewed a wide range of jammers and provided a summary [16] which listing four type of jammers that have been proven to be effective.

D. Jamming Countermeasures

The general approach of jamming countermeasures includes three steps, attack detection, attack prevention and attack mitigation [1].

Detection of jamming attacks can be done through observing quality of service. If there are lots of unreachable mesh routers in the same neighborhood, the probability of being jammed is high.

S. Misra*, et al.* [1] 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 case, however, the effectiveness greatly depends on the behavior of jammers and the number of jammers in the network.

Existing attack mitigation techniques have some limitations as S. Misra*, et al.* stated in [1]. Spatial Retreat [17] requires jammed nodes to physically move away from the jammed region. In Jammed-Area Mapping method [18], jammed-area will be mapped out. Thus, part of the network is inoperable. Channel Surfing, as stated in [1], is able to assure service continuity with minimal service disruption and additional requirement comparing to former techniques. Unlike Spread Spectrum techniques, Channel Surfing does not have to consume a large amount of bandwidth. In addition, it can apply to wireless infrastructure and wireless infrastructure-less (ad –hoc) networks. Consequently, this technique is widely applied.

E. Jammer Localization Schemes

Localization of jammers provides some addition strategies for network operator. In [4], the effect of jamming can be neutralized through human intervention, or provide information for routing protocols to redesign a route that avoids jammed areas. Generally, there are two restrictions of jammer localization: First, requirement of extra hardware [2-4]. Second, disturbed network communications makes it impossible to transmit signal out of jammed areas.

To address these difficulties, K. Pelechrinis*, et al.* proposed a lightweight jammer localization technique [2], which based on the idea "*PDR has lower values as we move closer to the jammer*". But this approach only finds out the locations of nodes which reside on the boundary of jammed range, which is not able to precisely indicate the location of jammers.

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 method 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 which are useful in jammers' localization, boundary nodes, is recognized. "*A boundary node is not jammed, but part of its neighbor is jammed*." [4].

This idea is further extend from [3]. The proposed algorithm uses least-squares approach (LSQ) to localize the jammer by exploiting jammed nodes' hearing ranges

based on free space propagation model. In their simulation results, the mean error of 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 assure the quality of service. Thus, in this work, the problem of jamming attack in wireless mesh network is addressed. There are two roles, the defender and attackers, in this problem. For the defender, deploying mesh routers to construct an infrastructure based wireless mesh network is the first step before providing services.

Since attackers' objective is to jam the network, before doing that, topology information gathering is a critical task. Accordingly, the defender has to appropriately allocate defense resources, both deception based and non-deception based resources, to maintain the level of QoS. In addition, attackers have different attacking strategies corresponding to distinct goals.

On the contrary, to maximize the effect of jamming attack, attackers have to gather topology information first. Obtaining complete information of target network before launching jamming attack is not realistic. Consequently, figuring out the spread of mesh routers and related defense information by compromising devices is an essential step. In general, attackers' actions can be classified into two periods: "Preparing Phase" and "Attacking Phase". The former is the stage in which attackers try to collect information from the network; then attackers launch jamming attack in Attacking Phase.

Likewise, the defender tries to deploy defense resources effectively to minimize the effect of jamming attacks. "Planning Phase" is the stage for the defender to deploy resources before attackers invade the network. In most cases, when the defender is aware of the presence of jamming attacks, the QoS level has already declined. As a result, defense resources have to be deployed before jamming attacks occurring. Hence, not only node compromising attempts but also the negative effects caused by jamming attack are serious problems for the defender to handle in "Defending Phase".

The time sequence of those phases mentioned above is illustrated in figure 1. In order to clearly detail the attack and defense scenario addressed in this paper, both defender and attacker's perspectives are discussed in following sections respectively.

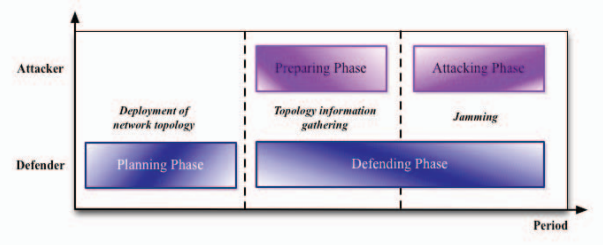

Figure 1 Period of the Defender and Attackers

➢ **Defender Perspective**

In this paper, infrastructure-based network is the main concern, and the security issue of jamming attacks in WMNs is addressed. In order to provide service as well as maintain the QoS level, there are four types (but not limit to) of nodes in the network environment, including base stations (BSs), mesh routers, honeynodes and jammer locators.

The usage of defense budget in Planning Phase is not only to construct the nodes mentioned above but also to deploy three categories of defense resources:

- **Topology planning:**
  The defender has to spend part of the finite budget to build the BSs, purchase mesh routers and deploy them in the field for providing services.

- **Non-deception based defense resources planning:**
  Decisions made in this category of resources including proactive defense resources and localization resources. Proactive defense resources stand for techniques that prevent nodes from being compromised, such as firewall, antivirus software and introduction protection system (IPS). Localization resources mean those can be applied to localize the jammers.

- **Deception based defense resources planning:**
  This category of resources is not only capable to deceive attackers and jammers but also waste attack resources. Mitigating the impact as well as reduce the duration of jamming attacks in wireless networks is another purpose.

➢ **Defending Strategy**

In defending phase, there are two strategies, which are population re-allocation and jammer removing. The former strategy can reduce the effect of jamming attack. When the defender knows that there is an attacker who tried to compromise a certain node, he/she can re-allocate the population on the target and its neighbors to ease the negative effect caused by the jamming attack.

As for jammer removing, there is a sub-decision to make, which is the priority of jammer removing. There are two possible heuristics, importance oriented and difficulty oriented. The intention of importance oriented strategy is to retrieve QoS level. The defender determines the sequence of jammer removing by the importance of corresponding jammed nodes despite of the complexity of the network environment. Regarding difficulty oriented strategy, however, the defender removes the jammers according to the difficulty of jammer removal.

➢ **Attacker Perspective**

For describing attackers, several attributes are considered, including budget, capability, aggressiveness, goal, strategy and preference.

- **Budget**
  To maximize the impact of jamming attacks, Acquisition of the information regarding topology and

defense resources allocation is the primary task. Owing to limited budget, the balance of allocating resources on node compromising and jammer purchasing is important.

- **Capability**

This attribute stands for how good an attacker is on attacking. The capabilities of compromising nodes, seeing through false targets and fake routing table information are taken into consideration.

Experienced attackers are more skillful in node compromising. In addition, they are more likely to penetrate if the compromised node is a honeynode. While the attacker aware of the gained information might be artificial, they can choose not to make decision depending on it or try to act in reverse.

- **Aggressiveness**

Aggressiveness describes the degree of risk acceptance for an attacker. Generally, an attacker which is risk tolerant is more likely to take chances on uncertainty. For instance, he may spend less on each attempt of node compromising attempt in spite of the fact the probability of success is much lower. On the other hand, attackers who tend to avoid risk will spend more to ensure the outcome. In other words, aggressiveness is the wanted compromise success probability of an attacker.

➢ **Goal, Strategy and Preference**

The behaviors of attackers are complicated since every single decision depends on their goal, strategies, preference of next hop selecting criteria, information gathered and the network environment at the instants. In this paper, some possible goals and strategies are considered for attackers:

- **Goal**

Maximizing attack effectiveness and maximizing jammed range are two different goals. The attackers pursuing the first goal tend to increase the difficulty of jammer removal to maximize attack effectiveness. Thus, they prefer to buy high quality jammers and spend more resources on compromising nodes which may contain valuable information, such as those with high defense strength or with high traffic amount.

As for attackers chasing for maximizing jammed range, they do not care the effectiveness of jammers; As a result, they purchase lots of cheap jammers and try to jam as many nodes as possible. In this case, they are less willing to spend large amount of budget on node compromising.

- **Strategies**

The effectiveness of jamming attack is affected by strategies of the defender as well as attackers. As Fred Cohen said [19], "*Attackers can select from many techniques for their attacks*", but the problem is when and which technique they should choose. Consequently, based on [19], several possible strategies are summarized for attackers in attacking phase, including aggressive, least resistance, stealthy, easiest to find, topology extending, and random strategies.

Attackers applying aggressive strategy prefer to compromise nodes with high defense strength since those are more likely to be important nodes. Regarding utilizing least resistance strategy attackers, they target nodes which are easiest for them to compromise. In this case, ideal nodes may be those with low defense resources.

Some attackers choose to conceal themselves to avoid being detected. They prefer to apply stealthy strategy. The ideal nodes are those with low traffic rate since they are seldom used.

As to easiest to find strategy, its characteristic is to choose the most obvious node, such as high traffic or signal strength. In such way, the attackers can spend less time on searching for next victim.

The purpose of topology extending strategy is to extend its knowledge of underlying topology for further decision making, for instance, to predict the real location of the BSs.

Some attackers just try whatever they happen to come across as an idea on any given day. This is called random strategy.

In attacking phase, initially, the attackers are able to gain some "Surface Information" through the wireless medium, such as defense strength, signal strength or traffic amount to make preliminary decisions. Attackers then apply different strategies to achieve their goal. With different strategies, corresponding preference of next hop selecting criteria are distinct. For example, an attacker who tends to maximize jamming effectiveness may choose "Aggressive" strategy since he believes the nodes with highest defense strength must contain valuable information.

On the other hand, attackers preferring "Easiest to find" strategy just selects the nearest node. Others who don't consider the quality of attacking tool may try to use a cheap one to attack as many victims as possible. Therefore, they prefer "Least resistance", "Stealthy" and "Topology extending" strategies.

Later on, attackers confront the problem of which nodes should be jammed. In attacking phase, attackers determine targets to jam by "Depth Information" which gathered from compromised nodes. Basically, the effect of jamming attack becomes significant when the number of jammed users increases.

B. Problem Formulation

The problem of minimizing the attacker's success probability is modeled as a mathematical formulation. Given parameters and decision variables are shown in table 1 and table 2 respectively.

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 locator
R	The index set of the nodes equipped with population re-allocation function
B	The defender's total budget
Z	All possible attack configuration, including attacker's attributes and corresponding strategies
E	All possible defense configuration, including defense resources 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 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 honeynode function, and 0 otherwise, where $i \in N$
x_i	1 if node i is equipped with localization function, and 0 otherwise, where $i \in N$
y_i	1 if node i is equipped with 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 defending phase
B_{node}	The budget of constructing nodes
$B_{proactive}$	The budget of allocating proactive defense resource
$B_{reactive}$	The budget of allocating reactive defense resource
$B_{honeynode}$	The budget of constructing honeynodes
$B_{locator}$	The budget of constructing locators
$B_{population}$	The budget of constructing 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:

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

Subject to:

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

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

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:

The attack and defense scenario is formulated as a minimization problem. IP 1 is the objective function, which represents the attackers' success probability. The numerator is attackers' total success times divided by the denominator which is the total attack times. The objective is to obtain a configuration which effectively minimizes system compromise probability.

IV. Solution Approach

A. Monte Carlo Simulation

Since the attack and defense scenario discussed in this paper is non-deterministic, it is quite difficult to solve purely by mathematics, for example, the probability of applying certain category of strategies to compromise nodes, likelihood of being deceived by false targets and uncertainty of compromising nodes. Hence, in order to obtain an effective solution, Monte Carlo simulation is adopted to measure the effectiveness of defense configurations.

At the beginning, a defense configuration is generated by heuristics and attackers' profiles are derived by general distributions. The next step is to evaluate the performance of the initial configuration for F times; it

allows the defender to obtain the compromise probability. The total attack times F, which is sufficient for the probability to converge is derived through subsequent experiments. The whole process is represented in figure 2.

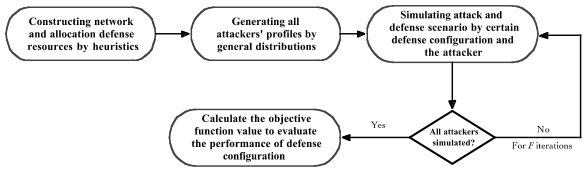

Figure 2 Monte Carlo Simulation Process

B. Initial Allocation Scheme

Obviously, different resource allocation schemes lead to diverse results. In this section, Initial allocation heuristics are discussed. For wireless service providers, the distribution of user is one of the most important issues. However, it is almost impossible to acquire this information in advance. As a consequence, two other important factors which can be derived instantly from the topology are proposed:

- **Number of hops from core node**

Hops to core node is an important factor when considering security issues. The risk level of core nodes increases when attackers are approaching.

- **Link degree**

Attackers are able to gain information regarding attack direction from nodes containing large amount of traffic and sources since they provide clues to important targets. Generally, nodes with the largest amount of traffic and sources are BSs. Consequently, Link degree is a good metric since nodes with high link degree have higher probability to contain useful information about the topology.

V. Computational Experiments

In this section, detail information and analysis of our computational experiments are illustrated, including simulation environment, convergence experiment, and performance evaluations.

Compared to our previous work, the attack and defense scenario is much more complicated. In our former work, attack strategy in preparing phase is trivial. Attackers find next victim node without thorough considerations. As for this paper, attackers jointly take traffic amount (stealth and easiest to find strategy), signal strength (topology extending strategy) and quantity of proactive defense resources (aggressive and least resistance strategy) as metrics. All these diversities make our scenario more close to the real world.

Since these strategies describing attackers' behavior is not expressed in mathematical formulation, the math structure is similar to our previous work. But specifically, they are totally different; all these discrepancies result in $\overline{A_i}$ and $T_i(\overline{D}, \overline{A_i})$ are completely distinct from our previous work. Although the format is identical, there are huge variances inside.

Further, only scale-free topology is examined in our previous research. An analysis regarding grid topology and comparisons between scale-free and grid topology is proposed.

A. Simulation Environment

The source code is written in C language, and the program was executed on several machines with Intel quad-core CPU. There are three categories of topology applied in the simulation, which are grid, scale free and random network.

Along with the scale of topology, the defender has different number of nodes, BSs, and budget. Other topology and defender relating information are presented in table 3.

Table 3 Parameter for the Defender

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 attacker's capability, aggressiveness and budget are determined by normal distributions, and their behavior are modeled by goals and corresponding strategies which are described in problem description. The lower bound and upper bound of normal distributions are listed in table 4.

Table 4 Parameter 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 an evaluation, the sufficient number of attack times for the process to converge must be figured out. Figure 3 depicted an experiment result on a 49 nodes scale-free network. The vertical axis represents compromise probability of the service, and the horizontal axis illustrates chunk number. Each chunk contains 500 attacking times.

In the result of 160 chunks (80,000 times), which is depicted in figure 3, the probability change is less than 0.2% after 100 chunks. Therefore, the convergence number M is determined to 100 chunks (50,000 times).

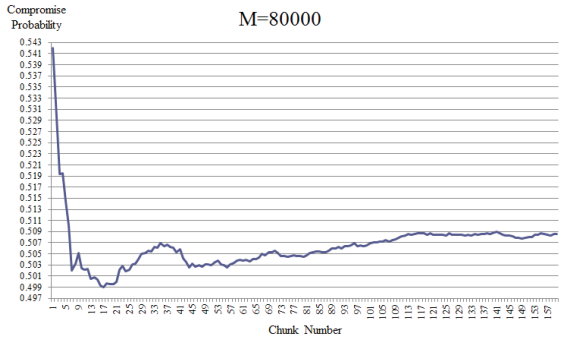

Figure 3 Convergence Experiment for 160 Chunks on a 49 Nodes Scale-free Network

➢ *Performance evaluation*

Two sets of simulations are constructed under the scale-free topology and grid topology to compare the performances regarding different ratios of initial allocation factors. The evaluation results are shown in Figure 4 and 5.

The 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 4 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 in the scale-free topology.

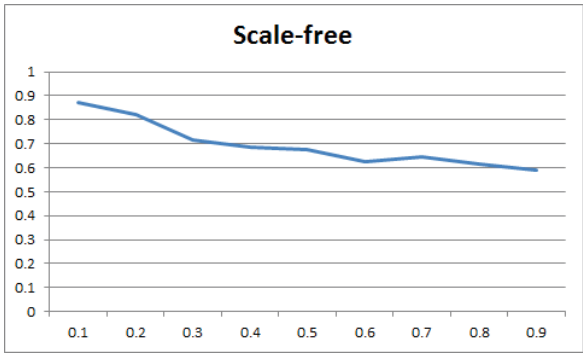

Figure 4 Performance of Different Initial Allocation in a 25 Nodes Scale Free Topology

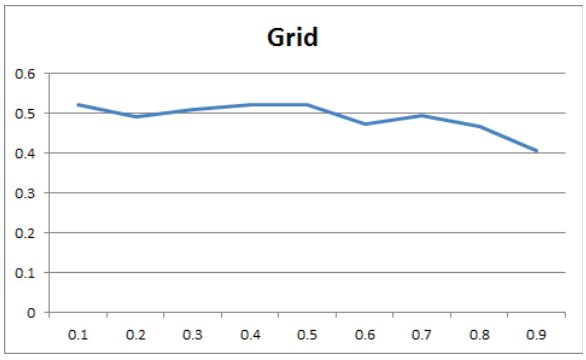

Figure 5 Performances of Different Initial Allocation in a 25-Node Grid Topology

Figure 5 shows the result in the grid topology. The trend depicted in Figure 5 is the same as in Figure 4. The compromise probability also decreases with the ratio of link degree. However, the change of probability is less than the one in scale-free network.

C. *Discussion of the results*

According to the results, the following defense guidelines are proposed.

➢ *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.

➢ *The improvement rate of compromise probability of the scale-free network is more significant than for the grid topology*

In scale-free networks, it is more likely that there are paths only have few hops to the core nodes. As a result, when considering hops from core nodes to allocate defense resources, those paths are strengthened, this will decrease the compromise probability of the core nodes.

On the other hand, the depth of grid topology is relatively stable. While applying the factor of hops from core nodes, there is a tendency to average the defense resources deployed on each node. Therefore, the improvement rate in grid networks is less significant.

➢ *The scale-free network is naturally more vulnerable than grid topology*

As shown in Figures 4 and 5, the compromise probability of the scale-free network is almost higher than the ones for the grid network for every case. This is because the depth of grid topology is much more stable than for the scale-free topology. There is no “easy way” for attackers to compromise the service; each route is nearly the same for the attackers.

However, the longer defense depth results in a poorer quality of service: the greater the number of hops legitimate users have to go through, the greater the delay or jitter they suffer. Therefore, how to balance security and quality of service is a dilemma for defenders.

VI. Conclusion and Future Work

In this paper, an attack defense scenario with non-deterministic characteristic is addressed. Corresponding mathematical formulation is also proposed. Solutions are derived from Monte Carlo Simulations. Further, meaningful defense guidelines are proposed.

For defenders, no matter what category the topology is, the factor of hops from core nodes is more effective than link degree. In addition, scale-free topology is more sensitive to the change of ratio regarding initial allocation than grid topology.

For future work, different types of defense resource allocation heuristics can be taken into consideration and other types of reactive defense mechanisms can be combined into the scenario.

Acknowledgment

This work was supported by the National Science Council, Taiwan, Republic of China (grant nos. NSC 101-2221-E-002-189).

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] R. J. Ellison, et al., "Survivable Network Systems: An Emerging Discipline," Technical Report CMU/SEI-97-TR-013, 1997 (Revised: May 1999).

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

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

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

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

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

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

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

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

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

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

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

[17] 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.

[18] 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.

[19] F. Cohen. *Managing Network Security: Attack and Defense Strategies*. Available: http://www.blacksheepnetworks.com/security/info/misc/9907.html