GAME THEORY AND NETWORK SECURITY:

ECONOMIC INCENTIVES AND BARRIERS

MARYAM ASGARIAZAD

A THESIS

IN

THE DEPARTMENT

OF

CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING

PRESENTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF MASTER OF APPLIED SCIENCE IN INFORMATION SYSTEMS

SECURITY

CONCORDIA UNIVERSITY

MONTRÉAL, QUÉBEC, CANADA

SEPTEMBER 2014

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Maryam Asgariazad**

Entitled: **Game Theory and Network Security: Economic Incentives and Barriers**

and submitted in partial fulfillment of the requirements for the degree of

Master of Applied Science in Information Systems Security

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Dr. A. Ben Hamza _____ Chair

Dr. J. Bentahar _____ Examiner

Dr. Walaa Hamouda _____ Examiner

Dr. A Youssef _____ Supervisor

Approved _____

Chair of Department or Graduate Program Director

_____ 20 _____ _____

Dr. Christopher Trueman, Dean

Faculty of Engineering and Computer Science

Abstract

Game Theory and Network Security: Economic Incentives and Barriers

Maryam Asgariazad

Nowadays, the Internet and computer networks play an increasing role in our modern society. However, we also witness new types of security and privacy incidents such as the propagation of malware, the growth of botnets, and denial-of-service (DoS) attacks against business and governments' websites. Therefore, experts must investigate security solutions to defend against these well-organized and sophisticated adversaries. Instead of designing a defence against a specific attack, game theory attempts to design a quantitative decision framework to determine the possibility of adversaries' attacks, and suggest defence strategies for the defenders. This thesis illustrates some examples for the potential usefulness of game theory in information systems security.

First, we present a game theoretic scenario to study the strategic behavior of two Internet Service Providers (ISPs) who have to decide whether to invest in deploying security technologies that detect and prevent malicious cyber-attacks. In particular, we consider the case where the ISPs can determine malware-infected machines among their subscribers, and their action (i.e., quarantining these infected machines) may well mitigate cyber security incidents. By analyzing the financial incentive for the ISPs to deploy security policy

among their subscribers, we find the best action of the ISPs considering their customers' security awareness and their market shares. We also identify the need for government regulations and incentives in order to better guide the role of ISPs in enhancing the global security of the Internet.

Then, we present a game theoretic model for analyzing the dynamic interaction between attackers and defenders as a two-player game with uncertainty while considering multi-level of detection for defence devices configurable by the defender and multi-level of severity for attacks chosen by the attacker. By assuming that higher levels of defence and high level of attack severity are associated with higher levels of investments by the defender and the attacker, respectively, we compute mixed strategy Nash Equilibria for both the attacker and defender considering the cases when the players' valuation follows a uniform distribution and the case where it follows a truncated normal distribution. We then formulate an n-player game to capture competition among n attackers who aim to successfully attack the same target and analyze the mixed strategy Nash Equilibria in both models.

Finally, we consider networks in which the worm propagator and the defender can dynamically decide their optimal propagation rate for the warm and security patches, respectively, considering their associated cost. We combine the propagation process with a game theoretic model as a two-player non-zero sum differential game. Then we formulate the decision problem as a continuous-time optimal control problem and solve it using the Pontryagin maximum principle. The obtained result leads to a better understanding of the worm propagator behavior and can be utilized to inhibit the scale of loss resulting from Internet worms.

Acknowledgments

I would like to express my gratitude to all the wonderful people who have contributed to this thesis and gave me the chance to accomplish a dream.

First and foremost, I am grateful to my supervisor, Dr. Amr Youssef, for giving me the opportunity to do research in a positive and stimulating environment, and above all, for showing me the way to conduct research. This dissertation would not have been possible without his suggestions, advice and support. Being a student of Dr. Amr Youssef packs me with pride and pleasure for my future career.

My warmest thanks to my family who has given me constant encouragement, support and inspiration.

Finally, I would like to thank my colleagues at CIISE for the great time we spent together and for their help and support.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In this chapter, we present a brief outline of our research work. First, we present our motivation for selecting this topic. After that, we present our objectives and contributions. Finally we conclude this chapter by presenting the organization of the remainder of this thesis.

1.1 Overview

Over the last decade, the Internet has been used across all industries to share information and conduct all kinds of communications and transactions between geographically distant resources and consumers. Unfortunately recent incidents in cyber security [37], [14], [22] prove that Internet attacks can cause huge amount of loss to governments, large organizations, home users, and all who rely on the Internet for their daily business in terms of

money, data confidentiality, and reputation. Traditionally, network security solutions employ defensive devices such as firewalls, Intrusion Detection Systems (IDSs), authentication servers or combination of all of them. Current defence technology may prove sufficient for defending against casual attackers, but there is still a need to design solutions to defend against sophisticated and well organized adversaries. The weakness of the traditional network security solutions is that they lack a quantitative decision framework. That is why security researchers have started advocating the utilization of game theory approaches. Since game theory deals with problems where multiple players with opposing purposes compete with each other, it can provide a mathematical framework for the analysis and modeling of network security problems in order to provide better insight into these problems.

1.2 Motivation

There are three legitimate players on the Internet that are confronted with security incident in different ways and the Internet security is greatly influenced by their behaviours. Their responses are motivated by specific incentives under which they decide and operate. These market players are home users, Internet service providers (ISPs), and network administrators in large organization. In the current network environment, cyber security is an interdependent security concept where actions and investment decisions of these market players impact the overall network security of the network of interconnected users. Given the sophistication and diversity of today's attacks, there is a demanding need to design a defence system and employ all the engaged players to counter attacks. Thus, we need

to study the motivations and barriers of all the engaged legitimate market players whose actions influence Internet cyber security.

Security Decision and Incentives for Home Users

A large portion of the machines in botnets are assumed to belong to home users and small and medium-size enterprise users who often do not achieve adequate levels of protection [17]. Combination of insufficient security knowledge and lack of incentive to take an action towards cleaning the infected computers by end users, are causing the Internet security to be impaired. End users usually do not realize that their machines are infected. Besides, they are unable to evaluate the relevant security risks and defence strategies. So they are not bearing the costs of their decisions to others. For instance, Anderson [39] stated that "while individual computers users might be happy to spend $100 on anti-virus software to protect themselves against attack, they are unlikely to spend even $1 on software to prevent their machine being used to attack a third party who is wealthy corporation". Thus, it has proven extremely difficult to improve the security of home users.

Security Decision and Incentives for Internet Service Providers (ISPs)

ISPs can play a critical role in the detection of malicious activities in the network and improving the Internet security. Although the traditional role of ISPs is to provide Internet access to end users, due to their topological position between the end users and the Internet, ISPs can observe all the traffic flowing into and out of their networks. Thus, based on the observed traffic, ISPs can determine malware infected machines among their subscribers.

Recent studies and security experts [5], [14] have suggested that ISPs can prevent, detect, and mitigate certain types of malicious cyber behavior, such as the operation of botnets on home users' computers. Obviously, the fact that ISPs can mitigate this does not mean they will do so. Under pressure from the government, in some countries, ISPs are now at least partially responsible for mitigating botnet activity in their own networks. For instance, Australia's largest ISPs have agreed on a voluntary code of conduct that includes contacting infected customers and filtering their connection [44]. Aside from the government interventions, we need to investigate the incentives under which ISPs are encouraged to take actions to improve the state of the Internet security. Thus, the following questions should be addressed: Is there any financial incentive for the ISP to take an action? Do users subscribe with the ISP who has restricted security policy? Does the service suspension of infected subscribes hurt the revenue of the ISP?

Our objective is to provide mathematical models that help analyzing and understanding the strategic behaviour of two ISPs in a competitive environment where they have the option to invest money for improving the Internet security according to their market share and security awareness of their subscribers.

Security Decision and Incentives for Network Administrators

Network administrators in large organization (public or private) spend a lot of effort to guarantee and maintain security of their information systems. In this, they set security policies to prevent attacks, perform tests to foresee future vulnerabilities, dictate responses to be taken in case of attacks, and lead recovery after security incidents. As security comes

at a cost, the incentive to deploy these actions is to avoid breaches of confidentiality, data integrity and therefore the brand damage and reputation effects. A study by Cavusoglu et al. [8] reported that an Internet security breach is negatively associated with the market value of the firm. Breached firms lost on average 2.1 % of their market value within 2 days of the announcement. Furthermore, in a large-scale network, the network administrator would face noticeably large number of threats such as DDoS attacks, intrusions, and malware spreading. Thus, network administrators adopt hundreds of security devices such as firewalls, Network Intrusion Detection Systems (NIDS) to defend their system against network-based attacks. Also, network administrators provide security policies to inhibit the propagation of malware in the network such as patching or spreading a special programs to clean infected computers.

The objective of a defence system is to be cost-effective, i.e., its cost should be less than the expected level of loss in the case of attacks or intrusions [27]. Thus, having a defence system requires assessing the cost-benefit trade-off between the information assets that are at risk and the cost of employing effective defence system. Additionally, intruders (attackers) are capable of launching attack with different aggressiveness which can be determined by the number of infected hosts participated in the attack session and amount of malicious traffic sent from them. Also, network administrators implement defence systems in their networks to detect malicious activities or policy violations and stop intrusion attempts. The objective is to adopt the practical defence setting while having a wildly configurable defence system with variety of detection levels in multi attacks network.

Different forms of malwares present threats against computer networks, so network administrator should provide proper countermeasure policy to inhibit worm spread and avoid the damage. Malware is commonly defined as a malicious software that is inserted into an information system, usually with the intent of compromising or disrupting the victim's system or other systems. Typical forms of malware include viruses, worms, trojans, key loggers, rootkits and malicious mobile code. Network administrators typically use various worm detection techniques such as Threat Monitoring Systems (TMS) to observer suspicious traffic among their network. With defensive systems in place, worms have consequently progressed and become more sophisticated. For instance, some worms deliberately reduce their propagation speed through the network to avoid detection [46]. After infecting a number of computers without being detected, the worm propagator can remotely control the infected computers and use them to launch further attacks such as distributed denial-of-service (DDoS), phishing, or spyware. For example, the "Code-Red" was programmed to unleash a denial-of-service attack on the Whitehouse.gov website by targeting the actual Whitehouse.gov IP address [41]. Despite using various warm- defence technique such as using Internet Threat Monitoring (ITM) systems to monitor suspicious traffic (e.g., scans unoccupied IP addresses or ports), it is essential to have additional defence strategy to inhibit the propagation of malware in the network such as performing patches to clean infected computers, and diminish the scale of loss and speed of worm propagation. Performing security patches as a defence strategy is a costly process. This motives the defender to vary the spreading rate of patching in order to find the trade-off between the operating costs and the loss caused by infectious hosts.

1.3 Objectives

In this thesis, we aim to investigate the incentives and strategic behaviour of ISP and network administrator as two market players who can mitigate the cyber-criminal activities and improve the overall security of the Internet. Specifically, we focus our efforts in two main areas, namely to deploy security technology by ISPs in order to detect the operation of botnets on home users' computers and the effect of network administrator in preventing cyber security incidents such as intrusion or malware propagation. To illustrate why our focus shifted from end users, who own most of the infected machines, to other parties, we discuss the following observation which is beyond information security. The decision by one apartment owner to install a sprinkler system will decrease his neighbours' fire risk and make them less likely to do the same. As a result taking protective measures creates positive externalities for others that in turn may discourage them from investment [4]. This insight has recently shifted the focus from end users to other market players which are Internet service providers (ISPs) and network administrators. It is important to note that we do not claim that end users are now freed from the responsibility of protecting their machines and keeping it secure against different forms of malware, but special attention should be paid to the efforts of the players such as ISPs and network administrators who could effectively function and control end user activities.

In particular, we first focus on mitigation of botnet activities and security incidents when ISPs implement different forms of security technologies to help them detect and monitor any malicious behaviour on their network and quarantine the infected machines. In this

case, the infected subscribers have only access to only Windows updates or a range of security services. We provide mathematical models that help analyzing and understanding the strategic behaviour and financial motives of two ISPs who have the option to invest in implementing the required technology to improve the Internet security considering their customers' security awareness and their market share.

Then we study the strategic behaviour of network administrators who plan to protect their networks against variety of malicious activities such as intrusions, attacks or malware spreading. In order to avoid these security incidents, security administrator uses configurable defence systems to provide a cost-effective and secured approach. Besides, to inhibit the worm propagation threat, performing patches to clean the possible infected machines seems to effectively reduce the worm propagation.

Although these defence approaches raise the maintenance costs, optimal cost effectiveness can significantly improve the cost saving for network administrators who aim to deploy the defence system. Thus we address this problem and assess the cost-benefit trade-off for effective defence approach against intrusions and malware spreading separately.

1.4 Contributions

In this thesis, we have achieved a set of contributions that can be summarized as follows:

- We investigate the financial incentive for identifying and quarantining the infected computers by ISPs in order to mitigate security incidents. We presented a game theoretic framework to analyze the strategic behaviour of two ISPs in deploying security

policies considering their customers' security awareness and their market share.

- We developed a game theoretic model to determine the best configuration of dynamic defence systems in order to prevent different attacks. The effective adopted defence system should balance security enforcement, deploying cost, and value of asset at risk. We also investigated the best strategy for the attacker seeing the accumulation cost of effective attack versus the reward of successful attack in competitive multi attackers' network.

- We modeled the interaction between the worm propagator who modifies the spreading rate to avoid detection where the defender performs patching to remove the worm from the infected machines and minimize the damage in the network. We combine biological epidemic model with differential game to dynamically derive the optimal spreading rate for the worm propagator and the defender.

The rest of this thesis is organized as follows. In Chapter 2, we introduce some preliminaries related to our work which include background about Internet security and ISPs investments' decisions, epidemiological frameworks of malware propagation, game theory and Pontryagin's maximum principle. In Chapter 3, we use game theory to represent interaction between two ISPs who have the option to deploy different security policies based upon the security threat they face, portion of infected hosts in the Internet, security awareness of their customers, and the behavior of other ISP. In Chapter 4, we model the interaction between attackers and defenders using a game theoretical framework, in

which both parties of the game seek to maximize their outcomes by investing in attack implementation (by the attacker) or defence system (by the defender) considering the value of the information asset at risk and the operation cost associated with their strategies. In Chapter 5, we use the biological epidemic model to analyze the interaction between the worm propagator and the defender in the network where they should dynamically decide their optimal propagation rate for the warm and security patch considering their associated costs. The problem is to find the continuous-time optimal control which can be formulated as a two-player non-zero sum differential game to compute the optimum decision of players. Finally, in Chapter 6, we conclude the research and give some suggestions for future research directions.

Chapter 2

Preliminaries

In this chapter, we present some preliminaries relevant to our work including security investment decision for the main network players including ISPs, and network administrators to prevent the cyber incidents such as intrusion and malware propagation. We then briefly review some game theory and Pontryagin's maximum principle (PMP) preliminaries to find the best possible decision of ISPs, network administrators, and attackers.

2.1 Game Theory

Game theory is a branch of applied mathematics and that is mainly used in economics, political science, psychology, and biology. In its origins, John von Neumann and Oskar Morgenstern [34] popularized the study of human behavior who are making strategic decisions with the assumption that these decisions were based on rationality. A game refers to any social situation involving two or more individuals called players. Within a game,

players perform actions that they choose from their individual action sets. The plan of actions that a player takes during a game play is called the strategy of that player. When all players play their strategies, their joint actions lead to outcomes in the game. An outcome gives a payoff to each player. Being rational, each player tries to choose the strategy that maximizes her own payoff. Different models of games have been considered, depending on what kind of interaction the players have and how much they know about each other. That is, when each player knows her action set and payoff as well as the other players' action sets and payoffs, the game is defined as complete information games whereas in incomplete information games, players are unaware of the possible actions or payoffs of other players.

Each game model considers a solution concept that determines the outcome of the game and its corresponding strategies. Nash equilibrium is the most famous concept of game solutions [36]. A Nash equilibrium is a set of strategies of the game in which no single player is willing to change her strategy if the strategies of the other players are kept fix. If the equilibrium strategy describes a particular action for each player, then we refer to it as a pure strategy equilibrium. Pure strategy equilibria do not always exist. We call an equilibrium a mixed strategy equilibrium when equilibrium is achieved by randomizing the choice of actions on the action set. Formally, a pure strategy is defined as a deterministic choice of action, while a mixed strategy chooses a probability distribution on the set of actions [33].

Recently, there have been an increased interest to use game theoretic models for addressing Internet security issues in order to provide a scientific basis for security-related decision making. In these models, the players or decision makers play the role of either

the attacker or the defender. They often have conflicting goals since an attacker attempts to breach the security of the system in order to disrupt or cause damage to its services, whereas a defender takes proper countermeasures to improve the security of the system. Since the success of a security system depends on the defence strategies implemented by the security administrator (defender) against the strategic actions taken by the attackers, it entirely matches the game theory seeing that one player's outcome depends not only on her decisions, but also on those of her opponents.

Game theory provides mathematical models to analyze these complex, competitive, and multi-agent interactions schemes. Also, game theory helps the players predict each other's behavior and proposes the best action in any given situation.

2.1.1 Game theoretic approaches to security investments of ISPs

Recent studies and security experts have suggested that ISPs are in a good position to prevent, detect, and mitigate certain types of malicious cyber behavior such as botnets' activities on home users' computers [5], [17]. Yet security investment decision made by the ISP is costly since it requires deploying intrusive technique, filtering the traffic and suspending the infected machine Internet service. Additionally the ISP should accept the cost and the risk of discarding some of the legitimate traffics accidentally, losing reputation and drop revenue. So we need to investigate the financial incentives for ISPs which would encourage them to take positive security investment decision.

Some policy solutions have been proposed to provide ISPs with a financial incentive to take a greater role in helping cyber security [32], [11]. One main strategy discussed

throughout the cyber security literature is to make ISPs liable for the damages caused by their subscribers when they are infected with malware. For instance, Anderson et al. [3] recommend imposing financial penalty on ISPs for ignoring the existence of malware on their subscribers' computers. Their study proposed that ISPs should be charged a fixed penalty if they do not quarantine infected entities in a specific time once they have been notified of their activities. However, there are some problems with this solution, such as who should be beneficiary of these penalty? Or what is the reliable time for taking an action from ISPs?

Furthermore, there are studies that construct the game theoretic model to address the economic motivation in competitive environment for investing in security by the ISPs. Garcia and Horowitz [19] used game theory to analyze economic motivation faced by an Internet service provider (ISP) to add Internet security. In their model, an ISP with a higher level of security is able to earn a higher expected revenue. However the expected revenue gains resulting from investments will decrease as competitors increase their security level. That leads to an interesting result saying that orientation toward Internet security investment will decrease when the number of Internet providers rises. Christin et al. [9] use game-theoretic analysis to study the impact of security experts in a network of competitive players. These competitive players could be selfish expert players, naïve players and cooperative players who faced a common security threat. Their aim was to find out to what extent information security expertise help making a network more secures, and leads to unexpected results showing that addition of selfish experts will never increase the expected security level of a network. The reason was that the expert users in the network act as a free-riders so a

network with the large share of sophisticated and expert users, such as Internet, will not achieve superior security level. On the other hand, having cooperative experts improves individual expected payoffs, and dramatically increases the expected security level of the network.

In chapter 3, we use a game theoretic model to analyze the strategic behavior of two ISPs as a non-cooperative security game with complete information. Both players aim to maximize their pay-off by choosing the best strategy regarding deploying security policy among their subscribers.

2.1.2 Game Theory and Attacker-Defender Models

Jose and Zhuang [23] investigate the dynamics between a defender and an attacker considering technology adaptation in a multi period sequential game with uncertainty. Jose and Zhuang study the impact of timing decision for defender and attacker on purchasing newer technologies for defending and attacking. They capture the trade-offs between immediately adopting a technology and delaying on such an action at every period by both players in which actions are dependent on the history of decisions that has been made until now. The study of Jose and Zhuang measure the difference in the optimal costs when the defender chooses the policy to invest immediately in the most effective and most expensive technology versus choosing to invest slowly in one level of technology at a time. Lee et al. [27] proposed cost-sensitive machine learning techniques as a model to help the network managers take optimal defence strategies and make intrusion detection more successful. Their study relies on the fact that cost factors need to be included in the process of developing and

evaluating intrusion detection system. This requires the intrusion detection models to be sensitive to the cost factors. The study of Lee et al. examined the major cost factors such as the development cost, the operational cost (i.e., the needed resources), the cost of damages resulted from an intrusion, and the cost of detecting and responding to a potential intrusion. Liu et al. [30] focused on the intrusion detection problem in mobile ad-hoc networks and presented two-player game based on a Bayesian formulation to analyze the existence of Nash equilibria in static scenario. In their game, the defender updates her prior beliefs about the opponent based on new observations. This allows the defender to constantly update her belief on her opponent's maliciousness as the game progresses. Lewis et al. [1] modeled the intrusion detection problem as a game played between the attacker and the IDS. In particular, they modeled it as a two-person, non-zero sum, single act, finite game with dynamic information. They considered a distributed IDS with a network of sensors, where a sensor is defined as an autonomous software (agent) that monitors and reports possible intrusions using a specific signature comparison technique. Lewis et al. analyzed the sensor output data by assigning security risk value to each documented intrusion signature to model attacker's behavior, intent, and target threats. Their scheme provides system administrators with a possibility to enable the IDS to operate in different modes specific to each security level.

In chapter 4, we use a game theoretic model to investigate the dynamic interaction between an attacker and the defender as two-player game with uncertainty. We consider dynamic defence device with multi-level of detection adaptable by the security administrator (defender) and the attacker who is capable of launching a variety of attacks with

different severity levels. It is critical to configure a detection level in a dynamic fashion to trade-off security overhead, deployment cost and system performance.

2.2 Pontryagin's Maximum Principle (PMP)

Pontryagin's Maximum Principle (PMP) is a classical result from optimal control theory that provides the necessary condition that must be satisfied to find the best possible control in dynamical system. In general, Pontryagin's Maximum Principle is a proposition which gives relations for solving the variational problem of optimal control and it is used for solving problems in dynamic optimization and differential games.

The principle states informally that the Hamiltonian must be minimized over U, the set of all permissible controls. If $u^* \in U$ is the optimal control for the problem, then the principle states that:

$$H\big(x^*(t), u^*(t), \lambda^*(t), t\big) \leq H\big(x^*(t), u, \lambda^*(t), t\big), \ \ \forall u \in U, t \in [t_0, t_f],$$

where x^* is the optimal state trajectory, and λ^* is the optimal costate trajectory, and t_f is the final time.

After the development of Pontryagin's maximum principle, it became clear that there was a connection between differential games and optimal control theory [7]. In fact, differential game problems represent a generalization of optimal control problems in cases where there are more than one controller or player.

2.2.1 Malware Propagation Models

The devastating outbreaks of Internet malwares [31], [12], [46] led to the widespread investigation of malware propagation on the Internet. In security breaches, such as the spread of viruses and worms in the Internet, an infected machine becomes a new source of infection, and attacks other vulnerable machines. In order to overcome such breaches and their implied damage, network users can be equipped with protection and curing tools. For example, a protection strategy can be performing security patches by the security administrator through the network.

The spread of Internet worms and viruses deals with epidemic processes, and it required employment of epidemic theory. When the Code Red v2 worm surged in July of 2001, Staniford et al. [41] presented a propagation model to explain the Random Constant Spread theory of the worm as a biological epidemic model, which is widely used in epidemiology. Since then epidemic modeling based on the classic Kermack-Mckendrick [18] has been used to analyze the spread of malware in the networks. It is proved that in a large-scale network the deterministic epidemic models can successfully represent the dynamics of the spread of the malware.

By checking the Code Red worm incident and networks properties, Zou et al. [47] present a more accurate Internet worm model, called two-factor worm model. They consider both effect of human countermeasures against worm spreading, such as cleaning, patching, filtering or disconnecting computers, and the reduction of worm infection rate due to worm's impact on Internet traffic and infrastructure. They demonstrate that only at

the beginning phase of a worm propagation the propagation speed is exponentially growing. In their two-factor worm model, the increasing speed in the number of infected hosts slow down when about 50% of susceptible hosts have been infected. Their simulations and the numerical solutions for the two-factor worm model show that this model matches well with the experimental Code Red worm in July 19th 2001.

Yu et al. [46] define a new class of worms called self-disciplinary worm which adapts its propagation patterns according to defensive countermeasures by intentionally reducing its propagation speed to avoid or delay detection and infect more computers. They divide self-disciplinary worms into two categories of static and dynamic self-disciplinary worms. That is, static self-disciplinary worms cleverly select a propagation speed at the initial time of attack and keep the same strategy during the attack session. On the other hand, dynamic self-disciplinary worms adjust their propagation speed dynamically during the attack session. They consider two existing defensive schemes of threshold-based and trace-back and used game-theoretic analysis to find the most effective defence pattern. Their result shows that the combination of the both schemes is effective against static self-disciplinary worms, while to be able to defend against dynamic self-disciplinary worms, additional scheme is required.

Pontryagin's maximum principle used to identify the optimum decision rules and formulate the dynamical decision in optimal control problems. The study of Khouzani et al. [26] represents the propagation of malware in a battery constrained mobile wireless network using an epidemic model. In particular, Khouzani et al. studied the worm that can kill the infected node considering the fact that killing an infective node sooner can extremely

disrupt networks functions as a node can be healed later. On the other hand, killing a node prevents it from propagating the infection in the network. It is therefore necessary to determine the instantaneous rate of killing to maximize the damage by the worm. The worm also can choose to accelerate its spreading rate among infected nodes by increasing their contact rates or selecting higher transmission gains and reduce the nodes' energy. Khouzani et al. formulate the decision problem using theorem of Pontryagin maximum principle to calculate the maximum value of the damage that this worm can impose on the network. Epidemiological frameworks have also been used to model the propagation of malware in a mobile wireless network assuming an infected node can transmit its infection to another node only if they are in communication range of each other [25]. Khouzani et al. suggest to quarantine the infection nodes by modifying their communication range. That is, the reception gain of the healthy nodes can be reduced to decrease the frequency of contacts between the mobile nodes in order to avoid the spread of the infection. They also propose an optimal control framework to characterize the trade-off between the communication range of nodes and the QoS offered by the network when end-to-end communication delay increases. Using Pontryagin's maximum principle, they identified the optimum policy for dynamically controlling the communication range to minimize the overall network cost.

In chapter 5, we use a differential game to model the worm propagation in a network and the corresponding dynamic defence countermeasure of patching infected hosts by the defender to inhibit the spread of worms. Then, we formulate the problem as continuous-time deterministic optimal control problems. Using Pontryagin maximum principle we compute the dynamically evolving optimal worm propagation rate for the worm propagator

and optimal recovery rate for the defender.

Chapter 3

ISPs cyber security solutions: barriers and incentives

The traditional role of ISPs is to provide Internet access to end users. Due to their topological position between the end users and the Internet, ISPs can also observe all the traffic flowing into and out of their networks. Consequently, based on the observed traffic, ISPs can determine malware-infected machines among their subscribers and hence they are in a good position to play a critical role in improving the security of Internet users. For example, ISPs can identify and quarantine infected machines to prevent any possible threat against other Internet users.

This problem cannot be solved exclusively by end users who have incomplete information about the infection of their PCs or the associated security risks and relevant defense strategies. Security professionals [5], [6] have recently studied whether Internet users are

ready to accept the price rise of Internet access required by ISPs who deploy security solutions, and whether these users are willing to take the cost of suspension of their Internet service when malware is detected on their computers, and if there is a demand from Internet users to subscribe with secure ISPs. August and Terrence [6] found out that all these costs would bring reductions in the risk of identity theft for Internet users when malware is removed from the users' computer. Additionally malware removal mitigates the presence of botnets in the Internet and reduce the risk of security threat towards others [14]. On the other hand, if the party that is in the position to protect a system is not the party that would suffer from the result of a failure of security then there will be problem. For instance, Anderson [39] stated that " while individual computers users might be happy to spend $100 on anti-virus software to protect themselves against attack, they are unlikely to spend even $1 on software to prevent their machine being used to attack a third party who is wealthy corporation." Wood and Row [45] claim that ISPs could raise price to help boost their revenues because security sensitive customs are willing to accept higher prices in order to avoid the impact associated with security attacks. Their study claims that some consumers are willing to accept higher processes, security training and account suspension in order to avoid impacts associated to security attack on the Internet. However, this solution requires voluntary action on the part of home users and no data exists to enable us to determine the effectiveness of this solution. For instance, Varian [21] reports some ISPs who provide antivirus software to their home Internet customers for free to improve the overall cyber security. Based on an interview with one of these ISPs, Varian found out that only 50% of their customers have downloaded the security software package that is free

with their subscription.

In this chapter, we present a game theoretic model to study some of the economic barriers and incentives for ISPs who can choose to deploy cyber security solutions. While the obtained results can be utilized by ISPs to determine their best strategy, our analysis also identifies scenarios that closely resembles the tragedy of the commons case where ISPs might be tempted not to deploy good security solutions in order to maximize their financial gain. The results obtained from our analysis clearly show the need for incentives, laws, and regulations to better guide the role of ISPs in enhancing the global security of the Internet.

3.1 Game Model

Considering the fact that customers are heterogeneous in their need and appreciation to the deployed security solutions, for the purpose of our analysis, we divide Internet users into two categories:

- Security sensitive: Individual users or business owners who are willing to spend more money to increase their level of security. We also assume that users in this category trust their ISP in the case they have been notified that their machines are infected and will not be upset if the ISP temporarily suspends their infected machine. For this category of Internet users, the reward of deploying security from their ISPs is more important than the increase in their Internet bill.

- Security insensitive: According to a recent study by McAfee [10], one in every six personal computers has zero protection (e.g., disabled or nonexistent anti-virus software). These machines are extremely vulnerable and they can easily become part of a botnet, spread viruses, or cause other threat to cyber security. Obviously, these home Internet users are unaware of the associated security threats and may also not be willing to invest in Internet security solutions that may not directly affect them. Individuals in this class of security usually subscribe with ISPs who offer less monthly fees without considering their security standpoint. The traditional behavior of these category of Internet users would be switching to another ISP when their current ISP suspends their malware infected machines.

While security insensitive users are threat to other Internet users, their monthly subscriptions fees can also be a non-negligible part of the ISP income. Thus, in deciding for their best strategy, ISPs should consider the privilege of their security sensitive customers and accept the fact that suspension of security insensitive customers may make them unhappy and they may decide to switch their service to another service provider with less stringed security requirements. What makes the decision of the ISP even more complex, especially if motivated only by financial gain, is the fact that infected machine of the security insensitive user might be attacking a target who is not a subscriber with this ISP and who might even be physically residing on the other side of the globe. To further illustrate the above case, consider a simple example of a Denial of Service Attack. The attacker is an infected machine (bot) belongs to ISP_1, while its target is a customer in the network of ISP_2. ISP_1 can decide to prevent this attack by deploying intrusive techniques, filtering

the traffic and suspending the attacker services. Additionally, ISP_1 should accept the risk of discarding some of its legitimate traffics accidentally which may result in losing its reputation and dropping its revenue. Paying all these costs in order to improve its competitors' security might be economically unconvincing. On the other hand, taking action from ISP_1 would definitely prevent all other possible attacks from that infected machine (bot) towards its customers in future.

Our game is a complete information game with two ISPs acting as two players. Without proper regulations and laws, ISPs will chose the strategy that increase the number of their subscribers and therefore increases their revenue. Since infected subscribers have an opportunity to change their service provider according to their preferred security standpoint, customers loss for one ISP causes a revenue for the other ISP.

In the complete information environment, each player has full knowledge of the expected loss of the other player whereas in an incomplete information environment, each player only knows her own expected loss. In our game, we claim that players have complete information about each other. Because both ISPs know their market share and they can easily estimate the portion of customers that are sensitive to security failure in the whole network. Thus, the loss of an ISP in case of security failure is predictable. Additionally, in our game, each ISP is considered as an expert player which makes decisions based upon intelligent consideration of the possible consequence. Therefore in our game, these expert players optimize their strategy by considering their market share and the security threat they face, the portion of bots in the Internet, the portion of sensitive customers in the network, and the behavior of the other players.

3.1.1 The Players Strategies

The strategy set of each player is defined by two actions:

- Deploy security: When deploying this strategy, an ISP identifies and cuts off the Internet access of infected subscribers until their machines have been cleaned. That is, the ISP implements the technology to monitor malicious behavior on the networks and quarantines the infected machines. Quarantining of infected subscribers implies limiting their Internet access, for example, to only Windows updates or to a range of security services.

- Not deploy security: When opting for this strategy, ISPs simply ignore the risk associated with infected subscribers (bots) in their networks and continue serving these subscribers.

3.1.2 Game Rules

The game requires some rules to become meaningful. We have two assumptions on this game:

- Security sensitive customers will leave their current Internet provider (ISP) and subscribe with the other ISP when their machine is being infected by a bot and their current provider does not deploy security solutions, whereas the other ISP is deploying security solutions.

- Security insensitive customers do not care whether or not their machines are infected and joining a botnet. However, they will leave their current Internet provider (ISP)

and subscribe with the other ISP who is not deploying security policies when their current ISP suspends their services if their machines are infected.

3.1.3 Pay-off

In what follows, we consider the different factors affecting the players' pay-off. Two parameters of cost and revenue are considered:

- Cost of deploying security: When ISPs decide to deploy security in their networks, there is a cost associated with deploying intrusive techniques and deep packet inspection. Throughout the rest of the chapter, we use C to donate the cost paid by the ISP for deploying such security solutions.

- Revenue of the ISP: The majority of the ISP's revenue comes from subscription fees. Each customer adds more income to her ISP and hence an ISP with more subscribers gains more money at the end of the month. We use R to donate the revenue gained by the ISP for each subscriber in the network.

There are also other elements that are required to determine the players' pay-off:

- Total number of Internet customer: We use N to donate the total number of Internet subscribers.

- Market share for the ISPs: We use f, and $1 - f$ to donate the market share for the first ISP (ISP_1) and the second ISP (ISP_2), respectively.

- Percentage of security sensitive customers: We use s_1 and s_2 to donate the percentage of customers that are sensitive to security failures in ISP_1 and ISP_2, respectively.

- Probability of getting infected: We use b to denote the probability that a machine connected to the Internet gets compromised and becomes a part of a botnet. ISPs should consider this percentage to estimate the probability of botnet infection in their networks.

Table 1 summarizes all the payoff factors discussed above.

Table 1: Summary of players' pay-off

Summary of players' pay-off	
N	Total number of network customers
C	Cost of deploying intrusive techniques for deep packet inspection
b	Probability of getting infected by a bot
f	Market share for ISP_1
s_1	Percentage of IPS_1 customers that are sensitive to security failures
s_2	Percentage of IPS_2 customers that are sensitive to security failures
R	Revenue gained from keeping a customer in the network

Considering the likelihood of playing each strategy by both ISPs (i.e., deploying security, or not deploying security), the expected payoff is shown in Table 2.

Table 2: Pay-off matrix of the game

ISP_1 \ ISP_2	Deploy Security	Do Not Deploy Security
Deploy Security	$-C, -C$	$-C - Nbf(1-s_1)R + Nb(1-f)s_2R$, $-Nb(1-f)s_2R + Nbf(1-s_1)R$
Do Not Deploy Security	$-Nbfs_1R + Nb(1-f)(1-s_2)R$, $-C - Nb(1-f)(1-s_2)R + Nbfs_1R$	$0, 0$

3.2 Equilibrium Strategies

The goal of the game for both players is to choose a strategy that maximizes her expected payoff by taking into account the other player's decision.

Best Response for ISP_1: Using Table 2, ISP_1 can find the best response between deploying security or not deploying security by comparing the expected payoff of each option. If ISP_2 chooses to deploy security, ISP_1's pay-off would be:

$$\begin{cases} -C, & \text{if } ISP_1 \text{ deploys security} \\ -Nbfs_1R + Nb(1-f)(1-s_2)R, & \text{if } ISP_1 \text{ does not deploy security} \end{cases} \tag{1}$$

So, ISP_1 will not deploy the security if

$$\begin{aligned} -Nbfs_1R + Nb(1-f)(1-s_2)R &> -C \\ \Rightarrow [fs_1 - (1-f)(1-s_2)] &< \frac{C}{NbR} \end{aligned} \tag{2}$$

Similarly, if ISP_2 chooses not to deploy security, ISP_1's pay-off would be:

$$\begin{cases} 0, & \text{if } ISP_1 \text{ does not deploy security} \\ -C - Nbf(1-s_1)R + Nb(1-f)s_2R, & \text{if } ISP_1 \text{ deploys security} \end{cases} \tag{3}$$

Hence, ISP_1 will not deploy the security if

$$\begin{aligned} -C - Nbf(1-s_1)R + Nb(1-f)s_2R < 0 \\ \Rightarrow [(1-f)s_2 - f(1-s_1)] < \frac{C}{NbR} \end{aligned} \tag{4}$$

Similarly, to find out when deploying security is a better choice for ISP_1, we should compare ISP_1 expected payoff. From equation (1), we can conclude that ISP_1 will deploy the security if

$$\begin{aligned} -Nbfs_1R + Nb(1-f)(1-s_2)R < -C \\ \Rightarrow [fs_1 - (1-f)(1-s_2)] > \frac{C}{NbR} \end{aligned} \tag{5}$$

Also from equation (3), ISP_1 will deploy security if

$$\begin{aligned} -C - Nbf(1-s_1)R + Nb(1-f)s_2R > 0 \\ \Rightarrow [(1-f)s_2 - f(1-s_1)] > \frac{C}{NbR} \end{aligned} \tag{6}$$

3.3 Numerical Illustration

In this section, we present some numerical examples to provide further insight into our theoretical results. To see what exactly the equations derived in the previous section suggest, we need to have some assumptions on the probability of getting infected by a bot malware in the Internet (i.e., an estimate for b) and also the cost of deploying security. Typical botnets have several hundred to several thousand members, though some botnets have been estimated to have over 1.5 million members [43]. Vinton Cerf estimated that up to 150 million computers (about 25% of all Internet hosts) could be infected with botnets [2]. Thus, throughout this chapter, we assume the probability of infection by a bot in the Internet, $b = 25\%$. We also consider the cost of deploying security as a fraction, x, of the ISP revenue, i.e., $C = xNfR$.

Our aim is to study the effect of the market share, f, and customer security awareness, i.e., portion of security sensitive customers, s_1 and s_2, on decision-making process of both ISPs.

3.3.1 The Impact of Market Share and Customers' Security Awareness

We assume different cases for the portion of security sensitive customers in both ISPs: $s_1 = s_2$, $s_1 = 2s_2$, and $s_1 = \frac{s_2}{2}$.

The case where $s_1 = s_2 = s$:

From equation (2), if we assume $s_1 = s_2 = s$, then we have

$$NbRf - NbR(1 - s) < C \tag{7}$$

This suggests that ISP_1 will not deploy security as long as the revenue gained from security sensitive customers who are infected is less than the cost of deploying security.

Similarly, equation (4) implies that

$$NbRs - NbRf < C \tag{8}$$

So, we have the additional condition that ISP_1 will not deploy security as long as the revenue gained from security insensitive customers who are infected is greater than the cost of deploying security.

In strategic analysis, a dominant strategy always does at least as good as the strategy it dominates. In order to have *not deploying security* as a dominant strategy for ISP_1, both equations (7) and (8) should be satisfied. Since we assume that the cost of deploying security is a fraction of ISP's revenue (i.e., C=xNfR), from equation (7) we have:

$$NbR(f + s - 1) < xNfR \Rightarrow \frac{b}{f}(f + s - 1) < x$$

Similarly, from equation (8):

$$NbR(s-f) < xNfR \Rightarrow \frac{b}{f}(s-f) < x$$

Thus, as long as $\frac{b}{f}(f+s-1) < x$ and $\frac{b}{f}(s-f) < x$, regardless of the action of ISP_2, the dominant strategy of not deploying security is a better choice for ISP_1.

Similarly, from equation (5) we have:

$$NbR(f+s-1) > xNfR \Rightarrow \frac{b}{f}(f+s-1) > x \tag{9}$$

With the same assumption, equation (6) implies;

$$NbR(s-f) > xNfR \Rightarrow \frac{b}{f}(s-f) > x \tag{10}$$

Thus, in order to have deploying security as a dominant strategy for ISP_1 regardless of the action of other ISP, the two conditions: $\frac{b}{f}(f+s-1) > x$ and $\frac{b}{f}(s-f) > x$ should be satisfied.

Next, we compare the cases where we assume that the cost of deploying security is one tenth of the customers' revenue for the ISP (i.e., $C = 0.1NfR$) and for the case where it is only one percent of the customers' revenue (i.e., $C = 0.01NfR$). Figure 1 shows the best response for ISP_1 and ISP_2 when we vary the cost of deploying security, C, as different percentage of ISP's income NfR , the percentage of market share, f, and the percentage of security sensitive customers , s.

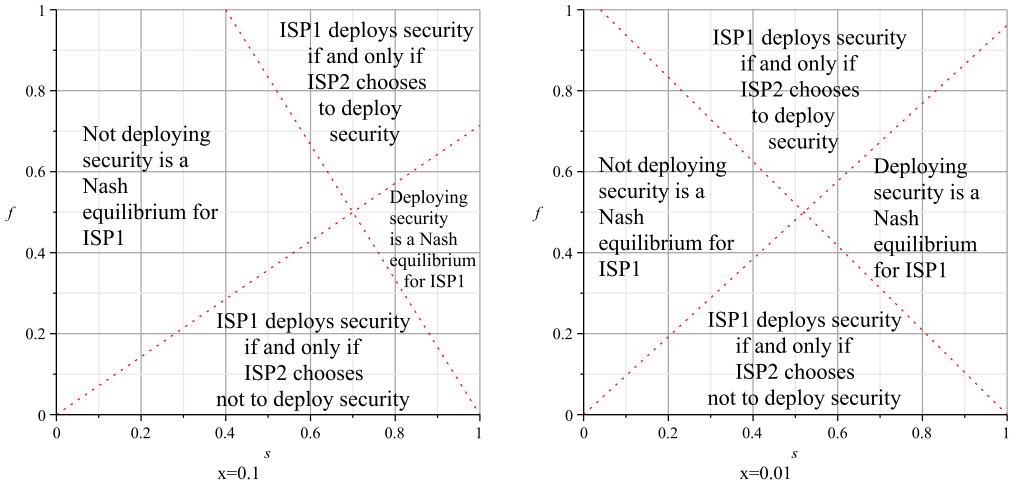
As depicted in the figure, in the case when deploying security is more costly, i.e., for $x = 0.1$, and the percentage of security sensitive customers is less than 70%, when the market share of the ISP grows, there is a large area in the figure (which corresponds to a large range of system parameters) where ISPs choose not to deploy security. Therefore, cyber security risk will be too high and will create significant damage in terms of public good. Comparing the best response of ISP_1 and ISP_2, there are two areas where the two players have a conflict of interest. That is, although it is better for the ISP with the majority of market share to get together with the smaller ISP, the smaller ISP gets a better payoff when it chooses the opposite strategy of the market leader. Obviously the lower cost of deploying security would encourage the ISP to invest in security.

Moreover, when the cost of deploying security is not very large (e.g., $x = 0.01$), if we assume the market share of both ISPs is almost the same, we can see that as the customers awareness increases such that more than half of the subscribers are security sensitive (i.e., $s \geq 0.5$), both ISPs choose the Nash equilibrium of deploying security. When the cost of deploying security grows, the security awareness of customers should also increase in order to have deploying security as a Nash equilibrium by both ISPs.

The case where $s_2 = s$ and $s_1 = 2s$:

From equation (2), when $\frac{b}{f}(f + s + fs - 1) < x$ and $\frac{b}{f}(s - f + fs) < x$, regardless of the action of ISP_2, the dominant strategy of not deploying security is a better choice for ISP_1. From equations (5) and (6), when $\frac{b}{f}(f + s + fs - 1) > x$ and $\frac{b}{f}(s - f + fs) > x$, regardless of the action of ISP_2, the dominant strategy of deploying security is a better

Response of ISP1



Response of ISP2

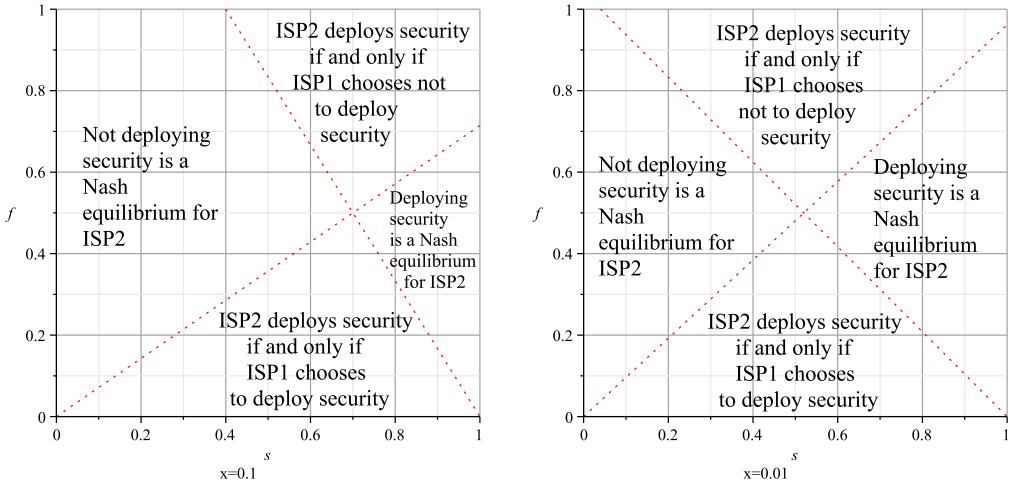


Figure 1: Best response of $ISPs$ when $s_2 = s_1 = s$

choice for ISP_1.

The case where $s_2 = s$ and $s_1 = \frac{s}{2}$:

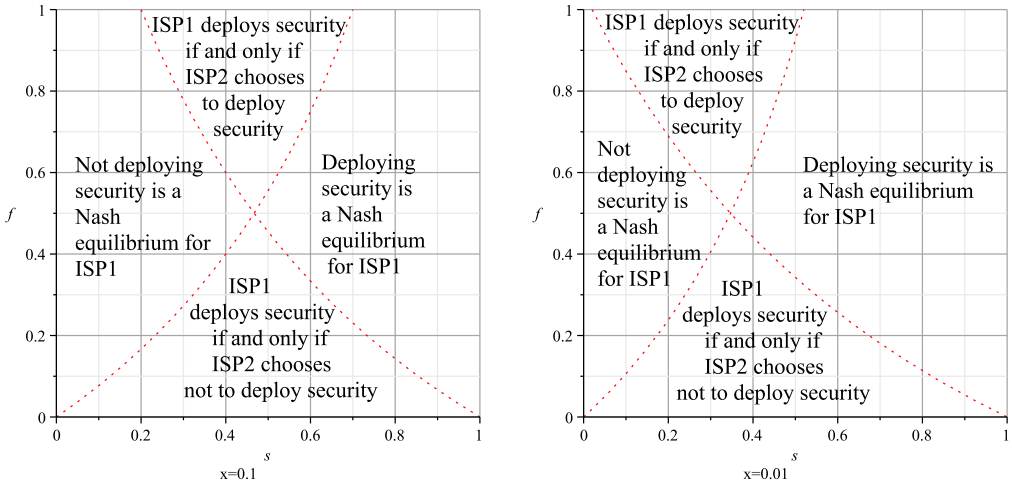
From equations (2) and (4), when $\frac{b}{f}(f + s - \frac{fs}{2} - 1) < x$ and $\frac{b}{f}(s - f - \frac{fs}{2}) < x$, regardless of the action of ISP_2, the dominant strategy of not deploying security is a better choice for ISP_1. From equations (5) and (6), when $\frac{b}{f}(f + s - \frac{fs}{2} - 1) > x$ and $\frac{b}{f}(s - f - \frac{fs}{2}) > x$, regardless of the action of ISP_2, the dominant strategy of not deploying security is a better choice for ISP_1.

Figure 2 shows the best response for ISP_1 for different costs of deploying security, different percentages of the market share, f, and different percentages of security sensitive customers, s. As depicted in the figure, when the portion of security sensitive customers in the ISP network rises, the incentive for that ISP to invest in security also increases. It is obvious that larger costs of deploying security discourages the ISP from improving the Internet security. Considering Figure 1 and Figure 2, we see that when the security awareness of customers are homogenous among both ISPs, the incentive for ISPs to deploy security is low.

3.3.2 Payoff Comparison and Possibility of Collusion

Assume that the two ISPs are competing in a geographical region for a common customer base. For example, we consider one ISP as the market leader which means that f range from 0.5 to 1 (for the purpose of our numerical illustration, we choose $f = 55\%$). According to MacAfee report [10], 17% of PC users worldwide do not have any security protection

$s_2 = s$ and $s_1 = 2s$ when $C = xNfR$



$s_2 = s$ and $s_1 = \frac{s}{2}$ when $C = xNfR$

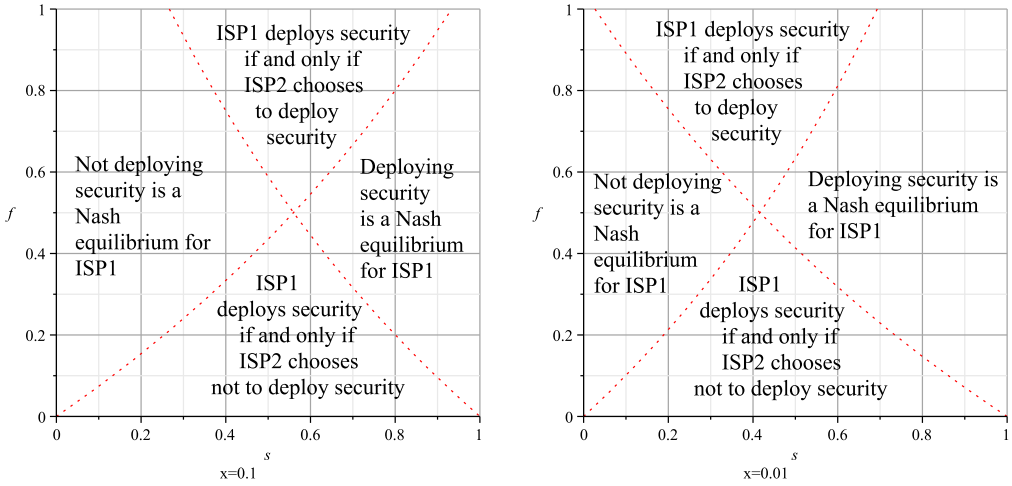


Figure 2: Comparison of best response of ISP_1 when $s_1 = 2s_2$ and $s_1 = \frac{s_2}{2}$

on their machines. So security sensitive customers would be almost 83% of the customers among both ISPs. We assume Vinton Cerf's [2] data is correct, i.e., the likelihood of becoming infected by a bot in the Internet is 0.25 (i.e, $b = 0.25$). We consider the starting point of the game when both ISPs have not deployed security. The cost of deploying security is assumed to be 1% of total revenue of the ISP (i.e., $C = 0.1NfR$). ISP_1 and ISP_2, as expert players, should calculate their expected payoff to see if they should change their security strategy among their network or not. In Table 2, we calculate the expected payoff of the two ISPs:

Table 3: Expected Pay-off of ISPs ($f = 55\%$)

	ISP_2 deploys security	ISP_2 does not deploy security
ISP_1 deploys security	$-0.055NR$, $-0.045NR$	$+0.015NR$, $-0.069NR$
ISP_1 does not deploy security	$-0.095NR$, $+0.05NR$	0, 0

Obviously, deploying security is a dominant strategy for the ISP_1. So there is an incentive for ISP_1 to change its current strategy to deploying security. For ISP_2, deploying security is also a dominant strategy. So ISP_2 will change its current strategy to deploy security. At the end, both ISPs select the strategy of deploying security and their expected payoff would be $(-0.055NR, -0.045NR)$ which is less than their previous payoff $(0, 0)$.

Although, in game theory, players must consider the preferences and rational choices of other players to make the best choice for themselves, in some situations it is possible and more profitable to cooperate with other players. This means that sometimes the outcomes from the strategy profile chosen by rational players in non-cooperative game does not lead

to the best payoff (e.g., losing for both player instead of winning). In these conditions, players can make binding agreements with each other and work together to improve their outcome. This would happen in our scenario where both ISPs are rational players, and they can determine the fact that the outcome obtained when both players are deploying security is worse than the outcome they obtain if they both choose not to deploy security. So there is a possibility that the two ISPs decide to collude and do not deploy security.

This expresses the lack of sufficient natural incentives for ISPs to help improve Internet security. To solve this concern, Clayton [11] suggests that Government should play a role in subsidizing the cost of clean-up and take an action towards improving security level of Internet users. Contrary, instead of Government subsidizing, we propose that it is in the best interest of Internet users if the government enforces collaboration between ISPs to deploy security in their network. Otherwise, ISPs will not step in, therefore cyber security risk will be too high and social welfare will be depressed.

However, as shown in Figure 1, there are also situations in which there is no dominant strategy for players, and ISPs are not interested in collaboration with each other. For instance, we assume a situation where market share for one ISP is 90% (i.e. $f = 90\%$). Table 4 illustrates the expected payoff of both ISPs:

Table 4: Expected Pay-off of ISPs ($f = 90\%$)

	ISP_2 deploys security	ISP_2 does not deploy security
ISP_1 deploys security	$-0.09NR$, $-0.01NR$	$-0.108NR$, $+0.018NR$
ISP_1 does not deploy security	$-0.182NR$, $+0.172NR$	0, 0

Obviously from Table 4, there is no dominant strategy for the players in this situation.

Although ISP_1 wants to coordinate with the other player to achieve a better payoff, ISP_2's best interest is to choose the opposite of the strategy chosen by ISP_1. In this scenario, ISP_1 as an expert player may choose to play a minimax strategy (a minimax strategy in the game theory is when a player chooses a strategy to minimize the maximum payoff of the other player and minimizes her own maximum loss). So ISP_1 should choose deploying security because otherwise if ISP_1 chooses the strategy of not deploying security, ISP_2 will play a deploying security to achieve a better payoff (i.e., $+0.172NR$) and causes the worst payoff for ISP_1 (i.e., $-0.182NR$). When ISP_1 selects deploying security, ISP_2 should choose not deploying security to maximize its expected payoff. As a result, the expected payoff for both ISPs would be $(-0.108NR, +0.0108NR)$. Now if $ISP2$ is forced to deploy the security, ISP_1 will get a better payoff of $-0.09NR$ which is its second best gain. This scenario indicates that beside government's interest in improving cyber security in the Internet, it is also in the best interest of ISP_1 as a market leader that the government enforces collaboration and pushes ISP_2, who has a small portion of Internet subscribers, to deploy security in its network.

3.4 Chapter Summary

In this chapter, we presented a game theoretic framework to analyze the interaction between two ISPs who have to decide whether to deploy security solutions among their customers to prevent, detect, and mitigate certain types of malicious cyber behavior. Our mathematical model provides an approach for analyzing and understanding the strategic behaviour of two

ISPs who have to decide whether to invest and improve the Internet security according to their customers' security awareness and their market share. We identified scenarios that closely resembles the tragedy of the commons situations where ISPs might be tempted not to deploy good security solutions in order to maximize their financial gain. The results obtained from our analysis clearly show the need for incentives, laws, and regulations to better guide the role of ISPs in enhancing the global security of the Internet. It should also be noted that enforcing laws, and regulations might not always be an easy achievable solution given the fact that ISPs span over different geographical territories and they may not operate in countries obeying the same set of rules.

Chapter 4

Investments of Attackers and Defenders in Security Games

4.1 Introduction

Nowadays, one major concern of networks and computer systems operators is to protect sensitive information against different forms of attacks including malware, intrusion, unauthorized access, and denial-of-service attacks. As a result, hundreds of security devices such as firewalls, intrusion detection systems (IDS), and authentication servers can be deployed in order to protect against these attacks. However, the objective of a defense system is to be cost-effective, i.e., it should cost no more than the expected level of loss in case of attacks or intrusions [27]. Thus, before investing in an information protection system, the defender needs to assess the cost-benefit trade-off between the information assets that are at risk and have value to the defender, and the cost of employing effective defense systems.

Defenders should precisely calculate the cost of detecting and responding to an intrusion or attack versus the value of the information assets that are at risk in order to determine the optimal investments in IT security.

In this chapter, we present a game-theoretic model for analyzing the interaction between attackers and defenders in networked computer systems. In particular, we investigate the dynamic interaction between the attacker and defender as two-player game with uncertainty while considering multi-level of detection for defence devices configurable by the defender and variety of attacks with different level of severity. It is critical for the defender to configure a detection level in a dynamic fashion to trade-off security overhead, deployment cost and system performance. For the attacker, it is also essential to launch an attack with an effective severity level seeing the cost of accumulating the required resource and the reward of successful attack. We compute mixed strategy Nash Equilibria (best-response) for both the attacker and the defender considering the cases when the players' valuation follows the uniform distribution and the case where it follows a normal distribution. We then formulate an n-player game to capture competition among n attackers who aim to successfully attack the same target and analyze the mixed strategy Nash Equilibria in both models.

4.2 The Game Model

We consider a security game between a defender who configures the defense device to protect a system versus an attacker who aims to attack the same specific system which contains

security sensitive information. The defender should choose the effective detection configuration for defense device in order to prevent attacks or intrusions towards the system. On the other hand, the attacker should choose between launching an attack using all or portion of her available resources, or not launching an attack and using the time to accumulate resources and improve the chances of success for future attack. If the attacker chooses to launch an attack, the attack's success is determined by the current levels of the attack and the level of defense chosen by the defender.

Obviously, the target system has a predefined value to both the attacker and defender. The rationale here is that a player with a higher valuation would do whatever it takes to succeed in achieving or avoiding an attack. If the target is more valuable, then the defender is likely to invest more in detection in order to cope with attacks with higher level of severity. We associate the severity level of attacks with the set of resources that are available to the attacker. Also, for the defender, detection level does not necessarily refer to a specific detection system but to the joint implementation of the tools that are used and employed to detect and prevent malicious traffic.

Our game theoretical framework models the interaction between the attacker and the defender as a non-zero-sum non-cooperative game with uncertainty. By assuming that higher levels of defence and high level of attack severity are associated with higher levels of investments by the defender and the attacker, respectively, we compute mixed strategy Nash Equilibria (best-response) for both the attacker and defender considering the cases when the players' valuation follows the uniform distribution and the case where it follows a normal distribution. We then formulate an n-player game to capture competition among

n attackers who aim to successfully attack the same target and analyze the mixed strategy Nash Equilibria in both models.

4.2.1 Game Assumption

Throughout the rest of this chapter, we assume the following:

- We have two players, one defender and one attacker, each have a private value about the attack target. This value is independently scaled between 0 and 1. This information is common knowledge among the two players. We used V_a, and V_d to donate the valuation of information on the target system for the attacker and the defender, respectively.

- Although many factors could potentially affect the probability of a successful attack, we model this success probability as a function of the detection level of the defender and the severity level of the attack. We order detection level of defense system and the severity level of attack such that higher values are considered to show higher quality, i.e., the higher detection level configuration, the lower the chance of a successful attack. As the detection configuration level increases, the detection quality of device rises and consequently the probability of effective defense increases but also the cost of this security solution will increase.

- A detection level is capable of detecting an attack with the same severity level or less. As a result, the adopted defense device is sure to fail for an attack with a higher severity level.

- When one of the players (attacker or defender) chooses not to participate in the game, this player must be the weak player who knows that she has a strong opponent, so this player simply decides not to have the cost of deploying detection technique or cost of attack implementation. For instance, for the defender, when the cost of implementing a detection technique outweighs the benefits of reduction in the expected loss of an attack, the defender will refuse to take an action in adopting this defense system.

- A profile of strategies in which the two highest level of attacks to launch and detection device to adopt are not the same is not a Nash Equilibrium [35]. The reason is that the player with the highest capability of attack/detection can increase her payoff by reducing the level of attack/detection in a way that it is still larger than the other player's, so that player pays a lower price and will continue to win.

- A strategy for a player is a function $S(v)$ that maps the true target value v to a non-negative investment for attacking/defending the target assets. This function shows the required investment to implement and configure the adopted detection system for the defender and the operating cost for the accumulation of necessary resource to launch an attack.

- $S(\cdot)$ is a strictly increasing, differentiable function. So, if the target has a different value for each players, then the players are likely to commit different levels of investments in attacking/protecting it.

- $S(v) \leq v$ for all v: players can shade their investment down but they will never invest above their true target values. Notice that since an investment is always non-negative,

this also means that $S(0) = 0$.

These assumptions permit a wide range of strategies. For example, the strategy of investing the true value is represented by the function $S(v) = v$, while the strategy of players shading their investment by a factor of $\beta < 1$ is represented by $S(v) = \beta v$. Additionally, we assume that the two players are identical in all aspects except the actual value they draw from the distribution. Hence, we will consider the case in which the two players follow the same strategy $S(\cdot)$.

4.2.2 The Utility of Players

In this game, the defender challenge is to make a decision on how much to invest in detection systems considering the value of information on the target machine. The defender incurs cost corresponding to the detection level she adopts. In terms of optimization, the defender tries to minimize the utility function U_d representing the expected cost associated with these investments in order to reduce the probability of successful attack and the expected damage when the attacker chooses to launch an attack. The attacker also chooses whether or not to launch an attack considering the chance of success in order to maximize the utility function U_a. The advantage of not launching an attack is that the attacker can further develop capabilities and resources to improve the chance of success in future attacks. The attacker also wants to maximize her utility by comparing the expected benefit of attacking (target value achievement) and attack implementation cost versus not launching the attack since failed attacks cause a negative utility for her. This means that if the attack cost is not significantly high and the expected value of target is greater than the cost of

the attack, the attacker would choose to attack. Otherwise, the attacker as a rational player would simply refrain from getting involved in this game.

In general, rational players want to make sure that the investment they put towards protecting (or attacking) a target system is below its true value, and they must balance the trade-off between investing high (increasing the probability of winning) and spending low (decreasing the expenditure if they lose). We want to find a function $S(\cdot)$ mapping target values to cost of deploying attack for the attacker and for the defender.

Finally, according to our assumptions, the player with the higher target valuation will win the game with the probability P_{win}. Thus, the expected payoff of the players can be expressed by

$$U_d(v_d) = P_{win}\big(-S(v_d)\big) + (1 - P_{win})\big(-S(v_d) - v_d\big) \tag{11}$$

$$U_a(v_a) = P_{win}\big(v_a - S(v_a)\big) + (1 - P_{win})\big(-S(v_a)\big) \tag{12}$$

4.3 Equilibrium Analysis when the Players Valuation Follows a Uniform Distribution Probability

4.3.1 Nash Equilibrium of Two-player Game

We assume that players' valuation are drawn from the uniform distribution on an interval $[0, 1]$. Although there is no pure strategy equilibrium for this game, a mixed strategy of a player is a probability distribution over the possible investment between 0 and 1 to attack

and defend [35]. Let $F(.)$ denote the cumulative probability function with $F(0) = 0$, and $F(1) = 1$. That is, for any x, the value $F(x)$ is the probability that a number drawn from the distribution is at most x. The probability that an attacker with a true valuation v_a succeed, is the probability that the defender has a less valuation, so it is equal to $F(v_a)$. Therefore, the expected payoff for the players is

$$U_a(v_a) = F(v_a)(v_a - S(v_a)) + (1 - F(v_a))(-S(v_a)) \tag{13}$$

$$U_d(v_d) = F(v_d)(-S(v_d)) + (1 - F(v_d))(-S(v_d) - v_d) \tag{14}$$

since the probability that the attacker's valuation is higher than the defender's valuation in the interval $[0, 1]$ is exactly v_a. Therefore, the attacker will win the game with probability v_a. Putting all this together, we see that the expected payoff of the players can be expressed by

$$U_a(v_a) = v_a(v_a - S(v_a)) + (1 - v_a)(-S(v_a)) \tag{15}$$

$$U_d(v_d) = v_d(-S(v_d)) + (1 - v_d)(-S(v_d) - v_d) \tag{16}$$

In both (15) and (16), the first term corresponds to the payoff in the event that the player wins, and the second term corresponds to the payoff in the event that the player loses.

In order for $S(\cdot)$ to be an equilibrium strategy, when both players use strategy $S(\cdot)$, there should be no incentive to deviate from it. Since analyzing deviations to an arbitrary strategy is not feasible, instead of switching to a different strategy, players can implement their deviation by keeping the strategy $S(\cdot)$ but supplying a different "true valuation" to it.

Since we assumed that the attackers' opponent is also using strategy $S(\cdot)$, then the attacker should never invest money to implement an attack above $S(1)$. So in any possible deviation by the attacker, the investment dedicated for an attack will lie between $S(0) = 0$ and $S(1)$. Therefore the attacker can simulate the deviation to an alternate strategy by pretending that her true valuation is not v_a, and then applying it to the existing function $S(\cdot)$. This means deviations in the investing strategy function can be viewed as deviations in the "true valuation" that players supply to their current strategy $S(\cdot)$.

Now consider an attacker with a target value estimation v_a, and investing strategy function $S(v_a)$. Suppose that this attacker chooses strategy $S(v)$ rather than the attacker true value given by $S(v_a)$. Then her payoff will be given by

$$U_a(v) = v(v_a - S(v)) + (1 - v)(-S(v)), 0 \leq v \leq 1 \tag{17}$$

Notice that the expected payoff consists of a fixed cost $S(v)$ that is paid regardless of the win/loss outcome, plus a value of v_a in the event that attacker wins. Canceling the common terms in above equality, we can rewrite it as

$$U_a(v) = vv_a - S(v)$$

Differentiating with respect to v, we have

$$\frac{\partial}{\partial v} = v_a - S'(v)$$

For $S(v_a)$ to be optimal, this derivative must be zero when evaluated at $v = v_a$. So

$$v_a = S'(v_a).$$

Integrating both sides with respect to v_a, we get

$$S(v_a) = \frac{{v_a}^2}{2} + constant.$$

Since we assumed $S(0) = 0$, thus we have

$$S(v_a) = \frac{{v_a}^2}{2}. \tag{18}$$

Similarly for the defender, we can think of a deviation from the investment strategy as supplying a fake value v to the function $S(\cdot)$. Hence if $S(\cdot)$ is an equilibrium choice of the strategies chosen by the defender, then

$$U_d(v) = v(-S(v)) + (1 - v)(-S(v) - v_d)$$

For all possible alternate "true valuation" v in the interval $[0, 1]$, the defender might want to supply to the function $S(\cdot)$. Canceling the common terms in above equality, we can rewrite it as

$$U_d(v) = vv_d - S(v) - v_d.$$

Differentiating with respect to v, we have

$$\frac{\partial}{\partial v} = v_d - S'(v)$$

For $S(v_d)$ to be optimal, this derivative must be zero when evaluated at $v = v_d$. So

$$v_d = S'(v_d).$$

Integrating both sides with respect to v_d, we get

$$S(v_d) = \frac{{v_d}^2}{2} + constant.$$

Since we assumed that $S(0) = 0$, thus we have

$$S(v_d) = \frac{{v_d}^2}{2}. \tag{19}$$

Interestingly both players have the same strategy function $S(\cdot)$ to map their investment to the target value. This shows that when both players follow equilibrium strategies, the player with the higher target valuation will win the game. However, if one player, for some reasons, uses non-equilibrium strategies, the other player should potentially play some other investing strategy.

Both the attacker and defender, as rational expert players, should try to gain information

about the target machine and estimate how much the target is worth to them. The information gathered by both players is not independent. This means that when one player's valuation is high, the other is also likely to be high. This learning information could cause player to re-assess their estimate and decide their expenditure according to this valuation. On the other hand, one might say that the defender always has a better observation about the target's value compared to the attacker. In this case, the attacker is a naïve player in the sense that she competes with the fully rational defender who has the complete information about the target's value. For simplicity, suppose that the defender knows the exact value of the target, which is V, and the attacker make unbiased estimates $v_a = V + e$, where e is an estimation error. If $e > 0$, it means that the attacker over-estimates the target so $v_a > v_d$, but when $e < 0$ we can say that attacker under-estimates the target value and $v_a < v_d$. We can conclude that if the attacker's valuation v_a is less than v_d, then any investment for v_a is a best response for the defender, i.e., attacker wins while investing $S(v_a)$. If the attacker's valuation is equal to v_d then investing $S(v_a)$ by the defender makes her win, so $S(v_a)$ is a best response. If the attacker's valuation v_a exceeds v_d, then any investment for v_a is a best response for the defender.

4.3.2 Nash Equilibrium of n-attacker Game

Now, suppose that the defender has to deal with n attackers, where n is greater than two. We continue to assume that each attacker draws the true value for the target from a uniform distribution on the interval $[0, 1]$. The basic formula for the expected payoff changes but previous analysis continues to hold. The probability that an attacker i with true value v_i

succeed is the probability that no other attacker has a higher valuation, so it is equal to $F(v_i)^{n-1}$. This means that all $n-1$ attackers invest less than the i^{th} attacker. This attacker still needs to beat the defender. Therefore, the expected payoff to v_i is:

$$U_i(v_i) = F(v_i)^n(v_i - S(v_i)) + (1 - F(v_i)^n)(-S(v_i))$$

If the attacker i chooses strategy v_i' instead, the payoff will be

$$U_i(v_i') = F(v_i')^n(v_i) - S(v_i') \tag{20}$$

Then, the attacker i does not want to deviate from strategy $S(v_i)$ to $S(v_i')$ for all v' in the interval $[0, 1]$, provided that derivative of equation (20) is zero when evaluated at $v_i' = v_i$. We assume that the derivative of the cumulative distribution function $F(.)$ is the probability density function $f(.)$ for the distribution. We get the differential equation by analyzing the uniform distribution

$$S'(v_i) = nv_iF(v_i)^{n-1}f(v_i). \tag{21}$$

For the uniform distribution on the interval $[0, 1]$, the cumulative distribution function is $F(v) = v$ and the density is $f(v) = 1$. Thus, from equation (21), we have

$$S'(v_i) = nv_i^n.$$

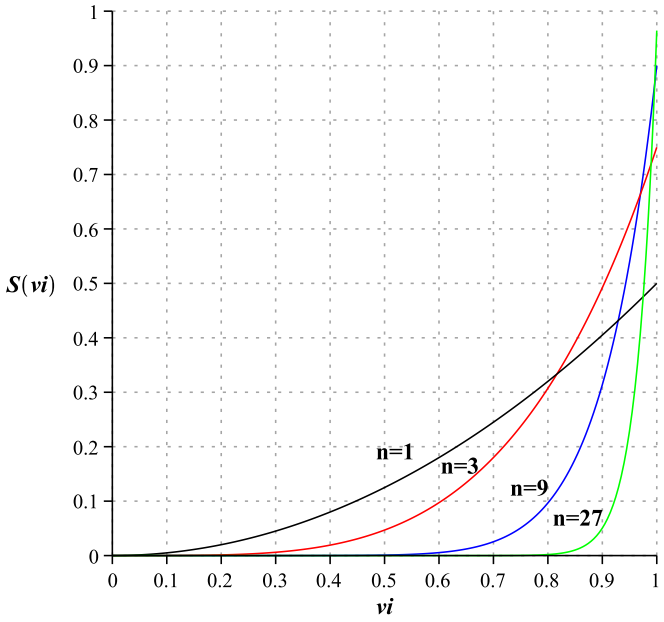
This differential equation is solved by the function

$$S(v_i) = \left(\frac{n}{n+1}\right) v_i^{n+1}. \tag{22}$$

This means that each attacker shades down her investment to implement an attack as her investment is wasted if she does not win. This is an optimal behavior given that every attacker is following this mixed strategy Nash Equilibrium. Since $v_i \leq 1$, raising it to the $n+1^{th}$ power, reduces it exponentially when n (the number of attackers) increases. Notice that $n = 2$ corresponds to our two-player game covered in the previous section.

Figure 3 illustrates the fact that when $v_i <<< 1$, attackers will shade their investment downward significantly as the number of attackers increases.

Figure 3: Equilibrium when the players' valuation follows a Uniform distribution



Games with this type of payoff could arise in a number of situations as an auctions where the notion of "bidding" is implicit. We can set up our game as a sealed-bid all-pay

auctions where bidders are players, and each bidder's strategy is an amount to bid as a function of her "true value" for the item. The fact that everyone must pay in this type of auction causes that bids are typically shaded much lower than in other types of auctions. Moreover, bidders will shade their bids downward significantly as the number of bidders in an all-pay auction increases [16].

4.4 Equilibrium Analysis when Players Valuation Follows a Normal (Gaussian) Distribution Probability

4.4.1 Nash Equilibrium of Two-player Game

The normal (Gaussian) probability distribution with mean μ and standard deviation σ is a normalized Gaussian function defined by

$$g(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(x-\mu)^2}{2\sigma^2}}.$$

The cumulative distribution function is

$$G(x) = \int_{-\infty}^{x} g(x)dx = \frac{1}{2}\big[1 + erf\big(\frac{x-\mu}{\sigma\sqrt{2}}\big)\big].$$

Since we want to know the probability density of the random variable after restricting the support to be between two constants $[a, b]$, we use truncated normal distribution which is

defined as

$$f(x;\mu,a,b) = \frac{g(x)}{G(b) - G(a)} = Tr(x)$$

As before, consider an attacker with target value estimation v_a, and investing strategy function $S(v_a)$. Suppose that the attacker chooses strategy $S(v)$ rather than $S(v_a)$. Thus, the payoff is:

$$U_a(v) = F(v)(v_a - S(v)) + (1 - F(v))(-S(v)),$$

where $F(v)$ is the probability of winning for the attacker and that is the probability that the defender chooses a value less than v. Canceling the common terms in the above equation, we can rewrite it as

$$U_a(v) = F(v)(v_a - S(v))$$

Differentiating with respect to v, we have

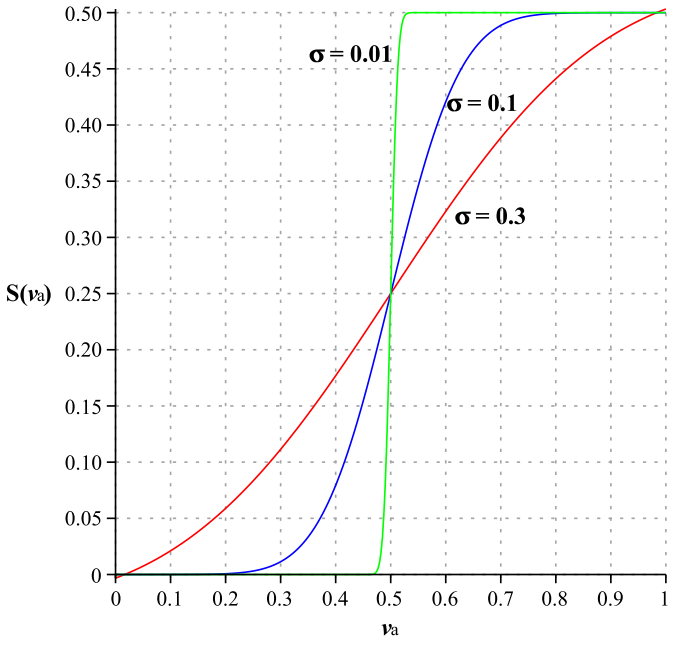
$$\frac{\partial}{\partial v} = F'(v)v_a - S'(v)$$

For $S(v_a)$ to be optimal, this derivative must be zero when evaluated at $v = v_a$. So $S'(v) = F'(v)v_a$. The mathematical steps to compute the optimal strategy of the attacker are detailed in Appendix A. Thus,

$$S(v_a) = \frac{\sqrt{\frac{2}{\pi}}\left[\sqrt{\frac{\pi}{2}}\mu\sigma erf\left(\frac{v_a-\mu}{\sigma\sqrt{2}}\right) - \sigma^2 e^{\frac{-(v_a-\mu)^2}{2\sigma^2}}\right]}{\sigma\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right) - erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]} + \frac{\mu\sigma erf\left(\frac{\mu}{\sigma\sqrt{2}}\right) + \sqrt{\frac{2}{\pi}}\sigma^2 e^{\frac{-\mu^2}{2\sigma^2}}}{\sigma\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right) - erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]} \quad (23)$$

Figure 4, illustrates the fact that if the attacker's valuation is greater than the mean (i.e.

Figure 4: Equilibrium when the players' valuation follows a truncated Gaussian distribution $(n = 1)$



$v_a \geq \mu$) then the attacker will shade her investment downward gradually when the standard deviation, σ, increases. On the other hand, if the attacker's valuation is less than the mean (i.e. $v_a < \mu$), then the attacker will shade her investment upward gradually when standard deviation, σ, increases. Having a relatively large standard deviation models situations when the attacker does not have adequate information about how much the defender invests for protection, whereas small standard deviation models situations when the information about the defender investment is available to the attacker.

Comparing between the uniform distribution and normal distribution cases (Figure 3 and Figure 4) clarifies the fact that in both cases the attacker increases her investment to implement an attack when the value of target increases. Obviously in both cases, it is not rational for the attacker to invest more than 0.5 when the maximum target valuation is 1.

However in the uniform distribution scenario, since the probability for every value of the random variable is equally likely, the attacker always invests slightly less compared to the case of the normal distribution model.

It should be noted that the case of normal distribution with small standard deviation is more likely to model situations in practice since rational players collect information about target value and other parties' valuation before investing in attacks or protection systems. Thus, the probability that the players pick random variable as a target value, is not expected to happen in practice.

4.4.2 Nash Equilibrium of n-attacker Game

Similarly, in the case of n players, the probability that an attacker i with true value v_i succeed, is the probability that no other attacker has a larger value, so it is equal to $F(v_i)^{n-1}$. This means that all other $n-1$ attackers invest less than she does. But she still needs to beat the defender to achieve the target. Therefore, the expected payoff to v_i is given by

$$U_i(v_i) = F(v_i)^n(v_i - S(v_i)) + (1 - F(v_i)^n)(-S(v_i))$$

If the i^{th} attacker chooses strategy v_i' instead, the payoff will be

$$U_i(v_i') = F(v_i')^n(v_i) - S(v_i') \tag{24}$$

Then, attacker i does not want to deviate from strategy $S(v_i)$ to $S(v_i')$ for all v' in the interval $[0, 1]$, provided that derivative of equality (55) is zero when evaluated at $v_i' = v_i$.

$$S'(v_i) = nv_iF'(v_i)F(v_i)^{n-1}$$

Integrating both sides with respect to v_i, we get

$$S(v_i) = \int_0^v nv_iF'(v_i)F(v_i)^{n-1}\,dv_i$$

The mathematical steps to compute the optimal strategy of n attackers is detailed in Appendix A. Thus,

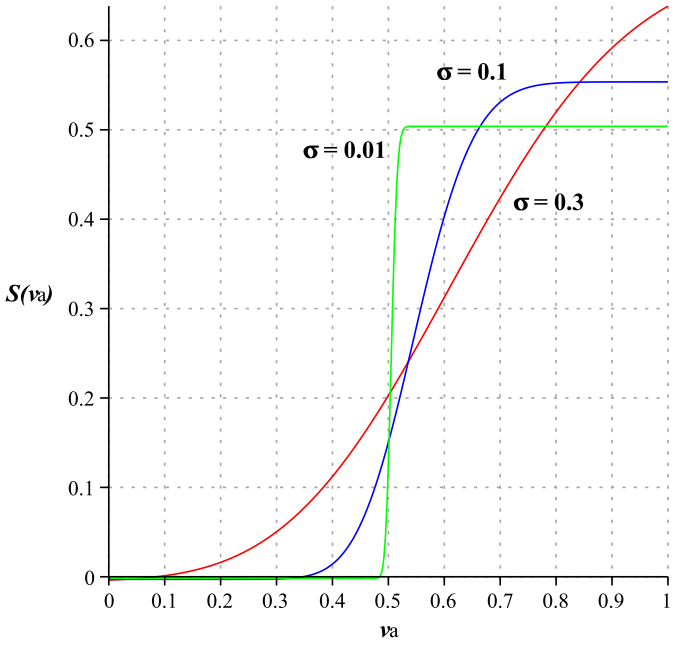
$$S(v_i) = v_i\big[\frac{erf\big(\frac{v_i-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}{erf\big(\frac{b-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}\big]^n - \int_0^v \big[\frac{erf\big(\frac{v_i-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}{erf\big(\frac{b-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}\big]^n dx. \tag{25}$$

Figure 5 illustrate how two attackers' strategy change for $\mu = 0.5$, and $a = 0, b = 1$ and $\sigma \in \{0.01, \sigma = 0.1, \sigma = 0.3\}$. As depicted in the figure, since the attackers' investment are wasted if they do not win, attackers will increase their investment to implement an attack as the number of attackers increases.

4.5 Chapter Summary

In this chapter, we presented a game theoretic framework to analyze the dynamic interaction between attackers and defenders as two-player game. It is assumed that both players

Figure 5: Equilibrium when the players' valuation follows a truncated Gaussian distribution $(n = 2)$



are investing in attack implementation or defence system considering the value of the information asset at risk and the operation costs associated with their strategies. While resource accumulation for the attacker is costly, it increases the severity of the attack and its success likelihood. Similarly, for the defender, investing more in defence systems increases her capability to stop intrusion attempts and malicious activities. Although there is no pure strategy equilibrium for this game, a mixed strategy of a player is a probability distribution over the admissible range of attack to launch and detection configuration to adopt. Our result shows that both players have the same strategy function to map their investment to the target value. This means that when both players follow this equilibrium strategies, the player with the higher target valuation will win the game. We then expand our model to the n player game and formulate the competition among n attackers as well as a defender in

order to find the mixed strategy Nash Equilibria. When the probability of choosing a strategy among all admissible strategies is modeled by a uniform distribution, then depending on the value of V, in some cases, the growth in the number of attackers discourage them to invest money in order to accumulate resources to launch an attack whereas when it is modeled by a Gaussian (normal) distribution, as the number of attackers increases, their motivation to invest money to launch an effective attack increases.

Based on our theoretical analysis, one might argue that the investments associated with Advanced Persistent Threat (APT) attacks are likely to exceed the investment associated with botnet attacks against random targets; the value of the target of an APT attack is more likely to be known and highly appreciated by both the defender and attacker (corresponding to the case with a small standard deviation in our analysis), while the attacker's valuation of a somewhat random target in botnet attacks is likely to be associated with a larger standard deviation.

Chapter 5

Optimal Strategies for Defenders and Worm Propagators

5.1 Introduction

A computer worm is an autonomous malicious program that exploits security flaws in widely-used services and spreads itself without human intervention through computer networks. Worms often discover vulnerable hosts using simple strategies, such as random or sequential scanning of the IP address space. That is, an infected host finds and infects other vulnerable hosts by scanning a list of randomly generated IP addresses.

Fortunately, for the defender who is using standard detecting techniques regularly to look for the continued scanning activities, worms that rely on random scanning strategies are often easy to be detected due to the unceasing scanning activities. As a result, new

sophisticated worms do not always propagate themselves at the highest possible speed, instead they adapt their propagation rates in order to reduce the probability of being detected and therefore infect more computers. For example, "Ata" worm attempts to remain hidden by suspending scans when it suspects it is under detection [46]. After infecting a number of computers without being detected, the worm propagator can remotely control the infected computers and use them to launch further attacks such as distributed denial-of-service (DDoS) attacks, phishing attacks, or identity theft. For example, the "Code-Red" was programmed to unleash a denial-of-service attack on the Whitehouse.gov website by targeting the actual Whitehouse.gov IP address [41]. Thus, to be able to defend against these sophisticated worms, better understanding of the propagation pattern and the impact of the network defender countermeasures such as patching, or spreading an anti-virus software is essential.

Computer worms and biological viruses are similar to one another in their self-replicating and propagation behaviors [13], [24]. Thus, the mathematical techniques that have been settled for the study of biological infectious diseases can be adapted for the study of computer warms and viruses [41], [47]. In epidemiology modeling, hosts that are vulnerable to infection by viruses are called susceptible hosts and hosts that have been infected and can infect others are called infectious hosts. The Kermack-Mckendrick model [18], also known as the SIR model, is a continuous-time Markovian model that describes the spread of a communicable disease in a population. It considers the removal process of infectious hosts by assuming that during an epidemic of a contagious disease, some infectious hosts either recover or die. That is, once a host recovers from the disease, it will be immune to

the disease forever.

In this work, we will use the same terminology for modeling the propagation of computer worms. Thus, each host stays in one of the following states at any time: susceptible, infectious, and removed. The state transition of a host in this system is "susceptible"→ "infectious"→ "removed" or staying in "susceptible" state forever. In particular, we provide an analysis of the worm propagation in the network using the biological epidemic model considering the dynamic defense countermeasure of patching by the defender through the network in order to recover the infected machines and inhibit the spread of the worm propagation. More precisely, we consider the network in which the worm propagator and the defender dynamically decide their optimal propagation rate for the warm and security patches considering their associated costs. The problem is to find the optimal propagation rate of the warm and optimal spreading rate of the security patches for the worm propagator and defender, respectively. This can be formulated as a continuous-time optimal control problem. We combine the propagation process with the game theoretic model (a two-player non-zero sum differential game) and investigate decisions of the players. Furthermore, we mathematically formulate the decision problem using the Pontryagin maximum principle [40] to compute the dynamically evolving optimal worm propagation rate for the worm propagator and optimal recovery rate (i.e., patching rate) for the defender. The obtained results can be used to better understand the worm propagator behavior and can be utilized to inhibit the scale of loss and speed of Internet worms propagation.

5.2 System Model

Throughout this work, we use the ordinary differential equations (ODEs) of Kermack-Mckendrick model as the state equations of the system. Let $I(t)$ and $S(t)$ denote the portion of infectious hosts and susceptible hosts at time t, respectively. Infectious hosts can propagate the worm through communication with susceptible hosts. In addition to adopting various defence techniques such as using Internet Threat Monitoring (ITM) systems to monitor suspicious traffic (e.g., scans unoccupied IP addresses or ports), we assume the network defender spreads security patches through the network in order to remove worms from the infected hosts and grant them permanent immunity. We use $R(t)$ to denote the number of recovered hosts from previously infected hosts at time t. Only susceptible hosts are vulnerable to the worm and the recovered hosts are immune. Thus $S(t)+I(t)+R(t) = 1$ always holds.

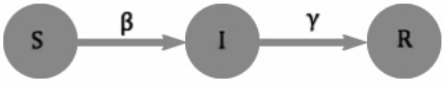


Figure 6: State transitions of the system

Let $\beta(t)$ denote the warm propagation rate at time t and $\gamma(t)$ denote the rate of removal of infectious hosts from circulation at time t. A mathematical model that describes the Kermack-Mckendrick model is given by the following system of differential equations [15]:

$$\begin{aligned} \frac{\partial S(t)}{\partial t} &= -\beta(t)S(t)I(t) \\ \frac{\partial I(t)}{\partial t} &= \beta(t)S(t)I(t) - \gamma(t)I(t) \\ \frac{\partial R(t)}{\partial t} &= \gamma(t)I(t) \end{aligned} \tag{26}$$

with initial states (S_0, I_0, R_0).

We assume that at $t = 0$, a nonzero portion of the hosts are infectious, i.e., $0 < I_0 < 1$. In general, some fraction of the hosts may be previously immunized to the infection, so $0 \leq R_0 < 1$. Using the fact that $S + I + R = 1$, the system of differential equations presented above can be reduced to the following two-dimensional system

$$\begin{aligned} \frac{\partial S(t)}{\partial t} &= -\beta(t)S(t)I(t) \\ \frac{\partial I(t)}{\partial t} &= \beta(t)S(t)I(t) - \gamma(t)I(t) \end{aligned} \tag{27}$$

with the state constraints $I, S \geq 0,\ S + I \leq 1$.

As we can see from the system dynamics in (27), the growth in the cleaning rate, $\gamma(t)$, can repress the propagation of the malware. With defensive systems in place, a worm propagator may attempt a more sophisticated spreading technique and change its propagation rate in order to avoid the detection and infect as many susceptible hosts as possible. The defense strategy of performing security patches and spreading anti-malware software across the network is a costly process which motives the defender to adjust the rate of spreading security patches in order to find a good trade-off between the costs of performing such patches and updates and the potential loss caused by infected/infectious hosts. Thus, the worm propagation rate, $\beta(t)$, and hence the recovery rate, $\gamma(t)$, can present the control variable from the two players which are bounded between a maximum and minimum values: $0 \leq \beta \leq 1,\ 0 \leq \gamma \leq 1$.

We now integrate the worm propagation process into our game model to form a two-player non-zero sum differential game and investigate the decisions of the two players. In

this game, we have two players: the worm propagator and the defender. We consider different schemes in which each player can choose to have either a fixed or variable control (strategy) during the attack session. We mathematically formulate the decision problems using the Pontryagin maximum principle, which is commonly used in optimal control theory [40] to compute the optimum decision rules and the Nash Equilibrium of the game. Finally, we validate our result by some numerical examples.

We denote the state of the system (i.e., the number of susceptible and infectious hosts in time t) by the vector x. So from equation (27) we have:

$$\dot{\mathrm{x}} = \frac{\partial}{\partial t} \begin{pmatrix} S(t) \\ \\ I(t) \end{pmatrix} = f\big(x(t), \beta(t), \gamma(t)\big) \tag{28}$$

With the initial condition $x_0 = \begin{pmatrix} S_0 \\ \\ I_0 \end{pmatrix}$.

The controls $\beta(t)$ and $\gamma(t)$ represent the strategies adopted by the worm propagator and the defender, respectively in $t \in [0, T]$.

Let J_w,J_d donate the payoff function for the worm propagator and the defender, respectively. Then we define J_w and J_d as follows [42]:

$$J_w = K_w[x(T)] + \int_0^T F_w(x, \beta, \gamma, t)dt \tag{29}$$

$$J_d = K_d[x(T)] + \int_0^T F_d(x, \beta, \gamma, t)dt \tag{30}$$

Naturally, each payer wants to maximize her payoff function. Here $K_w[x(T)]$ and $K_d[x(T)]$

are the terminal payoffs for the worm propagator and the defender, while F_w and F_d account for the instantaneous payoffs for the worm propagator and the defender, respectively. We define V_w and V_d as the value of the network for the worm propagator and the defender, respectively. So the terminal payoffs for the worm propagator and the defender can be presented as $K_w[x(T)] = I(T)V_w$ and $K_d[x(T)] = -I(T)V_d$ where larger values of $I(T)$ implies a larger number of infected host at the end of the botnet recruitment cycle which will allow the bot master to launch DDoS attacks more effectively.

Aside from the above one-time cost associated with the number of infectious hosts at time T for the defender and the worm propagator, we also include a period-dependent operating cost incurred every period when the cleaning rate $\gamma(t)$ and the propagation rate $\beta(t)$ are implemented by the defender and the worm propagator, respectively. We defined instantaneous payoff as $F_w = -\frac{\beta(t)^2}{2}$ and $F_d = -\frac{\gamma(t)^2}{2}$ for the worm propagator and the defender, respectively. To clarify what we mean by operating cost for the defender, we associate this cost with the set of technologies or resources that are adapted by the defender to provide cleaning procedures (e.g., running anti-virus tools and performing patches and software updates) across the network. For the worm propagator, we consider this cost as the cost of being detected by the defender, which is a function of the worm propagation rate. That is, the probability that the worm propagator remains undetected decrease when she chooses to increase its propagation rate. Thus, F_w will increase when the worm propagates with a higher rate because it can be detected more easily. Therefore, we can rewrite

equations (29) and (30) as

$$J_w = I(T)V_w - \int_0^T \frac{\beta(t)^2}{2} dt \tag{31}$$

$$J_d = -I(T)V_d - \int_0^T \frac{\gamma(t)^2}{2} dt \tag{32}$$

In this case, the Nash solution is defined by the admissible strategy trajectories (β^*, γ^*) which have the properties that

$$\begin{aligned} J_w(\beta^*, \gamma^*) &= max_\beta J_w(\beta, \gamma^*), \\ J_d(\beta^*, \gamma^*) &= max_\gamma J_d(\beta^*, \gamma) \end{aligned} \tag{33}$$

Here β^* and γ^* stand for $\beta(t)^*$, $t \in [0, T]$, and $\gamma(t)^*$, $t \in [0, T]$, respectively.

We can now apply the Pontryagin's Maximum Principle [38] on the unconstrained optimal control problem considering continuous control $\beta(\cdot)$, $\gamma(\cdot)$ and the corresponding state functions (S, I). The Hamiltonian H is the following function of the co-state or adjoint variables λ_1 and λ_2 for each player:

$$H_w = F_w + \lambda_w f = -\frac{\beta(t)^2}{2} + \beta(t)S(t)I(t)(\lambda_{w2} - \lambda_{w1}) - \gamma\lambda_{w2}I(t) \tag{34}$$

$$H_d = F_d + \lambda_d f = -\frac{\gamma(t)^2}{2} + \beta(t)S(t)I(t)(\lambda_{d2} - \lambda_{d1}) - \gamma\lambda_{d2}I(t) \tag{35}$$

Here, the following variational equation holds for the co-state λ_{w1} and λ_{w2} of the worm

propagator [28]:

$$\dot{\lambda}_{w1} = -\frac{\partial H_w}{\partial S} = \beta(t)I(t)(\lambda_{w1} - \lambda_{w2}) \tag{36}$$

$$\dot{\lambda}_{w2} = -\frac{\partial H_w}{\partial I} = \beta(t)S(t)(\lambda_{w1} - \lambda_{w2}) - \gamma\lambda_{w2} \tag{37}$$

Similarly, for the defender:

$$\dot{\lambda}_{d1} = -\frac{\partial H_d}{\partial S} = \beta(t)I(t)(\lambda_{d1} - \lambda_{d2}) \tag{38}$$

$$\dot{\lambda}_{d2} = -\frac{\partial H_d}{\partial I} = \beta(t)S(t)(\lambda_{d1} - \lambda_{d2}) - \gamma\lambda_{d2} \tag{39}$$

The state and co-state variables $(S, I, \lambda_{w1}, \lambda_{w2}, \lambda_{d1}, \lambda_{d2})$ are continuous functions of time and the chosen optimal controllers β^*, γ^* maximize the Hamiltonian $H_w = H_w(\beta)$, $H_d = H_d(\gamma)$ among all admissible β's and γ's, respectively.

$$\begin{aligned} H_w(\beta^*) &= max_\beta H_w(\beta), \\ H_d(\gamma^*) &= max_\gamma H_d(\gamma) \end{aligned} \tag{40}$$

5.3 Optimal Control

In order to calculate our dynamic policies, an estimation of the parameters of the system is required. We define different baseline scenarios to compute the dynamic optimal control of both players in order to maximize their payoff. First we assume the case where one player has a fixed constant control whereas the other player's control is a function of time. Then, we derive the optimum policy of the players for the case where both players vary their

control. For all the scenarios, we assume that the terminal time is fixed. The motivation behind this assumption is that the worm propagator aims to compromise as many hosts as possible before a pre-set time and recruit them to execute some illicit actions such as spamming and DDoS attacks.

We analyze the different behavior of the worm propagator and the defender in different environments where they have a static or dynamic spreading rate. In the case of static rate, the player initially selects the propagation rate at the initial time of the game and maintains the same strategy during the game. On the other hand, in dynamic spreading rates, the players may dynamically adjust their propagation during the game.

5.3.1 Fixed Terminal Time T, Fixed Recovery Rate γ, Free Terminal State $x(T)$:

Suppose we have a network of hosts where the defender chooses to perform patching at a constant rate (i.e., γ is constant). The objective is to find the optimal worm propagation rate for the worm propagator within the terminal time condition T. The worm propagator should plan her strategy $t \rightarrow \beta(t)$ in order to maximize the reward from the infected hosts considering value of the network and the cost associated with the increase in the worm propagation rate. Fixing the terminal time, gives the following final value constraints for co-states λ_{w1} and λ_{w2} :

$$\dot{\lambda}_{w1}(T) = \frac{\partial}{\partial S(T)} I(T) V_w = 0 \tag{41}$$

$$\dot{\lambda}_{w2}(T) = \frac{\partial}{\partial I(T)} I(T) V_w = V_w \tag{42}$$

The Nash control β^* for the worm propagator is obtained by its Hamiltonian H_w with respect to β, i.e., β^* must satisfy

$$H_w(x^*, \beta^*, \lambda_w, t) \geq H_w(x^*, \beta, \lambda_w, t), \ \forall t \in [0, T]. \tag{43}$$

From equation (34), the Hamiltonian maximizing condition leads to

$$\beta(t)^* = \begin{cases} 0, & S(t)I(t)(\lambda_{w2} - \lambda_{w1}) < 0.5 \\ S(t)I(t)(\lambda_{w2} - \lambda_{w1}), & 0.5 \leq S(t)I(t)(\lambda_{w2} - \lambda_{w1}) \leq 1, \\ 1, & S(t)I(t)(\lambda_{w2} - \lambda_{w1}) > 1 \end{cases} \tag{44}$$

Substituting (44) in (27), (36) and (37) and using the terminal conditions for the co-states system, (41) and (42), we get a system of ODEs which can be solved using the standard boundary value problem ODE solving techniques. In section V, we numerically solve the optimum control for the worm propagation rate using the Maple ODE analyzer.

5.3.2 Fixed Terminal Time T, Fixed worm propagation rate β, Free Terminal State $x(T)$

Suppose we have a network of hosts in which the worm propagator chooses to propagate a worm with a fixed rate across the network (i.e., β is constant). The objective is to find the optimal recovery rate for the defender within the terminal time condition T. The defender should plan its strategy $t \rightarrow \gamma(t)$ in order to minimize her loss from the infected hosts

seeing value of the network by considering the cost associated with increasing the recovery rate. Similarly, fixing the terminal time gives the following final value constraints for co-states λ_{d1} and λ_{d2} :

$$\dot{\lambda}_{d1}(T) = \frac{\partial}{\partial S(T)} - I(T)V_d = 0 \tag{45}$$

$$\dot{\lambda}_{d2}(T) = \frac{\partial}{\partial I(T)} - I(T)V_d = -V_d \tag{46}$$

The Nash control γ^* for the defender is obtained by its Hamiltonian H_d with respect to γ, i.e., γ^* must satisfy

$$H_d(x^*, \gamma^*, \lambda_d, t) \geq H_d(x^*, \gamma, \lambda_d, t),\ \forall t \in [0, T]. \tag{47}$$

From equation (35), the Hamiltonian maximizing condition leads to

$$\gamma(t)^* = \begin{cases} 0, & \lambda_{d2} I(t) \geq 0 \\ -\lambda_{d2} I(t), & -1 < \lambda_{d2} I(t) < 0 \\ 1, & \lambda_{d2} I(t) \leq -1 \end{cases} \tag{48}$$

Substituting (48) in (27), (38) and (39) and using the terminal conditions for the co-states system, (45) and (46), we get a system of ODEs. In section V, we numerically solve the optimum recovery rate for the defender using the Maple ODE analyzer.

5.3.3 Fixed Terminal Time T, Free Terminal State $x(T)$

Consider the case where the strategies adopted by the worm propagator and the defender $\big(\beta(t)$ and $\gamma(t)\big)$ are both varied with time. The goal of the worm propagator is to create as many infectious hosts as possible taking into account the other cost associated with a higher infection rate. Similarly, the defender aims to protect herself and recover as many hosts as possible taking into account the other cost associated with a higher recovery rate. The Nash control β^* for the worm propagator is obtained by its Hamiltonian H_w with respect to β, i.e., β^* must satisfy

$$H_w(x^*, \beta^*, \gamma^*, \lambda_w, t) \geq H_w(x^*, \beta, \gamma^*, \lambda_w, t),, \ \forall t \in [0, T]. \tag{49}$$

Thus, the Hamiltonian maximizing condition leads to the equation (44). Similarly for the defender the Nash control γ^* is obtained by its Hamiltonian H_d with respect to γ, i.e., γ^* must satisfy maximizing

$$H_d(x^*, \beta^*, \gamma^*, \lambda_d, t) \geq H_d(x^*, \beta^*, \gamma, \lambda_d, t) \tag{50}$$

in $t \in [0, T]$.

Therefore, the Hamiltonian maximizing condition leads to the equation (48).

5.4 Numerical Analysis

In this section, we present numerical examples to provide a better insight into the theoretical models developed in the previous section. The time horizon T is fixed to 1 in order to clarify the variations in the optimum controls, $\beta(t)$ and $\gamma(t)$, as a result of changes in I_0, S_0, V_w, and V_d.

Figure 7 illustrates the first scenario when the effective recovery rate is constant over time. Thus, $\gamma(t) = \gamma, \forall t \in [0, 1]$. It shows that when the portion of susceptible hosts grows, the incentive of the worm propagator to spread the worm propagation will also increase. Beside, when the initial portion of infected hosts rises, the worm propagates in the network more aggressively.

Figure 8 shows the second scenario when the worm propagation rate is constant over time. Thus, $\beta(t) = \beta, \forall t \in [0, 1]$. As shown in the figure, the recovery rate is changing as a result of variation of worm propagation rate across the network. It is clear that the growth in the portion of initial infected hosts has more effect on the recovery rate compared to the increase in the portion of susceptible hosts.

Figure 9 shows the two-player nonzero-sum differential games between the worm propagator and the defender of the network where the controls $\beta(t)$ and $\gamma(t)$ represent their different strategies in $t \in [0, T]$. We changed the value of the network for both players (i.e., V_w and V_d) to see how the players would vary their strategies in response to this. Clearly, the value of the network is the key factor for both players when choosing their strategies. But aside from that we can conclude that the growth in the portion of susceptible hosts

and infected hosts will increase the incentive of the worm propagator to spread the worm across the network. More precisely, the growth in the number of susceptible hosts increases the aggressiveness of the worm propagation across the network whereas growth in the initial infected hosts increases the incentive of the worm propagator to propagate the worm through the network even when the network is less valuable for her.

5.5 Chapter Summary

In this chapter, we presented a two-player non-zero sum differential game in order to investigate optimal controls (decisions) for the worm propagator and the defender. We characterize optimal controls using the Pontryagin maximum principle and computed the dynamically evolving optimal worm propagation rate and recovery rate for the worm propagator the defender, respectively. The developed models leads to a better understanding of the worm propagator behavior and can be utilized by security professionals to determine the optimal response when trying to slow down the speed of worm propagation and narrow their scale of damage.

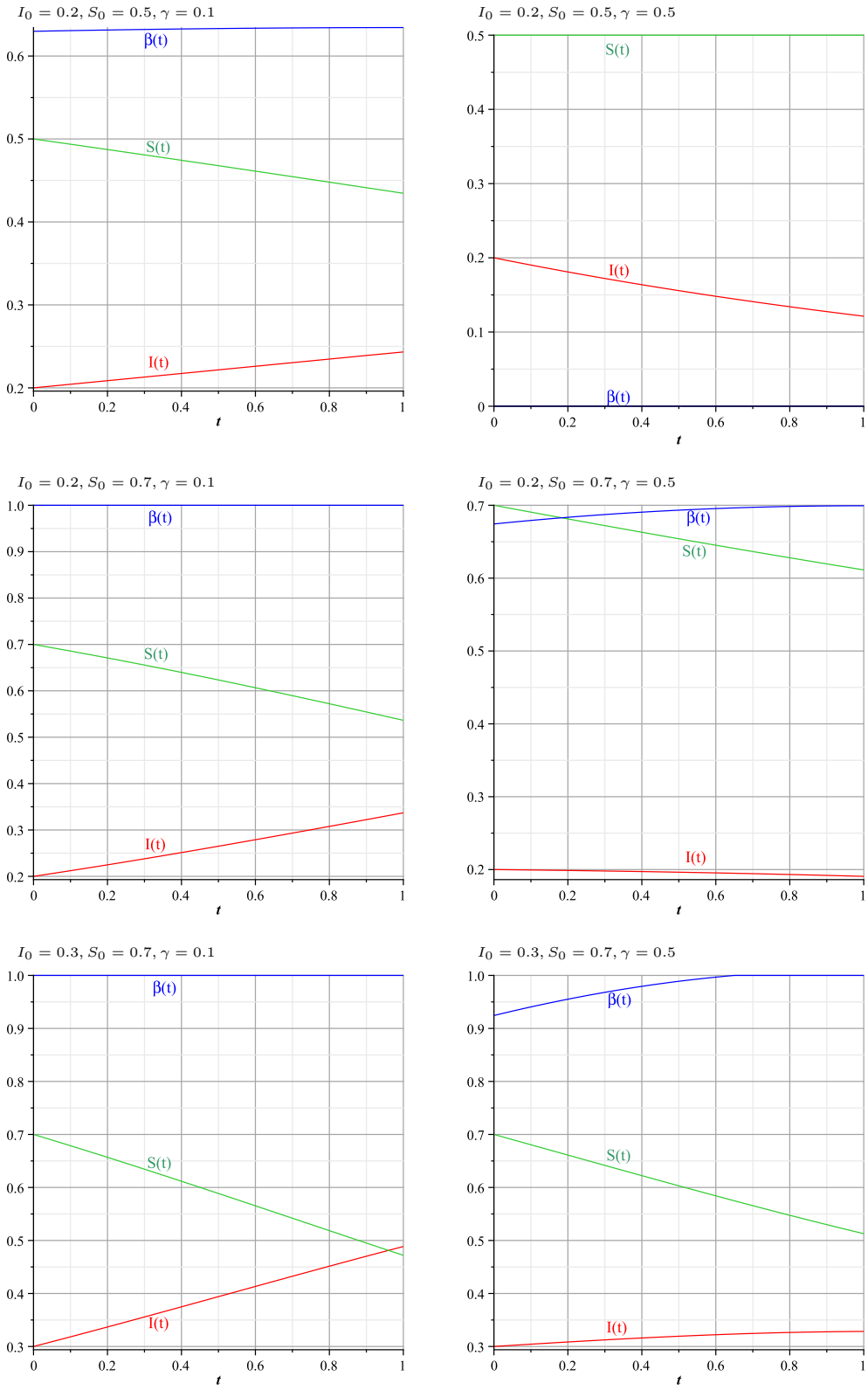


Figure 7: Optimal control of the worm propagator when the recovery rate is constant over time and $V_w = 6$.

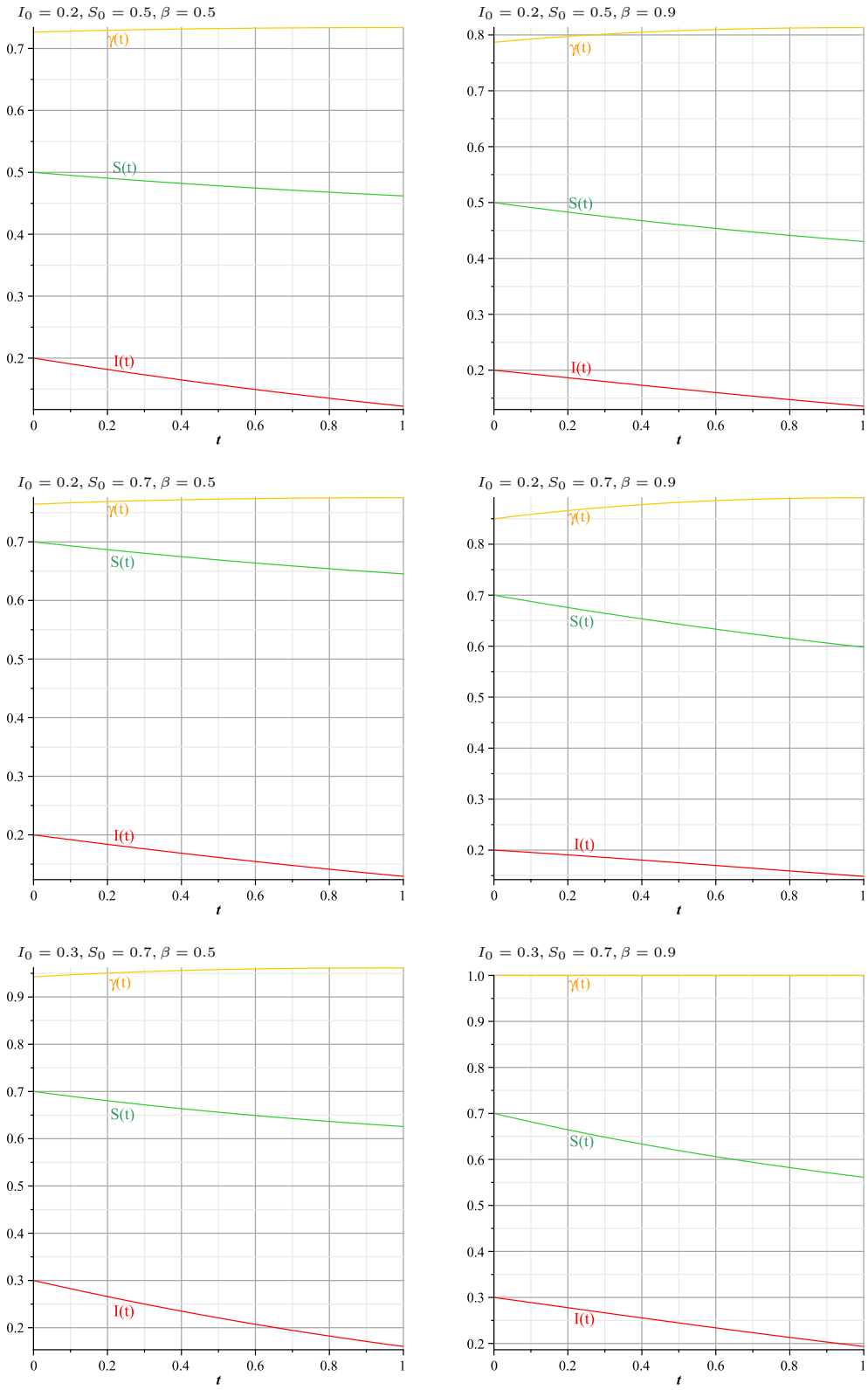


Figure 8: Optimal control of the defender when the worm propagation rate is constant over time and $V_d = 6$.

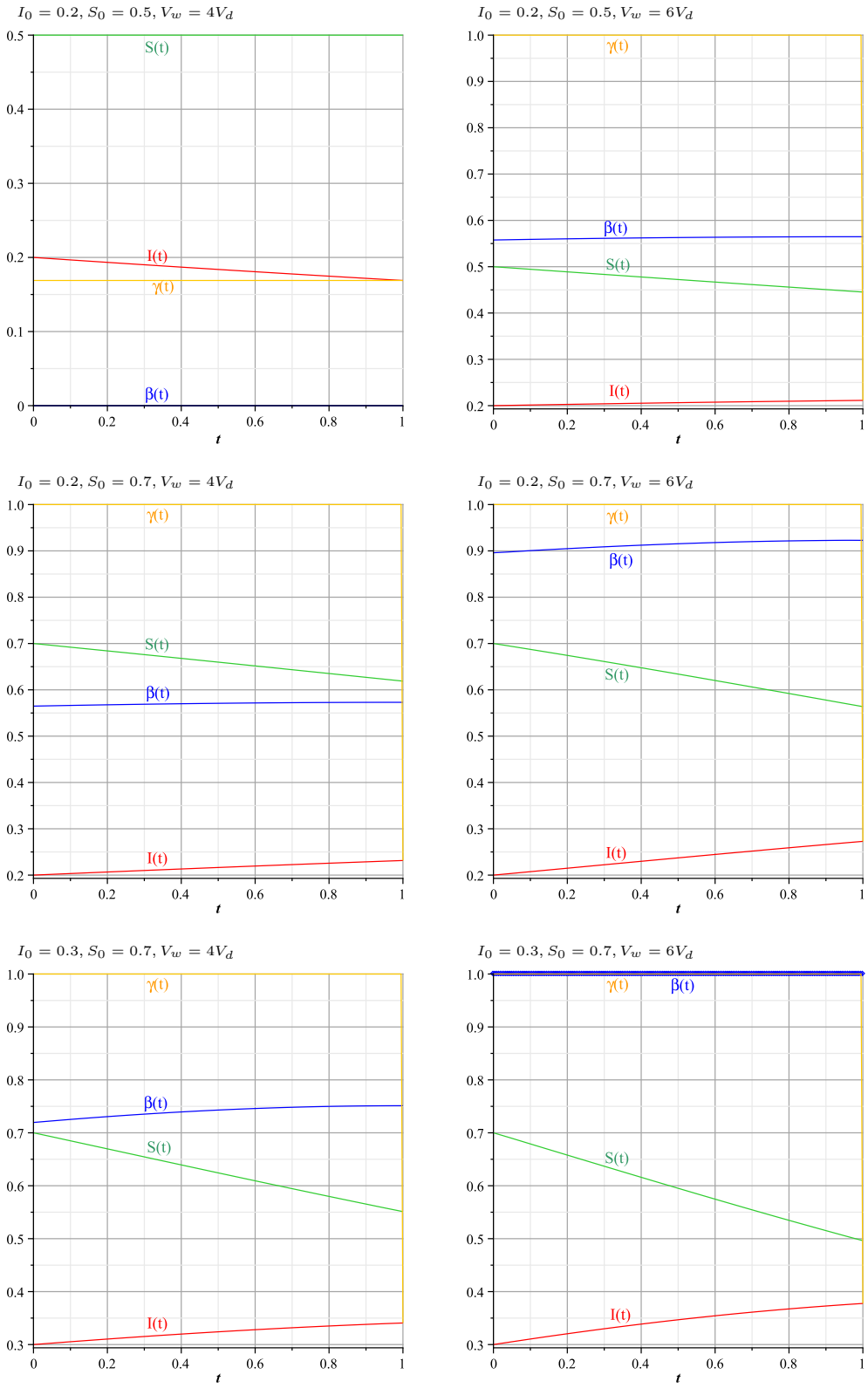


Figure 9: Optimal controls of the defender and the worm propagator when $V_d = 1$.

Chapter 6

Conclusions and Future Work

6.1 Summary and Conclusions

To illustrates the potential usefulness of game theory in studying information systems security, in this thesis we provided game theoretic models for several information systems security problems. In particular, we analyzed the strategic behaviour of ISPs and network administrators. The decision of these key market players when they are confronted with security incidents greatly influence the state of the Internet security. More precisely, throughout this thesis, we presented a game theoretic framework to analyze the interaction between two ISPs who have to decide whether or not to deploy security solutions among their subscribers to prevent, detect, and mitigate cyber security incidents and improve the overall security of the Internet. The market share of the ISPs and the security awareness of their customers can provide efficient economic incentives for the ISPs to take a role in improving the state of the Internet security. However there are scenarios where ISPs may

not be willing to deploy security policies in order to maximize their financial gain. Our analysis shows the need for laws and regulations that can drive ISPs in order to take actions towards enhancing the global security of the Internet. The limitation of this approach is that, in reality, ISPs are scattered over different geographical and political regions that follow different laws and in many situations it might be practically impossible to impose common laws on these ISPs.

Then, we presented a game theoretic framework to analyze the dynamic interaction between attackers and defenders as two-player game considering the associated cost for investing in attack and defense systems. In our multi attacks environment, the defender should adopt the best configuration of defense to trade-off between the deploying cost of security solutions and the information asset at risk. Similarly the attacker should balance the attack implementation cost and benefit of successful attack. Our analysis shows that if the attacker's valuation of the target machine follows a uniform distribution, most probably she will lose interest in investing to launch an attack when competing with other attackers. On the other hand, when the attacker's valuation follows a normal distribution, the incentive of the attacker to invest in more aggressive attacks increases as the number of attackers (competing for the same target) increases.

Finally, we used the mathematical models of biological infectious disease to formulate the propagation of computer worms in the network with defense mechanism of patching to clean the infected hosts by the defender. As sophisticated worms deliberately modify their propagation rate in order to avoid detection, defenders should also find the optimal patching rate to balance between the operating costs and the loss caused by infectious

hosts. We presented a differential game in order to investigate optimal spreading rate of worms and optimal patching rates by the worm propagator and the defender, respectively. Although the presented approach does not prevent the worm propagation, it can be used by security professionals to determine the optimal response to slow down the speed of worm propagation rate and narrow down the scale of damage.

6.2 Future Work

Based on the research elaborated in this thesis, further studies can be conducted in the following directions.

- Develop more accurate models that capture the effect of economic incentives, laws and regulations in improving the role of ISPs in enhancing the global security of the Internet.

- We have developed a game theoretic model to study the barriers and incentives for two ISPs deploying cyber security solutions. Given the fact that in real world there are many ISPs who compete together to increase their market share and maximize their financial gain, further research is required to generalize this model as an n-player game.

- In the defender-attacker game, both players can gain information by plugging in a reinforcement learning algorithm [29] where players adaptively interact with each other and based on available actions and observed rewards, the players decide the

optimal policy more intelligently. Deploying dynamic learning methods [20] can be embedded to solve these security games.

Bibliography

[1] T. Alpcan and T. Basar. A game theoretic approach to decision and analysis in network intrusion detection. *In Proceeding of the 42nd IEEE Conference on Decision and Control (CDC)*, 3:2595–2600, 2003.

[2] N. Anderson. Report:one quarter of all computers part of a botnet. *http://arstechnica.com/uncategorized/2007/01/8707/*, 2007.

[3] R. Anderson, R. Bohme, R. Clayton, and T. Moore. Analyzing barriers and incentives for network and information security in the internal market for e-communication (2008).

[4] R. Anderson and T. Moore. Information security economics and beyond. pages 68–91. Springer, 2007.

[5] T. August and TI. Tunca. Who should be responsible for software security? a comparative analysis of liability policies in network environments. *Management Science*, 57(5):934–959, 2011.

[6] T. August and TI. Tunca. Comments on incentives to adopt improved cybersecurity practices. 2013.

[7] A. Bressan. Noncooperative differential games. a tutorial. *Department of Mathematics, Penn State University*, 2010.

[8] H. Cavusoglu, B. Mishra, and S. Raghunathan. The effect of internet security breach announcements on market value,capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1):70–104, 2004.

[9] N. Christin, J. Grossklags, B. Johnson, and J. Chuang. Are security experts useful? Bayesian nash equilibria for network security games with limited information, 2010.

[10] C. SANTA CLARA. Report: Mcafee alert: One in every six personal computers have zero protection. *http://www.mcafee.com/ca/about/news/2012/q2/20120530-01.aspx*, 2012.

[11] R. Clayton. Might governments clean-up malware? *Communication, and Strategies*, (81):87–104, 2011.

[12] S. Savage C. Shannon D .Moore, V. Paxson, S. Staniford, and N. Weaver. Inside the slammer worm. *IEEE Security & Privacy*, 1(4):33–39, 2003.

[13] DJ. Daley, J. Gani, and JM. Gani. *Epidemic modelling: an introduction*, volume 15. Cambridge University Press, 2001.

[14] D.Reeves. Economic analysis of isp provided cyber security solutions. 2011.

[15] DJD. Earn. A light introduction to modelling recurrent epidemics. pages 3–17. Springer, 2008.

[16] D. Easley and J. Kleinberg. *Networks, crowds, and markets*, volume 8. Cambridge Univ Press, 2010.

[17] MJG. Van Eeten and JM. Bauer. Economics of malware: Security decisions, incentives and externalities. Technical report, OECD Publishing, 2008.

[18] JC. Frauenthal. *Mathematical modeling in epidemiology*. Springer-Verlag, New York, 1980.

[19] A. Garcia and B. Horowitz. The potential for underinvestment in internet security: implications for regulatory policy. *Journal of Regulatory Economics*, 31(1):37–55, 2007.

[20] J. Hu and MP. Wellman. Nash q-learning for general-sum stochastic games. *The Journal of Machine Learning Research*, 4:1039–1069, 2003.

[21] H.Varian. Managing online security risks,economic science column, the new yorkt imes. *http://www.nytimes.com/library/financial/columns/060100econ-scene.html*, June 1,2000.

[22] international Mass-Marketing Fraud Working Group. Report:mass-marketing fraud: A threat assessment. *http://www.fbi.gov/stats-services/publications/mass-marketing-fraud-threat-assessment*, 2010.

[23] V. Jose, R. Richmond, and J. Zhuang. Technology adoption, accumulation, and competition in multi-period attacker-defender games. 2012.

[24] JO. Kephart, SR. White, and DM. Chess. Computers and epidemiology. *Spectrum, IEEE*, 30(5):20–26, 1993.

[25] MHR. Khouzani, E. Altman, and S. Sarkar. Optimal quarantining of wireless malware through reception gain control. *Automatic Control, IEEE Transactions on*, 57(1):49–61, 2012.

[26] MHR. Khouzani, S. Sarkar, and E. Altman. Maximum damage malware attack in mobile wireless networks. *Networking, IEEE/ACM Transactions on*, 20(5):1347–1360, 2012.

[27] W. Lee, M.Miller W. Fan, SJ. Stolfo, and E. Zadok. Toward cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security*, 10(1):5–22, 2002.

[28] FL. Lewis, D. Vrabie, and VL. Syrmos. *Optimal control*. John Wiley & Sons, 2012.

[29] ML. Littman. Markov games as a framework for multi-agent reinforcement learning. *ICML*, 94:157–163, 1994.

[30] Y. Liu, C. Comaniciu, and H. Man. A bayesian game approach for intrusion detection in wireless ad hoc networks. *Proceeding from the 2006 workshop on Game theory for communications and networks*, page 4, 2006.

[31] D. Moore and C. Shannon. Code-red: a case study on the spread and victims of an internet worm. *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*, pages 273–284, 2002.

[32] T. Moore. The economics of cybersecurity: principles and policy options. *International Journal of Critical Infrastructure Protection*, 3(3):103–117, 2010.

[33] J. Nash. Non-cooperative games. *Annals of mathematics*, pages 286–295, 1951.

[34] J. Von Neumann and O. Morgenstern. *Theory of Games and Economic Behavior (60th Anniversary Commemorative Edition)*. Princeton university press, 2007.

[35] MJ. Osborne. *An introduction to game theory*, volume 3. Oxford University Press New York, 2004.

[36] MJ. Osborne and A. Rubinstein. *A course in game theory*. MIT press, 1994.

[37] Royal Canadian Mounted Police. Identity theft and identity fraud. *http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm*, 2013.

[38] LS. Pontryagin. *Mathematical theory of optimal processes*. CRC Press, 1987.

[39] R.Anderson. Why information security is hard-an economic perspective. *Computer Security Applications Conference, 2001 ACSAC 2001 Proceedings 17th Annual*, pages 358–365, 2001.

[40] A. Seierstad and K. Sydsaeter. *Optimal control theory with economic applications*, volume 20. North-Holland Amsterdam, 1987.

[41] S. Staniford, V. Paxson, and N. Weaver. How to own the internet in your spare time. *USENIX Security Symposium*, pages 149–167, 2002.

[42] AW. Starr and YC. Ho. Nonzero-sum differential games. *Journal of Optimization Theory and Applications*, 3(3):184–206, 1969.

[43] JR. Vacca. *Computer and information security handbook*. Morgan Kaufmann, 2009.

[44] M. van Eeten, JM. Bauer, H. Asghari, S. Tabatabaie, and D. Rand. The role of internet service providers in botnet mitigation: An empirical analysis based on spam data. Technical report, OECD Publishing, 2010.

[45] D. Wood and B. Rowe. Assessing home internet users' demand for security: Will they pay ISPs? *WEIS*, 2011.

[46] W. Yu, N. Zhang, X. Fu, and W. Zhao. Self-disciplinary worms and countermeasures: modeling and analysis. *IEEE Transactions on Parallel and Distributed Systems*, 21(10):1501–1514, 2010.

[47] CC. Zou, W. Gong, and D. Towsley. Code red worm propagation modeling and analysis. *Proceedings of the 9th ACM conference on Computer and communications security*, pages 138–147, 2002.

Appendix A

In the appendix, we compute the optimal strategy of the attacker in the two-player game and n-player game that we presented in Chapter 4.

A.1 Equilibrium Analysis for Truncated Distribution Case

A.1.1 Nash Equilibrium of Two-player Game

Following the same notation as in Chapter 4, the cumulative distribution function is given by

$$G(x) = \int_{-\infty}^{x} g(x)dx = \frac{1}{2}\big[1 + erf\big(\frac{x-\mu}{\sigma\sqrt{2}}\big)\big].$$

Since we want to know the probability density of the random variable after restricting the support to be between two constants $[a, b]$, we use truncated normal distribution which is defined as

$$f(x; \mu, a, b) = \frac{g(x)}{G(b) - G(a)} = Tr(x)$$

So, we can rewrite it as

$$f(x;\mu,a,b) = \frac{\frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(x-\mu)^2}{2\sigma^2}}}{\frac{1}{2}\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right)\right] - erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]} \tag{51}$$

Where the cumulative distribution function for the truncated normal distribution is given by

$$F(x;\mu,a,b) = \frac{erf\left(\frac{x-\mu}{\sigma\sqrt{2}}\right) - erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)}{erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right) - erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)} \tag{52}$$

Since

$$F'(v,\mu,a,b) = \frac{\sqrt{\frac{2}{\pi}} e^{\frac{-(v-\mu)^2}{2\sigma^2}}}{\sigma\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right) - erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]}, \tag{53}$$

from $S'(v) = F'(v)v_a$, we have

$$S'(v) = \frac{v_a\sqrt{\frac{2}{\pi}} e^{\frac{-(v-\mu)^2}{2\sigma^2}}}{\sigma\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right) - erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]}.$$

Integrating both sides with respect to v_a, we get

$$S(v_a) = \frac{\sqrt{\frac{2}{\pi}}\left[\sqrt{\frac{\pi}{2}}\mu\sigma erf\left(\frac{v_a-\mu}{\sigma\sqrt{2}}\right) - \sigma^2 e^{\frac{-(v_a-\mu)^2}{2\sigma^2}}\right]}{\sigma\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right) - erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]} + constant.$$

Since we assumed $S(0) = 0$, Thus we have

$$S(v_a) = \frac{\sqrt{\frac{2}{\pi}}\left[\sqrt{\frac{\pi}{2}}\mu\sigma erf\left(\frac{v_a-\mu}{\sigma\sqrt{2}}\right) - \sigma^2 e^{\frac{-(v_a-\mu)^2}{2\sigma^2}}\right]}{\sigma\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right) - erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]} + \frac{\mu\sigma erf\left(\frac{\mu}{\sigma\sqrt{2}}\right) + \sqrt{\frac{2}{\pi}}\sigma^2 e^{\frac{-\mu^2}{2\sigma^2}}}{\sigma\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right) - erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]} \tag{54}$$

A.1.2 Nash Equilibrium of n-player Game

If the ith attacker chooses strategy v_i' insted, her payoff will be

$$U_i(v_i') = F(v_i')^n(v_i) - S(v_i') \tag{55}$$

Then, the ith attacker does not want to deviate from strategy $S(v_i)$ to $S(v_i')$ for all v' in the interval $[0, 1]$, provided that derivative of equality (55) is zero when evaluated at $v_i' = v_i$.

$$S'(v_i) = nv_iF'(v_i)F(v_i)^{n-1}$$

Integrating with respect to v_i both sides, we get

$$S(v_i) = \int nv_iF'(v_i)F(v_i)^{n-1}\,dv_i$$

If we assume $V = nF'(v_i)F(v_i)^{n-1}$and $U = v_i$, by using integration by parts theorem, we have

$$\int UV\,dv_i = U\int V\,dv_i - \int \big(U'\int V\,dv_i\big).$$

Thus,

$$S(v_i) = v_iF(v_i)^n - \int F(v_i)^n\,dv_i$$

From equations (52) and (53), we get

$$S'(v_i) = \frac{nv_i\sqrt{\frac{2}{\pi}}e^{\frac{-(v_i-\mu)^2}{2\sigma^2}}}{\sigma\big[erf\big(\frac{b-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)\big]}\big[\frac{erf\big(\frac{v_i-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}{erf\big(\frac{b-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}\big]^{n-1}$$

$$S(v_i) = v_i\big[\frac{erf\big(\frac{v_i-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}{erf\big(\frac{b-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}\big]^{n} - \int \big[\frac{erf\big(\frac{v_i-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}{erf\big(\frac{b-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}\big]^{n} dx. \tag{56}$$

Thus for $n = 1$, we have

$$\int \big[\frac{erf\big(\frac{v_i-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}{erf\big(\frac{b-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}\big]\, dx =$$

$$\frac{-v_i erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big) + (v_i-\mu)erf\big(\frac{v_i-\mu}{\sigma\sqrt{2}}\big) + \sqrt{\frac{2}{\pi}}\sigma e^{\frac{-(v_i-\mu)^2}{2\sigma^2}}}{erf\big(\frac{b-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)}$$

$$S(v_a) = \frac{\sqrt{\frac{2}{\pi}}\big[\sqrt{\frac{\pi}{2}}\mu\sigma erf\big(\frac{v_a-\mu}{\sigma\sqrt{2}}\big) - \sigma^2 e^{\frac{-(v_a-\mu)^2}{2\sigma^2}}\big]}{\sigma\big[erf\big(\frac{b-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)\big]} + constant.$$

By noting that $s(0) = 0$, we get the same equation as (54).

Similarly, for $n = 2$, we have

$$S(v_a) = \frac{erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)\big[-2\mu erf\big(\frac{v_i-\mu}{\sigma\sqrt{2}}\big) + 2\sqrt{\frac{2}{\pi}}\sigma e^{\frac{-(v_i-\mu)^2}{2\sigma^2}}\big]}{\big[erf\big(\frac{b-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)\big]^2}$$

$$+\frac{erf\big(\frac{v_i-\mu}{\sigma\sqrt{2}}\big)\big[\mu erf\big(\frac{v_i-\mu}{\sigma\sqrt{2}}\big) - 2\sqrt{\frac{2}{\pi}}\sigma e^{\frac{-(v_i-\mu)^2}{2\sigma^2}}\big]}{\big[erf\big(\frac{b-\mu}{\sigma\sqrt{2}}\big) - erf\big(\frac{a-\mu}{\sigma\sqrt{2}}\big)\big]^2}$$

$$+\frac{\mu erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)^2+\frac{2\sigma erf\left(\frac{v_i-\mu}{\sigma}\right)}{\sqrt{\pi}}}{\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right)-erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]^2}+constant.$$

Since

$$\int\left[\frac{erf\left(\frac{v_i-\mu}{\sigma\sqrt{2}}\right)-erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)}{erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right)-erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)}\right]^2 dx =$$

$$\frac{erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\left[-2(v_i-\mu)erf\left(\frac{v_i-\mu}{\sigma\sqrt{2}}\right)-2\sqrt{\frac{2}{\pi}}\sigma e^{\frac{-(v_i-\mu)^2}{2\sigma^2}}\right]}{\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right)-erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]^2}$$

$$+\frac{erf\left(\frac{v_i-\mu}{\sigma\sqrt{2}}\right)\left[(v_i-\mu)erf\left(\frac{v_i-\mu}{\sigma\sqrt{2}}\right)+2\sqrt{\frac{2}{\pi}}\sigma e^{\frac{-(v_i-\mu)^2}{2\sigma^2}}\right]}{\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right)-erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]^2}$$

$$+\frac{(v_i-\mu)erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)^2-\frac{2\sigma erf\left(\frac{v_i-\mu}{\sigma}\right)}{\sqrt{\pi}}}{\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right)-erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]^2}+constant.$$

The value of the constant can be calculated by noting $s(0)=0$. Thus we have

$$constant=\frac{erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\left[-2\mu erf\left(\frac{\mu}{\sigma\sqrt{2}}\right)-2\sqrt{\frac{2}{\pi}}\sigma e^{\frac{-\mu^2}{2\sigma^2}}\right]}{\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right)-erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]^2}$$

$$-\frac{erf\left(\frac{\mu}{\sigma\sqrt{2}}\right)\left[\mu erf\left(\frac{\mu}{\sigma\sqrt{2}}\right)-2\sqrt{\frac{2}{\pi}}\sigma e^{\frac{-\mu^2}{2\sigma^2}}\right]}{\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right)-erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]^2}$$

$$-\frac{\mu erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)^2-\frac{2\sigma erf\left(\frac{\mu}{\sigma}\right)}{\sqrt{\pi}}}{\left[erf\left(\frac{b-\mu}{\sigma\sqrt{2}}\right)-erf\left(\frac{a-\mu}{\sigma\sqrt{2}}\right)\right]^2}.$$