Passivity Framework for Modeling, Composing and Mitigating Cyber Attacks

Phillip Lee

A dissertation submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington

2016

Reading Committee:

Radha Poovendran, Chair

Linda Bushnell, Chair

Baosen Zhang

James Ritcey

Program Authorized to Offer Degree:
Electrical Engineering

University of Washington

Abstract

Passivity Framework for Modeling, Composing and Mitigating Cyber Attacks

Phillip Lee

Co-Chairs of the Supervisory Committee:
Radha Poovendran
Electrical Engineering

Linda Bushnell
Electrical Engineering

Cyber systems form the backbone of our society, serving infrastructures for health, energy, transportation, and finance to name a few. As the reliance on cyber systems grows, the impact of cyber attacks also increases. Recent cyber incidents demonstrate that cyber attacks result in not only financial cost, but also compromise the safety of critical infrastructures.

Emerging cyber threats including advanced persistent threats (APT) show growing sophistication of attackers. Attackers exploit large number of entry points with different vulnerabilities and adaptively change attack strategies based on observed information of the targeted system. These features are captured by existing adversary models. To defend against such emerging threats, a new approach is needed for modeling and mitigating cyber attacks.

The goal of this thesis is providing fundamental approaches toward addressing these challenges. In this thesis, we study control and game theoretic approaches, both of which are developed under the passivity framework. Using dynamical systems theory, we model adaptive and time-varying dynamics of cyber attacks. We develop passivity-based composition rules that characterizes the impact of multiple simultaneous attacks, and design mitigation strategies against adversary models using passive structures. We have developed this ap-

proach for attacks including wormhole, jamming and malware propagation. Patrolling and resource takeover games are also studied under passivity framework.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGMENTS

First, I would like to thank my advisors, Professor Radha Poovendran and Professor Linda Bushnell. Professor Radha Poovendran has taught me not only how to conduct research but also how to overcome personal hardships since my undergraduate years at the University of Washington. This thesis would not have been possible without their mentoring and support. I would also like to thank my PhD supervisory committee, Jim Ritcey, Baosen Zhang and Arvind Krishnamurthy for helpful discussions, time and service.

I thank current and former members of the Network Security Lab (NSL). I thank Andrew Clark for all the intellectually stimulating discussions in front of the whiteboard and all the good times outside the lab. I extend my thanks to Basel Alomair, Kalikinkar Mandal, Sidharth Nabar, Xuhang (Shaun) Ying, Elisabeth Senmarti Robla, Zhipeng (Leo) Liu, Hossein Hosseini, and Laila Abudahi for their friendship.

I would like to thank my parents for always supporting me and believing in me throughout my life. I thank my wife for all her support and love. Anything I have achieved in my life, I owe it to my family.

DEDICATION

To my parents.

Chapter 1

INTRODUCTION

Networked systems are becoming prevalent in every aspects of individuals' lives including health, energy, finance, and transportation. Networked systems are characterized by complex interconnection of heterogeneous components with varying capabilities ranging from web servers and personal computers to wearable devices. An emerging class of networked systems is Cyber-Physical Systems (CPS) where physical infrastructures including power grid, transportation, and manufacturing infrastructure are tightly coupled with cyber systems, enabling real-time monitoring and control of physical components. This tight coupling, however, introduces multiple entry points for adversaries via cyber components, which could result in severe degradation of safety, performance and availability of physical components.

Recent cyber attack incidents on networked systems including Stuxnet and Duqu [26, 20] indicate growing capabilities and sophistication of attackers. Postmortem analysis reveal that attackers exploit multiple vulnerabilities, including zero-day exploits, and adaptively change the attack strategies based on observed system information to avoid detection, allowing these attackers to operate inside system for an extended period of time. Traces of log data also revealed that due to a large number of heterogeneous components, a single networked system may be targeted by multiple attackers with differing goals and capabilities exploiting different vulnerabilities [28], competing or colluding to compromise system resources.

The first step toward designing defense strategies against these emerging threats is developing adversary models that characterize the set of potential attacks and the resulting impact on the system. The existing adversary models, however, consider static capability of attackers (Byzantine [44]), assume cryptographic secrets cannot be compromised (Dolev-Yao [23]), or rely on the assumption that cryptographic primitives are secure (Random Oracle

[10]), leaving them inadequate to describe one or more adversaries that adaptively change the attack strategy, using zero-day exploits. Currently, the pure digital modeling of attacks in existing adversary models prevent the description of the impact of cyber attacks on the physical components in CPS due to the hybrid digital (cyber)-continuous (physical) nature of CPS. Both government agencies [1, 2] and research community [67] have identified a need for a *science of security* to overcome these challenges. The goal of science of security is to develop a body of laws from first principles that are invariant to specific attacks and vulnerabilities, enabling the defender to predict even unforeseen attacks and the resulting impact on the targeted system.

A new framework toward a science of security should incorporate the following characteristics of emerging threats. First, it should describe the *adaptive and time-varying nature* of advanced attackers. Second, the framework should provide *composition rules* for multiple attacks in order to guide the design of efficient mitigation strategies. Third, the *impact of cyber attacks on CPS* should be characterized. Fourth, the framework should predict unforeseen attacks by *identifying new attack primitives*.

The goal of this dissertation is to provide initial approaches toward addressing these challenges. The overview of my approach is illustrated in Figure 1.1. The approach consists of control and game-theoretic approaches, both of which are developed under a *passivity framework*. Passivity is an energy dissipation property of dynamical systems that provides basic rules for composition and analysis of interconnected systems. Dynamical system provides a promising step in describing temporal dynamics of adversarial actions by modeling time-varying nature of intelligent attacks. The composition rules provided by passivity framework will enable composition of multiple adversary models targeting different system components. The passivity framework will enable seamless integration into the existing models of CPS. The decomposition techniques for the identification of new attack primitives is an open research question that we will investigate.

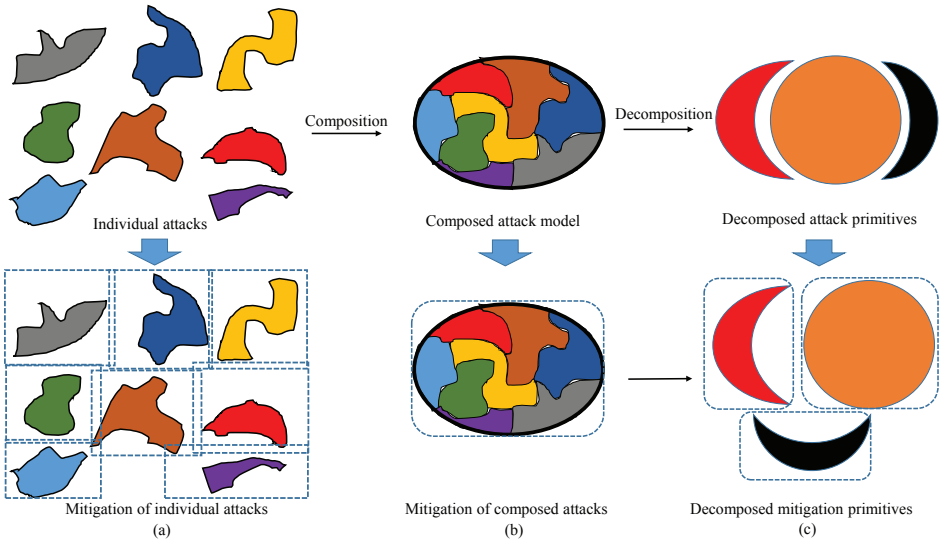


Figure 1.1: Overview of the proposed framework for modeling, composing and mitigating cyber attacks. a) Individual attacks with distinct mitigation mechanisms. (b) Composed adversary model enables compact representation of the attack and resource-efficient mitigation. (c) Decomposition of composed adversary model to identify of new attack primitives and their mitigation strategies. Part (c) is an open research question left for future work.

1.1 Contributions of this Thesis

Two themes of this thesis are (a) Control-Theoretic Approach for Composing and Mitigating Attacks and (b) Game-Theoretic Approach for Modeling Strategic Adversarial Interaction. The problems studied under each theme are illustrated in Figure 1.2 and discussed in more detail as follows.

1.1.1 Passivity Framework for Composing and Mitigating Wormhole Attacks

In wormhole attack, attackers create artificial links (wormholes) between distant regions to attract traffic. Wormhole links can be created either via a high-directional antenna (out-of-band) or misinforming the network of one-hop link between malicious compromised nodes (in-band).

Detection strategies have been developed against both types of wormholes from the secu-

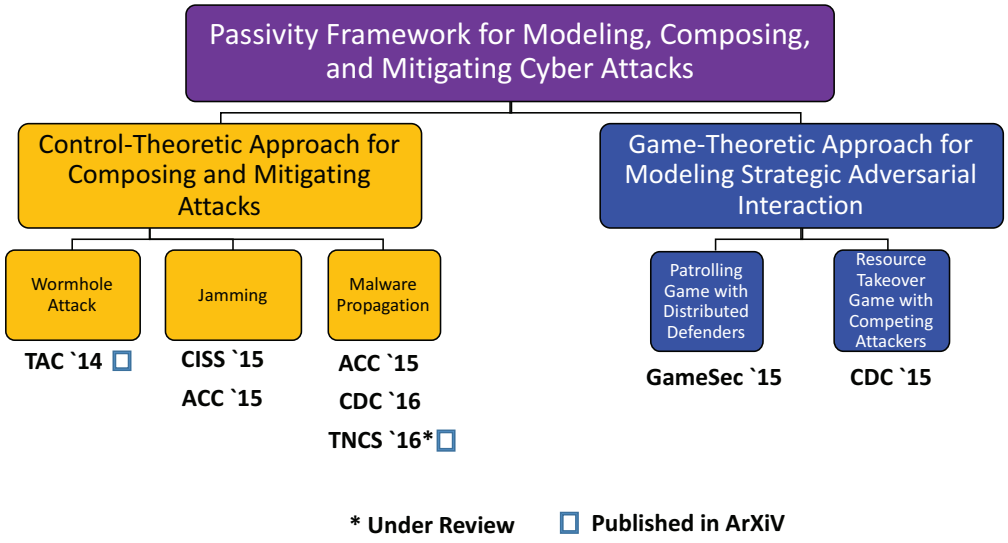


Figure 1.2: Organization of this thesis.

rity community. However, existing literatures studied different types of wormholes separately. In addition, the impact on the network delay and throughput in the presence of multiple different types of wormholes has not been studied.

In this thesis, we propose a passivity framework for modeling and composing wormholes in wireless networks. The main insight is we can view the flow allocation, delays induced through wormholes, and delays induced by mitigation mechanisms as coupled dynamical passive systems. Through passivity, we are able to *compose* different types of wormholes in different locations of the network and derive sufficient conditions that guarantee the flow allocation to reach a stable equilibrium. In addition, we can characterize the delay and throughput experienced by network at the steady state in the presence of wormholes and mitigation strategies.

We numerically study the impact of wormholes on networked control systems (NCS). Numerical results show that wormholes, left unmitigated, can induce large disturbances on the physical plant. We numerically demonstrate that by implementing properly tuned

mitigation strategies, the stability of the NCS can be guaranteed.

1.1.2 Passivity-Based modeling of Routing Attacks

Congestion control algorithms dynamically adjusts the flow rate at each path based on the observed end-to-end delay due to congestion. Such protocols allow sources to avoid creating bottleneck links while satisfying fairness conditions.

An intelligent attacker, however, can exploit these network protocols by jamming a set of links to reallocate traffic to colluding malicious nodes. Such attacks will result in a large fraction of packets flowing through malicious nodes, which increases the risk of being subjected to higher level attacks including man-in-the-middle.

In this thesis, we model the flow redirecting attack via jamming using a passivity-based analysis. The passivity framework allows us to model the flow allocation, delay due to congestion, and delay due to jamming as coupled dynamical systems, and derive resource efficient jamming strategy to allocate a desired amount of packets to malicious nodes. We formulate convex optimization problem to identify the optimal jamming strategy and prove that passivity-based jamming strategy achieves the optimal jamming power efficiency given the fraction of packets allocated to malicious nodes.

1.1.3 Passivity Framework for Composing and Mitigating Malware Propagation

Advanced malwares, which propagate through the network by exploiting software vulnerabilities, are a major threat to cyber infrastructures where malwares. As the number of malwares increase, different types of interaction between malwares, including competing and coexisitng, interactions have been observed.

In this thesis, we develop analytical models for malware propagation, where multiple malwares may be competing or coexisting with each other. We show that the proposed propagation dynamics are output feedback passive (OFP) dynamical systems, and the propagation rates can be characterized by passivity index of OFP systems. Using passivity

framework, we design patching-based mitigation strategies to remove all malwares at a *desired rate* when the propagation rates are known to the defender. When propagation rates are unknown to the defender, we develop adaptive patching and filtering defense strategies that dynamically update the defense parameters based on observed infections. We show that the proposed adaptive defense strategies remove all malwares at the cost of potentially high patching effort at the equilibrium or achieve non-zero, but arbitrarily small probability of infection at a relatively low patching effort.

1.1.4 Passivity-Based Distributed Strategies for Patrolling Games

Intelligent and persistent adversaries typically observe a targeted system and its security policies over a period of time, and then mount efficient attacks tailored to the weaknesses of the observed policies. These attacks have been analyzed within the framework of Stackelberg Security Games (SSG), where the defender (leader) selects a policy in order to maximize its utility under the best response strategy of the adversary (follower).

A *Patrolling game* is a type of SSG where defenders patrol through a large area to block the attacker from infiltrating one or more targets. The patrolling game has been used in design of patrol policies in large critical infrastructures including airport and coast area.

In this thesis, we develop a distributed patrol strategies among set of defenders who are limited by communication and mobility constraints. We derive a set of conditions that guarantee the proposed patrol policy to achieve the desired Stackelberg equilibrium (SE) and prove that the derived conditions can be mapped to convex constraints that can be used to formulate optimization problems. In particular, we study the tradeoff between the convergence rate to SE and the cost of mobility, and characterize the optimal tradeoff by solving convex optimization problems.

1.1.5 Resource Takeover Game Model for Advanced Persistent Threats

Recent cyber-attack incidents including Stuxnet and Duqu indicate growing capabilities and sophistication of attackers. Postmortem analyses have revealed that attackers exploit multi-

ple vulnerabilities, including zero-day exploits, and adaptively change the attack strategies based on observed system information to avoid detection, allowing these attackers to operate inside system for an extended period of time. Traces of log data also revealed that due to a large number of heterogeneous components, a system may be targeted by multiple attackers with differing goals and capabilities exploiting different vulnerabilities, competing or colluding to compromise system resources. The persistent and adaptive nature of malware creates a continuous, strategic interaction between the system owner and multiple competing malwares, which must be modeled and understood in order to develop effective mitigation strategies.

Recently, the FlipIt game [74] was proposed in the security community to model defense against such advanced persistent threats. In FlipIt, two players (attacker and defender) continuously compete for control of a host. The fraction of the time that each player controls the device, together with the resources expended to take over the device at different time instances, quantify the effectiveness of the defense strategy. While the FlipIt game provides the first step in modeling the impact of advanced persistent threats, it only considers scenarios when two-person Nash equilibrium exist, but does not describe the transient behaviors of advanced malwares until it reaches the equilibrium. Also, modeling behaviors of intelligent malwares which first observe the system defense to adjust its attack strategy as well as modeling competing multiple malwares are open research areas.

In this thesis, we propose a passivity framework for modeling and mitigating multiple competing malwares that describe the continuous strategic interaction between the system and malwares. We extend the FlipIt game by modeling the intelligent attackers who first observe the system defense under the Stackelberg game framework. Using passivity-based analysis, the time-varying behaviors of advanced malwares are modeled as passive dynamics systems. We show that greedy dynamics, where each malware continuously updates its attack strategy to maximize its utility guarantee convergence to Stackelberg-Nash equilibrium, and formulated optimal defense strategy to maximize the systems utility at the equilibrium.

1.2 Related Work

Control theoretic tools have been used to analyze the impact of cyber attacks on networked systems. Existing literatures mainly focus on the stability of physical plant of a cyber-physical system when subjected to a class of attacks including denial-of-service attack on control packets [17, 54], and false data injection attacks in which the attacker injects false information in one or more observation and control channels [50]. Existing literatures assume static capabilities of attackers assuming that either a fixed number of packets can be lost in the network due to attacks or only a subset fixed channels can be compromised for the false data injection attack [54]. For the ease of analysis, the physical plant models are assumed to be linearized, which lead to defense strategies relying on linear system control literatures including Kalman filters with intermittent observations [69] and robust control techniques for the uncertainty induced by false data injection attacks [16]. Modeling the adaptive and time-varying nature of intelligent attacks that dynamically change its attack strategy based on system information is in its early research stage.

Game theory has emerged as an important methodology for modeling the interaction between intelligent cyber attackers and defenders, and developing efficient mitigation strategies [4, 52]. Game theory is used in the applications including the defense of critical infrastructure in the context of Stackelberg security games [60, 68] as well as firewall placement and malware filtering [4]. Notions of deception and proactive defense such as moving target defense have recently been incorporated in game theory [22, 21]. Game theoretic models of emerging advanced persistent threats (APTs) is still in its nascent stage. An abstracted model of APT was introduced in [74], where attacker and a defender are competing over the same shared resource over an infinite horizon of time. This model captures the persistent nature of APT as an average utility of the long-term reward. However, incorporating the multi-stage nature of APTs is an open research area.

Summaries of related work for each of the sections in this thesis are given as the following.

1.2.1 Wormhole attack in wireless networks

The wormhole attack was originally identified as a form of routing misbehavior in ad hoc and sensor networks [37]. In [33], the packet leash defense was proposed, in which each packet is given a fixed expiration time and any packet received after its expiration time is discarded. Valid packets may also be discarded, however, due to propagation delays or clock skews between nodes, leading to a trade-off between detection effectiveness and network performance. Local broadcast keys, which are cryptographic keys that are distributed using specialized guard nodes and known only to nodes within a local neighborhood, were introduced in [63]. Anomalies in link delays, caused by propagation through the wormhole tunnel, are analyzed in [70], in which an FFT-based approach to identifying likely wormholes was presented. While these methods can be used to mitigate the impact of the wormhole attack, an analytical approach to dynamically tune each method in response to changes in the network state and adversary behavior, as well as estimate the stable operating point of the system, is currently lacking.

The in-band wormhole, in which the adversary creates the appearance of a link between two colluding nodes by tunneling packets through valid nodes, was identified as a security threat in [43]. The authors observed that the wormhole tunnel itself could contain routing loops, diminishing its effectiveness, a phenomenon they denoted as wormhole collapse. Necessary and sufficient conditions for the adversary to avoid wormhole collapse are derived in [51]. A statistical approach to detecting in-band wormholes, based on identifying increased delays or packet drops through wormhole links using sequential probability ratio testing, was studied in [8]. Our framework incorporates the probability of wormhole collapse, as well as the statistical detection algorithms, when modeling the temporal dynamics of the flow rates and resulting delays.

Passivity-based techniques have been used to model network flow control and derive novel flow allocation algorithms in [82]. The work of [82] fits within the broader context of dual decomposition-based methods for designing network protocols as distributed algorithms for

solving network optimization problems [19]. Passivity of networked control systems with packet drops was studied in [79], [79], where the authors studied the passivity of networked control systems where the plant dynamics switches between open and closed loop due to control packet drops. Currently, however, such models do not incorporate security threats or network defenses. In this thesis, by modeling the wormhole attacks as passive dynamical systems, we describe the dynamics of networked systems and impact of wormhole attacks in unifying control-theoretic language. This approach enables seamless integration of adversary models into existing models of networked control systems.

1.2.2 Jamming attack on secure routing

In existing works, the goal of a jamming attack is to minimize the network throughput subject to power constraints, and efficient jamming mechanisms have been studied in the optimization framework in [73]. The feasibility of a jamming attack to redirect the network flow into adversarial region, thus exposing the redirected traffic to higher-layer attacks, have been introduced in [48, 9, 37]. Currently, however, there exists no analytical framework to study the feasibility and efficient jamming strategies for the flow redirection attacks.

Control and game theory have been used to study the impact of jamming on cyber-physical systems in [11, 59, 45] where the impact of jamming is modeled as unavailability of sensor measurements or control packets.

Passivity-based approaches for rate allocation [82] and control of networked CPS [72] have been proposed in the absence of security threats. In [49], a passivity framework was used to study the impact of wormhole attacks on network flows. The impact of jamming, however, was not considered.

1.2.3 Modeling and mitigating malware propagation

Standard approaches for modeling propagation of a single malware are based on ordinary differential equation models from epidemiology, such as the Kermack-McKendrick model [39].

These models have been extensively analyzed theoretically and empirically, including applications to specific outbreaks such as the Code Red and Slammer worms [90]. Eigenvalue bounds on the rate of malware propagation, as well as the threshold rate for patching infected nodes in order to eliminate viruses, were presented in [78]. Multi-virus propagation has also received recent study [83, 80]. Propagation models have been developed to capture features of specific application domains, including mobile phones [88] and social networks [86]. Control-theoretic techniques for designing optimal malware propagation and attack strategies were presented in [29].

Dynamical models of virus propagation provide an analytical framework for designing mitigation strategies. An optimal control approach to mitigating a single virus is given in [13]. Geometric programming techniques for selecting the least-costly patching and vaccination rates were developed in [64]. Defenses against malware propagation in time-varying networks were considered in [56]. Recently, an optimization approach to defense against epidemics with uncertain propagation parameters was proposed [31]. Under this approach, fixed mitigation parameters were selected to ensure robustness to propagation parameters within an *a priori* known range. Our approach, on the other hand, adaptively increases the level of filtering in the network and makes no assumptions regarding the propagation parameters. An adaptive approach for virus mitigation under budget constraints was presented in [24].

1.2.4 Stackelberg Patrolling Game

Stackelberg Security Games (SSGs) have been prevalent in applications including the defense of critical infrastructures such as airports [60, 15], or large interconnected computer networks [18, 89]. In particular, stochastic Stackelberg games have been used to design randomized security policies instead of deterministic policies that can be learned by the attacker with certainty.

Computing the Stackelberg equilibria has been studied in the existing literatures [87, 42]. Computation of mixed-strategy Stackelberg equilibria against a worst-case (minimax or zero-sum) attacker was considered in [15]. Randomized security policies against bounded

rational adversaries were proposed in [87]. When the defender has partial or uncertain information on the adversary's goals and capabilities, a repeated Stackelberg framework was proposed to model the learning and adaptation of the defender strategy over time [42]. In [53], a human adversary with bounded rationality was modeled as the quantal response (QR) in which the rationality of the adversary is characterized by a positive parameter λ, with perfect rationality and worst-case (minimax) behavior as the two extremes. Games when the defender is uncertain about the behavioral models of the attacker has been studied. In [35], a monotonic maximin solution was proposed that guarantees utility bound for the defender against a class of QR adversaries. These existing works focus on computing the Stackelberg equilibria, where optimization framework including mixed-integer programming has been used for the computation.

Centralized algorithms for choosing which targets to defend over time to achieve a Stackelberg equilibrium have been studied in [3, 77], leading to deployment in harbor patrols [68] and mass transit security [60, 76]. In [3], randomized patrolling of a one-dimensional perimeter by multiple robots was considered, where all robots are governed by a parameter p determining to move forward or back. In [77], a game when the attacker not only has the knowledge of the randomized policy but also the current location of the defender was analyzed, leading to attacker's strategy being function of the defense policy and the previous moves of the defender. In these works, mixed integer linear programming techniques were proposed to compute the defender strategy, which provide guaranteed optimality but require a centralized entity with worst-case exponential complexity in the number of defenders, time steps, and targets.

1.2.5 Modeling and Mitigating Advanced Persistent Threats

Modeling and mitigating malwares have been significant areas of research in both control and security research communities [12, 28]. The existing literatures have focused on modeling the self-propagating aspect of a malware on a network. In these works, variations of epidemic dynamics were adapted to model the propagation of a single malware, and efficient mitigation

strategies were derived from control theoretic approaches [12, 29].

The competing nature of advanced malwares has been observed in the security community as in the cases of SpamThru and Tigger [28]. Analytically modeling the interaction between different malwares has only been investigated recently. In [83], malware interactions including coexisting and competing cases were modeled as continuous time Markov chains. This model, however, assumes that the compromise rates of malware are static, and hence does not incorporate the adaptive nature of malwares.

Game theory has emerged as an important methodology for modeling the interaction between intelligent cyber attackers and defenders, and developing efficient mitigation strategies [4, 52]. Recently, the FlipIt game was proposed to model persistent resource takeover of a single attacker and defender [74]. FlipIt was generalized to competition between two players over multiple resources in [47]. Empirical analysis of takeover strategies in FlipIt was performed in [65].

1.3 Organization of this Thesis

This thesis is organized as follows. Chapter 3 presents our passivity framework for modeling, composing and mitigating wormhole attacks. Chapter 4 presents the flow redirecting attack via jamming. The optimal strategy of such coordinated jammers is characterized via a passivity approach. In Chapter 5, we study the problem of modeling and mitigating multi-virus propagation. Mitigation strategies are derived by decomposing the propagation and the mitigation as coupled dynamical systems. Chapter 6 proposes a distributed patrol strategy. The proposed patrol strategy is derived through passivity-based analysis and the convergence rate to the desired operating point is characterized. Chapter 7 presents passivity framework for modeling advanced persistent threats.

Chapter 2

BACKGROUND ON PASSIVITY

2.1 Background on Passivity

In this section, we define basic notions of passivity, as well as a sufficient condition for exponential stability. All definitions and theorems can be found in [41].

Definition 2.1. *A system is defined to be output feedback passive (OFP) if there exists a positive semidefinite function V such that*

$$\dot{V}(t) \leq \rho y(t)^T y(t) + u(t)^T y(t) \tag{2.1}$$

for all input u and output y for all time t. If $\rho = 0$, then the system is called passive. The parameter ρ is defined as the output feedback passivity index of the system. If there exists a symmetric matrix Q such that

$$\dot{V}(t) \leq y(t)^T Q y(t) + u(t)^T y(t) \tag{2.2}$$

then the output feedback passivity index ρ is given by $\rho = \lambda_{\max}(Q)$, where $\lambda_{\max}$ is the largest eigenvalue.

Lemma 2.1. *Suppose that the system (Σ) is passive with $u(t) \in \mathbb{R}^m$ and $y(t) \in \mathbb{R}^n$. Then for any $m \times n$ matrix A, the system Σ', defined by*

$$(\Sigma') \begin{cases} \dot{x}(t) &= f(x(t), A^T u'(t)) \\ y'(t) &= Ag(x(t), A^T u'(t)) \end{cases}$$

is passive from input $u' \in \mathbb{R}^n$ to output $y' \in \mathbb{R}^m$.

Lemma 2.2. *A parallel interconnection between two passive systems is also passive.*

Definition 2.2. *Given a dynamical system* $\dot{\mathbf{x}} = f(\mathbf{x}), \mathbf{x}(0) = \mathbf{x}_0$*, an equilibrium point* $\overline{\mathbf{x}}$ *is exponentially stable if there exist positive constants* c *and* α *such that*

$$||\mathbf{x}(t) - \overline{\mathbf{x}}|| \leq c \exp(-\alpha t)||\mathbf{x}_0|| \tag{2.3}$$

for all initial states $\mathbf{x}_0$*.*

Theorem 2.1. *Let* $\dot{\mathbf{x}}(t) = f(\mathbf{x})$ *be a dynamical system with equilibrium point* $\overline{\mathbf{x}}$*. Suppose that there exists a positive semidefinite function* V *with* $V(\overline{\mathbf{x}}) = 0$ *and positive constants* c_1, c_2, c_3, p *such that*

$$c_1||\mathbf{x} - \overline{\mathbf{x}}||^p \leq V(\mathbf{x}) \leq c_2||\mathbf{x} - \overline{\mathbf{x}}||^p$$
$$\dot{V} \leq -c_3||\mathbf{x} - \overline{\mathbf{x}}||^p.$$

Then $\overline{\mathbf{x}}$ *is exponentially stable with rate of convergence given by*

$$||\mathbf{x}(t) - \overline{\mathbf{x}}|| \leq (\frac{c_2}{c_1})^{\frac{1}{p}} \exp(-\frac{c_3}{pc_1}t)||\mathbf{x}_0|| \tag{2.4}$$

The following two theorems provide sufficient conditions for asymptotic convergence.

Theorem 2.2. *[40] The negative feedback interconnection of two strictly passive systems* $\dot{W}_1 \leq u_1^T y_1$ *and* $\dot{W}_2 \leq u_2^T y_2$ *where* $u_2 = y_1$ *and* $u_1 = -y_2$ *is asymptotically stable.*

Theorem 2.3. *[40]* LaSalle's Invariance Principle*: Given a set* $\Omega \subset D$ *that is positively invariant with respect to dynamics* $\dot{\mathbf{x}} = f(\mathbf{x})$*, and* $W : D \to R$ *being a continuously differentiable function such that* $\dot{W}(\mathbf{x}) < 0$ *in* Ω*, every solution starting in* Ω *will converge to the largest invariant set* $M \subset \mathcal{I}$ *where* $\mathcal{I}$ *is the set of points in* Ω *such that* $\dot{W}(\mathbf{x}) = 0$*.*

Chapter 3

A PASSIVITY FRAMEWORK FOR COMPOSING AND MITIGATING WORMHOLE ATTACKS ON NETWORKED CONTROL SYSTEMS

3.1 Introduction

Cyber-physical systems that are deployed over a wide geographic area often consist of distributed embedded devices, such as sensors and actuators, that exchange sensed data and control signals via a wireless network [57], thus forming a networked control system. When deployed in critical applications such as the smart grid, the real-time control system may be targeted by adversaries attempting to drive it to an undesirable or unsafe operating point. By introducing and modifying delays in the communication network, the adversary can cause violations of the timing constraints that are critical in maintaining safe operation of real-time cyber-physical systems [34].

The wormhole attack, first introduced in the context of wireless routing [33], is one such attack that exploits the time delays and violates the timing constraints of the targeted system. In the wormhole attack, an adversary records messages observed in one region of the network and replays them in a different region [37]. By doing so, the adversary creates a communication link (a wormhole tunnel) between two end points in otherwise disjoint geographic areas. This can be accomplished by either compromised or colluding network nodes, known as the in-band wormhole [43] or via a side channel such as high-gain directional antennas, known as the out-of-band wormhole [33]. Unsuspecting network nodes will route network traffic through the wormhole. Once significant traffic starts flowing through the wormhole, the adversary can selectively drop or delay time-critical packets in order to destabilize or degrade the system performance. As the attack replays or reroutes

valid messages, it does not require compromising any cryptographic keys, and hence cannot be detected using cryptographic verification mechanisms alone [63].

While the wormhole attack does not violate cryptographic mechanisms, it does violate the physical constraints imposed by propagation delay and relative position of nodes. Current approaches that detect these violations include include graph-based methods [63], statistical methods [43], and timing analysis [33]. The current security analysis of the mitigation strategies, however, do not incorporate the time-varying node behaviors or the adaptive strategy of the adversary. Hence, while the wormhole attack can significantly degrade the performance of cyber-physical systems, there is currently no analytical approach that represents the impact of wormholes and mitigation on the system dynamics. Furthermore, the composition of different types of wormhole attacks and the impact on system performance has not been studied.

In this chapter, we introduce one such control-theoretic framework for modeling and mitigating the wormhole attack on networked control systems. The proposed framework models the impact of wormholes, as well as the integration of existing mitigation strategies, on the allocation of network flows and resulting delays. Our approach models three interdependent components, namely, flow allocation by network nodes, delay characteristics introduced by wormholes, and mitigation algorithms employed by the network. We develop this framework for both out-of-band and in-band wormholes. In addition, using our framework, we are able to model, represent and mitigate complex wormhole attacks that simultaneously make use of both in- and out-of-band wormholes. For each case, we prove that the flow allocation, wormhole delay, and mitigation components can be modeled as a passive dynamical system which allows the characterization of flow allocation and delay at the steady state. Since our framework is in control-theoretic language, it enables ease of composition with control models of cyber-physical systems. We make the following specific contributions:

- We study the wormhole attack and mitigation by first identifying the network throughput and delay as time-varying system performance parameters that are impacted by

the attack. We formulate dynamical system representations of the network flow allocation, delays and packet drops at the wormhole link, and the mitigation strategies of the system, for out-of-band, in-band, and joint in- and out-of-band wormhole attacks. We show that the overall flow allocation and delay are characterized by the interconnection of these dynamical systems.

- For the out-of-band wormhole, we develop dynamical models for the flow allocation by network nodes, the delays introduced by wormholes, and network mitigation. For the flow allocation by network nodes, we introduce a distributed algorithm for each node to adaptively divide its flow among a set of paths based on their delays. We model the delay characteristics of out-of-band wormhole links based on the rate at which the adversary drops packets traversing the wormhole link. We map the packet dropping strategy of the adversary to the optimization problem of selecting the optimal dropping rate which balances the goals of increasing delay and attracting flows to the wormhole. We then develop a dynamical model that integrates timing-based mitigation mechanisms, such as the packet leash, into our framework.

- We prove the dynamical systems describing the flow allocation, delays introduced by wormhole, and the mitigation schemes are passive. We leverage the passivity property to prove that the interconnection of these models is globally asymptotically stable with respect to a unique equilibrium point.

- For the in-band wormhole, we derive the delays introduced by wormhole as a function of number of colluding nodes and the network topology. We represent statistics based mitigation method against in-band wormhole as a penalty added to suspected wormhole links during the flow allocation. We then prove that the flow allocation algorithm introduced earlier together with the delay and mitigation models in the in-band case, can be represented as an interconnection of passive systems, which converges to a stable equilibrium point.

- We use our framework to model more complex wormhole attacks, which consists of both in- and out-of-band wormholes. Our approach composes the models of individual wormhole links via parallel interconnections of passive systems.

- We illustrate our approach via a numerical study, in which we compare the flow allocation and delay resulting from both out-of-band and in-band wormhole attacks and the detection mechanisms, and evaluate the impact of the wormhole attack and mitigation on a cyber-physical system. In the out-of-band case, simulation results show that detection mechanisms reduces the flow traversing through the wormhole link at the cost of increased delay. For the in-band case, simulation results suggest that detection mechanisms enable the source rates to converge to the same equilibrium regardless of the presence of a wormhole. We find that an adversary who creates an out-of-band wormhole can cause large disturbances on the physical plant by selectively dropping packets that are allocated to the wormhole link. We empirically determine parameters of the mitigation strategy that reduces the flow allocated to the wormhole link, while satisfying the system's delay constraints.

Our proposed framework enables quantitative analysis of the impact of the wormhole attack on system performance and the effectiveness of different mitigation mechanisms, as well as modeling of any arbitrary composition of in-band and out-of-band wormholes. Hence, this approach is complementary to recent efforts towards a science of cyber-security [67], where the goal is a scientific approach to characterizing, composing, and mitigating security threats. Moreover, our proposed framework explicitly captures the temporal dynamics of the attack and mitigation, including the adaptation and co-evolution of the adversary and defender strategies.

3.2 Model and Preliminaries

In this section, we state our assumptions regarding the capabilities of the network and adversary. We then give background on the wormhole attack.

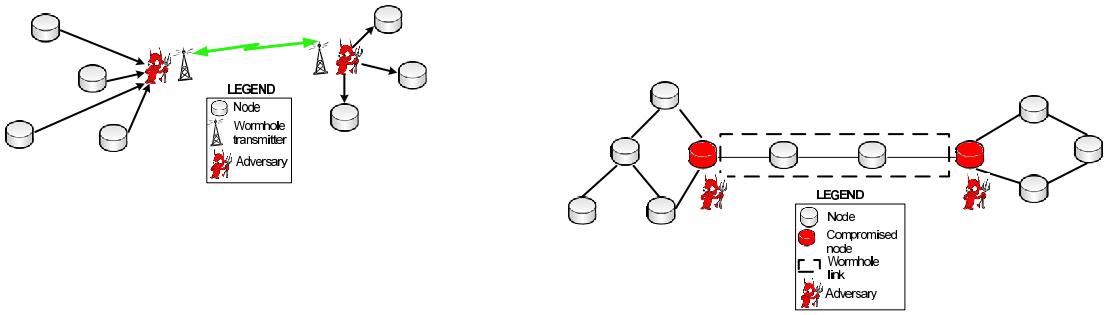
3.2.1 Network Model

We consider a wireless network of n nodes. We assume that two nodes can communicate directly if their positions are within the maximum node communication range. We denote the set of links by $\mathcal{L}$, with $|\mathcal{L}| = L$. In order to facilitate sensing and control of the system, network flows must be maintained between a set of source nodes $\mathcal{S}$ and destination nodes $\mathcal{D}$. The ordered pair (S_i, D_i) denotes the source and destination of flow i. We assume that source S_i maintains a constant rate r_i, and that flows are originating from the set of sources. External flows that do not originate from $\mathcal{S}$ are not considered in this chapter.

Any source and destination pair that is not in direct radio range relies on multi-hop communication. Since the topology changes due to node sleep/wake cycles and nodes joining and leaving the network, each source S_i uses a distributed routing protocol to identify a set of source-destination paths $\mathcal{P}_i = \{P_1, \ldots, P_{m_i}\}$, where m_i denotes the number of paths for source-destination pair (S_i, D_i).

3.2.2 Adversary Model

The network is deployed in a hostile environment where one or more mobile adversaries are present. We assume that each adversary is capable of eavesdropping as well as recording and replaying eavesdropped messages, including routing protocol messages. By eavesdropping on routing protocol messages, the adversary determines the network topology. The adversary is also capable of physically capturing the unattended nodes. Once the adversary has compromised a node, the adversary can extract its cryptographic secrets. This enables the adversary to replace the captured node with a malicious node assuming the identity of the captured node. Malicious nodes are under the control of the adversary and are capable of colluding with other malicious nodes. One such collusion attack is the wormhole, described as follows.

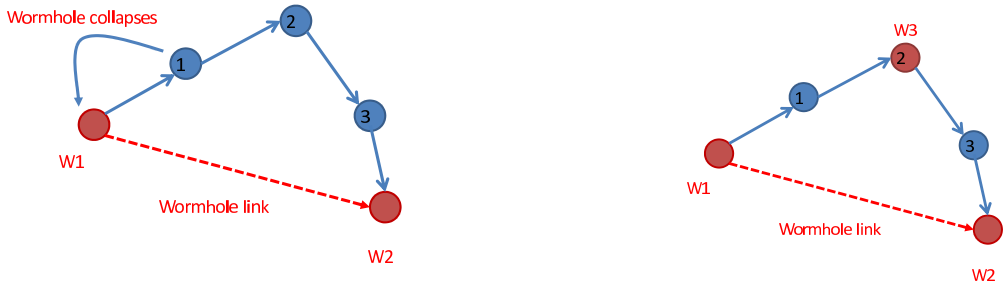


(a) (b)

Figure 3.1: Illustration of the two classes of wormhole. (a) In an out-of-band wormhole, the adversary creates a low-latency link between two network regions using a high-capacity channel, such as a directional antenna or wired link. (b) In an in-band wormhole, the adversary compromises network nodes in different regions and advertises a false one-hop link between two compromised nodes. The link actually consists of a path between unsuspecting valid nodes.

3.2.3 Wormhole Attack and Mitigation

In a wormhole attack, an adversary creates a covert path (referred to as *wormhole tunnel*) that connects two distant regions of the network. Since the wormhole creates the appearance of a short path between distant regions of the network, shortest-path routing protocols will route a large fraction of the network traffic through the wormhole tunnel. The adversary can then control this traffic and selectively drop packets, increase delays, or create routing instability. The wormhole link can also be used to record messages overheard in one network



(a) (b)

Figure 3.2: Illustration of the collapse of in-band wormholes. (a) When the colluding nodes W_1 and W_2 advertise a one-hop link between them, the intermediate nodes on the path between W_1 and W_2 will attempt to forward packets through the advertised (W_1, W_2) link, creating a routing loop that causes the wormhole to collapse. (b) By tunneling packets to an intermediate node W_3 satisfying the conditions of Lemma 3.1, which then forwards the packets to W_2, the adversary avoids wormhole collapse.

region, such as sensed data or control signals, and replay those messages in order to disrupt the performance of one or more system components. The wormhole can be further classified as out-of-band or in-band, depending on the nature of the wormhole tunnel.

Out-of-band wormhole formation

In the out-of-band wormhole, an adversary establishes a low-latency link (wormhole link) between two distant regions of the network (Figure 3.1(a)). This may be done through wired links that are not available to network nodes, or through high-gain directional wireless antennas. Once the adversary has gained control over a large amount of packets flowing through the wormhole link, the adversary can disrupt the system performance by dropping or delaying packets. In order to create an out-of-band wormhole, the adversary does not need to compromise any node or cryptographic secrets.

Out-of-band wormhole mitigation

The out-of-band wormhole is based on replaying messages that are intended for a local geographic area in a different geographic region. As a result of physical constraints on propagation through the medium, the time for a message to propagate to a node's immediate neighbors will be less than the time required for the message to propagate to the eavesdropper, traverse the wormhole tunnel, and then propagate to any nodes on the other side of the wormhole tunnel. This discrepancy is the basis for the packet leash defense [33], in which the sender of each packet attaches an expiration time to the packet, equal to $t_s + \frac{R}{c} + \Delta$, where t_s is the transmission time, $\frac{R}{c}$ is the propagation time, and Δ is an estimate of the clock skew between the sending and receiving nodes. All packets received after their expiration time are discarded. Packets are signed using message authentication codes to prevent the adversary from modifying the expiration time.

In-band wormhole formation

In the in-band wormhole attack, an adversary compromises two nodes in different regions of the network and falsely advertises a one-hop link between those nodes via the routing protocol. As in the out-of-band case, the appearance of this short path will result in a large traffic flow into the two compromised nodes. The adversary then chooses a path, consisting of

both valid and compromised nodes, between the two nodes comprising the wormhole tunnel. The in-band wormhole requires the adversary to compromise at least two nodes, but does not require any specialized hardware. The in-band wormhole is illustrated in Figure 3.1(b).

In-band wormhole collapse

In order to create an in-band wormhole, the adversary must avoid wormhole collapse, which occurs under the following conditions. The wormhole tunnel consists of a path between two colluding nodes, denoted W_1 and W_2. The intermediate nodes in the tunnel, however, will attempt to route packets from W_1 to W_2 using shortest-path routing. Since the wormhole tunnel is advertised as a one-hop link between W_1 and W_2, any packets sent from W_1 to W_2 are likely to be forwarded back to W_1, creating a routing loop (Figure 3.2(a)).

To avoid wormhole collapse, the adversary must capture a third node, denoted W_3. Instead of routing packets directly from W_1 to W_2 in the wormhole link, the adversary sends packets from W_1 to W_3, and then from W_3 to W_2, as shown in Figure 3.2(b). The conditions on W_3 to prevent wormhole collapse are given by the following lemma.

Lemma 3.1 ([51])**.** *Let $d(i, j)$ denote the length of the shortest path between nodes i and j. Then the wormhole tunnel formed by colluding nodes W_1, W_2, and W_3 does not collapse if*

$$d(W_1, W_3) < d(W_2, W_3) + 3.$$

In-band wormhole mitigation

Since the in-band wormhole is mounted using compromised nodes and their stored cryptographic keys, defenses against the out-of-band wormhole may be ineffective against in-bandwidth wormholes. The in-band wormhole, however, will incur longer delays than the out-of-band wormhole, since it relies on a multi-hop path of network nodes to forward packets. By performing statistical analysis, the network nodes can identify one-hop links with exceptionally long delays and/or packet-loss rates, which are then suspected of being wormhole links and ignored for routing purposes [43].

3.3 Proposed Passivity Framework for Out-of-Band Wormhole

In this section, we introduce our passivity-based framework for modeling and mitigating out-of-band wormholes in a networked control system. Our model considers the effect of the wormhole attack and mitigation on the delay and flow allocation of the network traffic. We first develop a dynamical model for the flow allocation by the network nodes. We then model the delays experienced due to the out-of-band wormhole, followed by the effect of mitigation mechanisms. Lastly, we consider the interconnection of these three dynamical models and characterize the flow allocation and delay at the unique equilibrium point via a passivity-based approach.

3.3.1 Dynamical Model of Network Flow Allocation

We assume that each source node S_i maintains a flow with total rate r_i to destination D_i. This flow is divided among the paths $\mathcal{P}_i$ used by source S_i in order to minimize the overall delay. Let $r_P(t)$ denote the flow allocated to path $P \in \mathcal{P}_i$ at time t, so that $\sum_{P\in\mathcal{P}_i} r_P = r_i$. The vector of flow rates is denoted $\mathbf{r}_i(t) \triangleq \{r_P(t) : P \in \mathcal{P}_i\}$. Furthermore, let $f_l(r_l)$ denote the delay experienced on link l when the rate of flow on link l is given by r_l. Let $q_P(r_P) \triangleq \sum_{l\in P} f_l(r_l)$ denote the total delay on path P, equal to the sum of the delays on each link comprising the path, where $\{l \in P\}$ denotes summing over the links l in path P. Finally, define the $L \times (\sum_{i=1}^{n} m_i)$ matrix A by

$$A_{lP} = \begin{cases} 1, & \text{link } l \text{ in path } P \\ 0, & \text{else} \end{cases}$$

so that $r_l = (A\mathbf{r})_l$.

Achieving the minimum possible delay is equivalent to finding $\{r_P : P \in \mathcal{P}_i\}$ satisfying

$$\min\left\{\sum_{P\in\mathcal{P}_i} r_P q_P(r_P) : \sum_{P\in\mathcal{P}_i} r_P = r_i\right\},$$

since $r_P q_P(r_P)$ is the total delay on path P, $\sum_{P\in\mathcal{P}_i} r_P$ is the overall delay experienced on all paths, and $\sum_{P\in\mathcal{P}_i} r_P = r_i$ is a constraint on the total throughput. Determining whether this

condition is satisfied requires the source S_i to determine the incremental change in delay from shifting flow from path P to path P' for all $P, P' \in \mathcal{P}_i$. The incremental change, however, depends on parameters that the source cannot observe, such as the rates of the other sources and the excess capacity of each link, and hence cannot be computed directly by the source. Instead, we assume that each source attempts to minimize the total delay based on the currently observed delay characteristics of each link. This condition is formalized by the concept of a *Wardrop equilibrium* [5], defined as follows.

Definition 3.1. *The flow allocation* $\{r_P : P \in \mathcal{P}_i\}$ *is a* Wardrop equilibrium *for source* S_i *if for any path* P, $r_P > 0$ *implies that* $q_P \leq q_{P'}$ *for all* $P' \in \mathcal{P}_i$.

Definition 3.1 implies that a positive flow rate is allocated to path $P \in \mathcal{P}_i$ if and only if there is no path P' currently experiencing lower delays than path P. We now introduce flow rate dynamics that, when used by each source S_i to choose $\mathbf{r}_i(t)$, cause the network to converge to a Wardrop equilibrium. We prove convergence to the Wardrop equilibrium by first proving that $\mathbf{r}_i$ is a steady state for the dynamics if and only if it is a Wardrop equilibrium, and that the Wardrop equilibrium is unique. We then use a passivity-based approach to prove the system converges to a unique steady state and hence converges to the Wardrop equilibrium.

Let $P_i^{min}(q)$ denote a time-varying index satisfying

$$P_i^{min}(q) \in \arg\min \{q_P : P \in \mathcal{P}_i\}.$$

We define the dynamics of the flow rate $r_P(t)$ allocated to path $P \in \mathcal{P}_i$ by

$$\dot{r}_P(t) = \begin{cases} -\{q_P(r_P(t)) - q_{P^{min}}(r_{P_i^{min}}(t))\}_+^{r_P}, & P \neq P_i^{min}(q) \\ -\sum_{P \neq P_i^{min}(q)} \dot{r}_P(t), & P = P_i^{min}(q) \end{cases} \tag{3.1}$$

where

$$\{x\}_+^{r_P} = \begin{cases} 0, & x > 0 \text{ and } r_P = 0 \\ x, & \text{else} \end{cases}$$

Equation (3.1) has the following interpretation. When the observed delay on path P is greater than the delay observed on path P^{min}, which has the minimum delay of any path in $\mathcal{P}_i$, the flow allocated to path P is reduced if it is positive. When the path P has the minimum delay of any path in $\mathcal{P}_i$ ($P = P_i^{min}(q)$), additional flow is allocated to path P (note that, since $\dot{r}_P(t) \leq 0$ if $P \neq P_i^{min}(q)$, $-\sum_{P \neq P_i^{min}(q)} \dot{r}_P(t) \geq 0$). Since the total flow from source S_i is constant, the dynamics are chosen such that $\sum_{P \in \mathcal{P}_i} \dot{r}_P(t) = 0$. The following proposition verifies that the dynamics (3.1) define a feasible flow allocation for all time t.

Proposition 3.1. *Suppose that $\sum_{P \in \mathcal{P}_i} r_P(0) = r_i$ and $r_P(0) \geq 0$ for all $P \in \mathcal{P}_i$. Then for all $t > 0$, $\sum_{P \in \mathcal{P}_i} r_P(t) = r_i$ and $r_P(t) \geq 0$ for all $P \in \mathcal{P}_i$.*

A proof is given in [49]. We next show that the equilibria of (3.1) are equivalent to the Wardrop equilibria of the system.

Proposition 3.2. *The dynamics (3.1) have an equilibrium at $\mathbf{r}_i^*$ if and only if $\mathbf{r}_i^*$ is a Wardrop equilibrium.*

Proof: First, suppose that $\dot{r}_P(t) = 0$ for all $P \in \mathcal{P}_i$, and assume that $\mathbf{r}_i(t)$ is not a Wardrop equilibrium. By Definition 3.1, there exists P such that $q_P(r_P) > q_{P_i^{min}(t)}(r_{P_i^{min}})$ and $r_P(t) > 0$. The condition $\dot{r}_P(t) = 0$ implies that

$$\{q_P(r_P) - q_{P_i^{min}}(r_P^*)\}_+^{r_P} = 0. \tag{3.2}$$

Since $q_P(r_P) > q_{P_i^{min}}(r_{P_i^{min}})$, condition (3.2) holds if and only if $r_P = 0$, contradicting the assumption that $r_P > 0$.

Now, suppose that $\mathbf{r}_i$ is a Wardrop equilibrium. The goal is to show that $\mathbf{r}_i$ is an equilibrium of (3.1). Consider $P \in \mathcal{P}_i$, and suppose that $P \neq P_i^{min}$. We show that $\dot{r}_P(t) = 0$ by separately considering the cases where $q_P(r_P) = q_{P_i^{min}}(r_{P_i^{min}})$ and $q_P(r_P) > q_{P_i^{min}}(r_{P_i^{min}})$ ($q_P(r_P) < q_{P_i^{min}}(r_{P_i^{min}})$ contradicts the definition of P_i^{min}).

If $q_P(r_P) = q_{P_i^{min}}(r_P^*)$, then $\dot{r}_P(t) = 0$. On the other hand, if $q_P(r_P) > q_{P_i^{min}}(r_{P_i^{min}})$, then the delay experienced on path P exceeds the minimum delay, and therefore $r_P(t) = 0$ by Definition 3.1. Hence $\dot{r}_P(t) = \{q_P(r_P) - q_{P_i^{min}}(r_{P_i^{min}})\}_+^{r_P} = 0$.

Finally, we have

$$\dot{r}_{P_i^{min}} = -\sum_{P \neq P_i^{min}} \dot{r}_P = 0,$$

which proves that $\mathbf{r}_i$ is an equilibrium point of (3.1). ■

Proposition 3.2 implies that the equilibria of (3.1) are equal to the Wardrop equilibria of the system. The following Lemma proves the equilibria of (3.1) are unique.

Lemma 3.2. *If the functions $f_l : \mathbb{R} \to \mathbb{R}$ are strictly increasing for all links l, then there exists a unique equilibrium for the dynamics (3.1).*

A proof of Lemma 3.2 is given in [49]. Finally, we show that the dynamics (3.1) converge to the unique Wardrop equilibrium. As a first step, we present an equivalent representation of (3.1). We define the system $\tilde{H}_1$, which takes input $u^1 \in \mathbb{R}^{m_i}$, by

$$(\tilde{H}_1) \begin{cases} \dot{\tilde{r}}_P(t) = -\{q_P^* - u_P - q^*_{P^{min}(q^*-u)} + u_{P^{min}(q^*-u)}\}_+^{r_P}, & P \neq P_i^{min}(q^*-u) \\ \dot{\tilde{r}}_P(t) = -\sum_{P \neq P^{min}(q^*-u)} \dot{\tilde{r}}_P(t), & P = P_i^{min}(q^*-u) \\ \tilde{y}_P(t) = \dot{\tilde{r}}_P(t), & \forall P \in \mathcal{P}_i \end{cases}$$

We define a system $(\tilde{H}_2)$, which takes input $u^{(2)}(t) \in \mathbb{R}^L$, as

$$(\tilde{H}_2) \begin{cases} \dot{z}_l(t) = u_l^{(2)}(t) \\ y_l(t) = f_l(z_l(t)) - f_l(z_l^*) \end{cases}$$

where z_l^* is the rate through link l in the unique equilibrium guaranteed by Lemma 3.2. We let $(\tilde{H})$ denote the system formed by a negative feedback interconnection between $(\tilde{H}_1)$ and $(\tilde{H}_2)$ (Figure 3.3). The following proposition establishes the equivalence between the state dynamics defined by (3.1) and system $(\tilde{H})$.

Proposition 3.3. *For all t, $\tilde{\mathbf{r}}(t) = \mathbf{r}(t)$.*

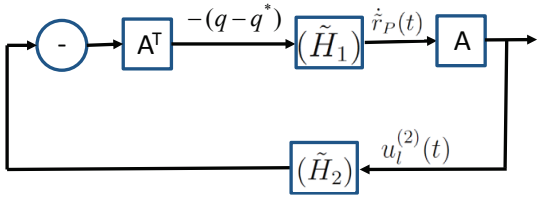


Figure 3.3: Illustration of the flow allocation and link delay dynamics $(\tilde{H}_1)$ and $(\tilde{H}_2)$. The passive system $(\tilde{H}_1)$ represents the flow allocation by each source based on the observed delays at each path. The passive system $(\tilde{H}_2)$ represents the delays experienced at each link as a function of the flows allocated to the link. Since $(\tilde{H}_1)$ is strictly passive and $(\tilde{H}_2)$ is passive, the overall system is asymptotically stable (Theorem 3.1).

The proof can be found in [49]. The following theorem establishes that the flow rate allocation converges to the unique Wardrop equilibrium.

Theorem 3.1. *Suppose that* $\sum_{P\in\mathcal{P}_i} r_P(0) = r_i$. *If the link delay* $f_l(r_l)$ *is strictly increasing as a function of* r_l *for all links* l, *then*

$$\lim_{t\to\infty} \mathbf{r}_i(t) = \mathbf{r}_i^*,$$

where $\mathbf{r}_i^*$ *is the unique Wardrop equilibrium.*

Proof: It suffices to show that the system $(\tilde{H}_1)$ is strictly passive from input $u_P^{(1)}(t)$ to output $\tilde{y}_P^{(1)}(t)$ and the system $(\tilde{H}_2)$ is passive from input $u_l^{(2)}(t)$ to output $\tilde{y}_l^{(2)}(t)$.

Define the function $V_1(\mathbf{r}) = q^{*T}(\mathbf{r} - \mathbf{r}^*)$, and let $q = q^* - u$. Then

$$\dot{V}_1(\mathbf{r}) = q^{*T}\dot{\mathbf{r}} = q^T\dot{\mathbf{r}} + \tilde{u}^{(1)}(t)^T\dot{\mathbf{r}}.$$

To prove strict passivity, it therefore suffices to show that $q^T\dot{\mathbf{r}} < 0$. Without loss of generality, suppose that $|\mathcal{P}_i| = m_i + 1$ and $P_i^{\min}(q^* - u) = P_i^{\min}(q) = m_i + 1$. Then

$$\begin{aligned} q^T\dot{\mathbf{r}} &= \sum_{j=1}^{m_i+1} q_j\dot{r}_j(t) = \sum_{j=1}^{m_i} q_j\dot{r}_j(t) - \sum_{j=1}^{m_i} q_{m_i+1}\dot{r}_j(t) \\ &= -\sum_{j=1}^{m_i} q_j(q_j - q_{m_i+1})_+^{r_j} + \sum_{j=1}^{m} q_{m_i+1}(q_j - q_{m_i+1})_+^{r_j}. \end{aligned}$$

By definition, $(q_j - q_{m_i+1})_+^{r_j} \geq 0$. Furthermore, $q_j \geq q_{m_i+1}$ for all j, and so

$$q^T \dot{\mathbf{r}} \leq -\sum_{j=1}^{m_i} q_{m_i+1}(q_j - q_{m_i+1})_+^{r_j} + \sum_{j=1}^{m_i} q_{m_i+1}(q_j - q_{m_i+1})_+^{r_j},$$

thus establishing the passivity of $(\tilde{H}_1)$. To prove passivity of $(\tilde{H}_2)$, define the storage function

$$V_2(z_l) = \int_0^{z_l - z_l^*} f_l(s + z_l^*) - f_l(z_l^*)\, ds.$$

We have $\dot{V}_2(z_l(t)) = (f_l(z_l(t) - f_l(z_l^*))\dot{z}_l(t) = u_l^{(2)}(t)\tilde{y}_l^{(2)}(t)$, implying passivity of $(\tilde{H}_2)$. ■

Theorem 3.1 implies that the flow allocation converges to a unique equilibrium when the delays experienced at each link is a strictly increasing function in flows allocated to each link. The next step in modeling the wormhole attack is to characterize the delays experienced by the wormhole links, which is the topic of the following section.

3.3.2 Delay Characteristics of the Out-of-Band Wormhole

For the out-of-band wormhole, we assume that the wormhole tunnel uses a high-throughput channel, so that the delay for packets traversing the wormhole tunnel l is equal to the propagation delay α_l. Let $\Phi_l(r_l)$ denote the fraction of packets dropped by the wormhole, which we assume to be increasing in r_l. The delay for packets traversing the wormhole tunnel, equal to the time per packet transmission multiplied by the average number of retransmissions, is therefore given by $p_l = \alpha_l/(1 - \Phi_l(r_l))$.

Since the packet-loss rate Φ_l is increasing in r_l, p_l is increasing as a function of r_l as well, thus preserving the passivity property required by the proof of Theorem 3.1. In what follows, we provide a method for modeling the packet-loss rate $\Phi_l(r_l)$ based on the goals of the adversary.

In mounting the wormhole attack, the goal of the adversary is to attract flow to the wormhole tunnel, in order to either selectively drop packets or mount secondary attacks. The rate at which packets are dropped by the adversary is equal to $\Phi_l(r_l)r_l$, while we model the utility of the adversary from mounting secondary attacks as $U_A(r_l)$. The adversary's overall

utility is therefore given by $\Phi_l(r_l)r_l + U_A(r_l)$. By decreasing Φ_l, the adversary increases r_l and hence $U_A(r_l)$, at the cost of dropping fewer packets.

The optimal dropping rate depends on the flow rate through the wormhole link in steady-state, which in turn depends on the delays experienced by the other links in the network, since higher delays at other links will increase the flow allocated to the wormhole link. Based on the network topology, the adversary estimates the delay between source S_i and destination D_i as $\zeta d(S_i, D_i)$, where $\zeta \geq 0$ is the per-hop delay and $d(\cdot, \cdot)$ is the length of the shortest path between two nodes. Similarly, the delay experienced by the wormhole path will be equal to $\zeta d(S_i, W_1) + \frac{\alpha_l}{1-\Phi_l(r_l)} + \zeta d(W_2, D_i)$, where W_1 and W_2 are the entrance and exit to the wormhole tunnel, respectively. Define $\Delta_{i,l}$ by

$$\Delta_{i,l} = \zeta(d(S_i, D_i) - (d(S_i, W_1) + d(W_2, D_i))).$$

By Proposition 3.2, the flow from source S_i to destination D_i will traverse the wormhole tunnel if and only if the delay experienced by the wormhole path is less than the delay experienced by the next-shortest path. Hence, the flow from source S_i to destination D_i that traverses the wormhole tunnel in steady-state will be equal to

$$r^*_{i,l} \triangleq \begin{cases} r_i, & p_l < \Delta_{i,l} \\ 0, & \text{else} \end{cases}$$

Without loss of generality, assume that the indices i are rank-ordered such that $\Delta_{1,l} > \Delta_{2,l} > \cdots > \Delta_{n,l}$, and define $i^* = \max\{i : p_l < \Delta_{i,l}\}$. The flow rate r^*_l traversing the wormhole in steady-state is equal to

$$r^*_l = \sum_{i=1}^{i^*} r_i. \tag{3.3}$$

The following proposition describes the set of possible optimal packet-dropping rates Φ^*_l at equilibrium.

Proposition 3.4. *The possible solutions* Φ_l^* *to the optimization problem*

$$\begin{aligned} &\textit{maximize} \quad r_l^*(\Phi_l)\Phi_l + U_A(r_l^*(\Phi_l)) \\ &\Phi_l \\ &\textit{s.t.} \qquad\qquad \Phi_l \in [0,1] \end{aligned} \tag{3.4}$$

are given by $\{\gamma_1, \ldots, \gamma_n\}$*, where*

$$\gamma_i = 1 - \frac{\alpha_l}{\Delta_{i,l}} - \epsilon$$

for some $\epsilon << 1$.

Proof: Suppose that the optimal solution Φ_l^* to (3.4) lies within the interval (γ_i, γ_{i+1}) for some i. Then by definition of γ_i, $p_l^* > \Delta_{l,i+1}$ and $p_l^* < \Delta_{l,i}$, so that $i^* = i$. Consider $\Phi_l^* + \delta$ for some $\delta > 0$ satisfying $\Phi_l^* + \delta < \gamma_{i+1}$. Then by (3.3),

$$r_l^*(\Phi_l^*) = \sum_{k=1}^{i} r_k = r_l^*(\Phi_l^* + \delta).$$

We therefore have that

$$\begin{aligned} r_l^*(\Phi_l^*)\Phi_l^* + U_A(r_l^*(\Phi_l^*)) &< r_l^*(\Phi_l^*)(\Phi_l^* + \delta) + U_A(r_l^*(\Phi_l^*)) \\ &= r_l^*(\Phi_l^* + \delta)(\Phi_l^* + \delta) \\ &\quad + U_A(r_l^*(\Phi_l^* + \delta)), \end{aligned}$$

contradicting the assumption that Φ_l^* is optimal. ■

The adversary can therefore determine the optimal packet-dropping rate at equilibrium, Φ_l^*, by evaluating $r_l^*\Phi_l^* + U_A(r_l^*)$ at the set of points $\Phi_l^* = \gamma_1, \ldots, \gamma_n$ and choosing Φ_l^* that gives the maximum value of $r_l^*(\Phi_l)\Phi_l + U_A(r_l^*(\Phi_l))$.

3.3.3 Model of Mitigation for Out-of-Band Wormhole

The mitigation model is as follows. Each packet is assigned a packet leash chosen by the source, so that the packet is valid for time $\frac{R}{c} + \Delta_{max}$, where R is the propagation distance, c is the speed of light, and Δ_{max} is the maximum permissible value of the clock skew. When

the packet traverses a wormhole, the packet violates the packet leash requirement and is dropped when

$$\frac{R_1}{c} + \frac{R_2}{c} + \alpha_l + \Delta > \frac{R}{c} + \Delta_{max},$$

where R_1 and R_2 are the distances of the sender and receiver from the wormhole start and end points, respectively, and α_l is the wormhole tunnel propagation time as in the previous section. The random variable Δ represents the clock skew between the nodes comprising the link. Hence the probability of a packet drop is equal to

$$P_d = \begin{cases} Pr\left(\Delta > \Delta_{max}\right), & l \text{ valid} \\ Pr\left(\Delta > \frac{1}{c}(R - R_1 - R_2) - \alpha_l + \Delta_{max}\right), & l \text{ wormhole} \end{cases} \tag{3.5}$$

We assume that the network maintains a lower threshold Δ_{max}, representing a more stringent mitigation strategy, when the rate of flow through a link increases. From (3.5), the packet drop rate is therefore an increasing function of Δ_{max}.

The effect of the packet leash can be modeled by the increase in delay for each packet due to retransmissions. This additive delay is equal to $\left(\frac{1}{1-P_d} - 1\right) f_l(r_l)$, which represents the additional delay due to packet leash. The dynamics of the additive delay introduced by the mitigation mechanism are given as

$$(H_3) \begin{cases} \dot{r}_l(t) = u_l^{(3)}(t) \\ y_l^{(3)}(t) = \left(\frac{1}{1-P_d} - 1\right)\left(f_l(r_l(t))\right) \end{cases}$$

3.3.4 Steady-state and Stability Analysis for the Out-of-Band Wormhole

In this section, we analyze the steady-state characteristics of the overall system. As a first step, we define the system $(\tilde{H}_3)$ as

$$(\tilde{H}_3) \begin{cases} \dot{r}_l(t) = u_l^{(3)}(t) \\ \tilde{y}_l^{(3)}(t) = \left(\frac{1}{1-P_d} - 1\right)\left(f_l(r_l(t))\right) \\ \qquad\quad - \left(\frac{1}{1-P_d^*} - 1\right) f_l(r_l^*) \end{cases}$$

where P_d^* is the probability of packet drops when the flow allocated to link l is r_l^*. The joint dynamics of the flow allocation, wormhole delay, delays on valid links, and delay introduced by mitigation mechanisms can be represented as a negative feedback interconnection between dynamical systems $(\tilde{H}_1)$, $(\tilde{H}_2)$, and $(\tilde{H}_3)$ (Figure 3.4). The following lemma guarantees global asymptotic stability of the overall system.

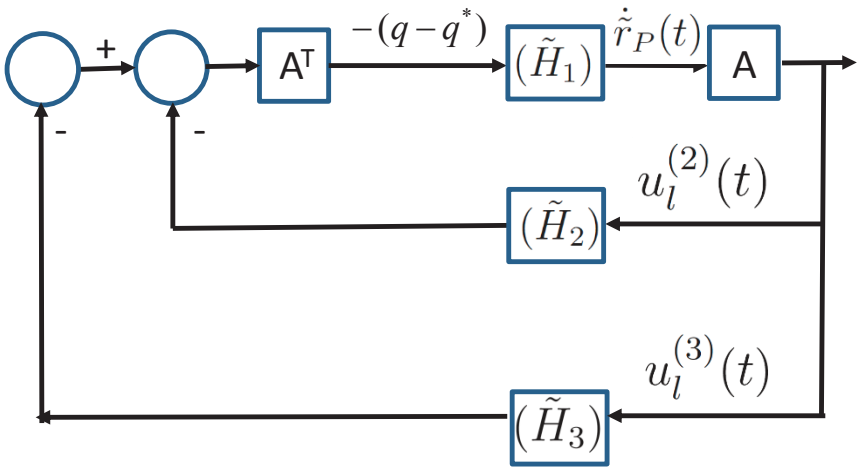


Figure 3.4: Block diagram illustrating the out-of-band wormhole link and mitigation. As in Figure 3.3, systems $(\tilde{H}_1)$ and $(\tilde{H}_2)$ are passive dynamical systems representing flow allocation and link delays respectively. Passive dynamical system $(\tilde{H}_3)$ represents the network mitigation mechanisms. By Corollary 3.1, the interconnection of these passive systems is asymptotically stable.

Lemma 3.3. *The system* $(\tilde{H}_3)$ *is passive from input* $u_l^{(3)}(t)$ *to output* $\tilde{y}_l^{(3)}(t)$.

Proof: Define

$$V_l(r_l) = \int_{r_l^*}^{r_l} \left(\left(\frac{1}{1 - P_d(s)} - 1 \right) f_l(s) - \left(\frac{1}{1 - P_d^*} - 1 \right) f_l(r_l^*) \right) ds.$$

Since $\left(\frac{1}{1-P_d(s)} - 1\right) f_l(s)$ is nondecreasing as a function of s, $V_l \geq 0$. Furthermore, $V_l(r_l^*) = 0$ and

$$\begin{aligned}\dot{V}_l(t) &= \left(\left(\frac{1}{1-P_d(r_l)} - 1\right) f_l(r_l) \right. \\ &\quad \left. - \left(\frac{1}{1-P_d^*} - 1\right) f_l(r_l^*)\right) \dot{r}_l \\ &= \dot{r}_l \tilde{y}_l^{(3)}(t),\end{aligned}$$

thus establishing passivity of $(\tilde{H}_3)$. ■

Corollary 3.1. *The system of Figure 3.4 is globally asymptotically stable.*

Proof: By Theorem 3.1, the blocks $(\tilde{H}_1)$ and $(\tilde{H}_2)$ in Figure 3.4 form a negative feedback interconnection of passive systems, and hence are passive. Since $(\tilde{H}_3)$ is passive by Lemma 3.3, the system consists of a negative feedback interconnection of passive systems, which is globally asymptotically stable. ■

Corollary 3.1 implies that the overall system consisting of the flow allocation, out-of-band wormhole, and mitigation converges to a unique stable equilibrium point. This enables the characterization of delay experienced by the networked control system in steady state.

Our passivity based approach for modeling and mitigating in-band wormhole attacks is described in the following section.

3.4 Proposed Passivity Framework for In-band Wormhole

In this section, we present a passivity framework for modeling and detecting in-band wormhole attacks mounted by colluding malicious nodes. As in the out-of-band case, the goal of each source is to select the flow rate on each path in order to minimize the average delay experienced while avoiding the wormhole tunnel. In designing network dynamics, including the source rates and detection mechanism, that achieve this goal, we first model the delay experienced on the wormhole link as a function of the number of compromised nodes. Since the delay depends on the number of compromised nodes, we then model the temporal

dynamics of the number of compromised nodes. Lastly, we incorporate the impact of the detection mechanism described in Section 3.2 on both the valid and wormhole links, and show stability of the overall system.

3.4.1 Delay Characteristics of the In-Band Wormhole

Delays experienced by packets traversing an in-band wormhole are proportional to the number of nodes comprising the wormhole tunnel. Let W_1 and W_2 denote the compromised nodes that create the in-band wormhole tunnel. Recall from Section 3.2 that, in order to avoid wormhole tunnel collapse, packets entering the wormhole tunnel must be routed through a third colluding node, denoted W_3. The number of hops in the wormhole tunnel is therefore equal to $d(W_1, W_3) + d(W_3, W_2)$. Furthermore, from Lemma 3.1, the node W_3 must satisfy

$$d(W_1, W_3) < d(W_2, W_3) + 3. \tag{3.6}$$

While the locations of W_1 and W_2 are fixed for a given wormhole tunnel, the location of W_3 depends on the set of nodes compromised by the adversary, denoted $\mathcal{C}$.

In order to minimize delays, and therefore attract more network flow to the wormhole tunnel, the adversary selects the node $W_3 \in \mathcal{C}$ that minimizes $d(W_1, W_3) + d(W_3, W_2)$ to collude in establishing the wormhole, subject to the constraint (3.6). Letting x denote the fraction of nodes that are misbehaving, and letting $\tilde{\mathcal{C}} = \{W_3 \in \mathcal{C} : d(W_1, W_3) < d(W_2, W_3) + 3\}$, we define

$$\beta(x) \triangleq \mathbf{E}\left[\min_{W_3 \in \tilde{\mathcal{C}}} \{d(W_1, W_3) + d(W_3, W_2)\} \mid |\mathcal{C}| = nx\right],$$

where $\mathbf{E}(\cdot)$ denotes expectation and n is the total number of nodes.

Since the delay experienced by the in-band wormhole is a function of the fraction of compromised nodes, a dynamical model of the fraction of compromised nodes is required.

3.4.2 Dynamics of Fraction of Compromised Nodes

The goal of the adversary is to minimize the delay of the wormhole link by compromising nodes. We let $c_A x$, where $c_A > 0$, denote the cost of compromising a fraction x of the nodes,

and define the adversary's utility function by $U_A(x) \triangleq (n - \beta(x)) - c_A x$, where the first term is the reduction in the path length caused by compromising the fraction of nodes x, and $c_A x$ is the cost. In order to obtain the maximum value, we assume that the adversary chooses the rate at which nodes are compromised via a gradient ascent algorithm, so that

$$\dot{x}(t) = (-\beta'(x) - c_A)_+, \tag{3.7}$$

where $(z)_+ = z$ if $z \geq 0$ and $(z)_+ = 0$ otherwise. The following proposition proves that $U_A(x)$ has a unique global maximum.

Proposition 3.5. *Suppose that, for a given value of x, the set of compromised nodes is chosen uniformly at random from $\mathcal{C}_x = \{\mathcal{C} : |\mathcal{C}| = nx\}$. Then the function $\beta(x)$ is decreasing and convex in x.*

A proof can be found in [49]. Intuitively, $\beta(x)$ is a non-increasing function in x since as the number of colluding malicious nodes increases, the number of paths that can potentially be used as in-band wormhole tunnels also increases.

Proposition 3.5 implies that the dynamics (3.7) converge to a unique equilibrium which is the global maximum of the utility function. To complete the model of the in-band wormhole, the next step is modeling the mitigation by the network.

3.4.3 Model of Mitigation for In-Band Wormhole

The detection of the in-band wormhole is based on the probability that a communication link is a wormhole tunnel, given observation of the flow rate through the link and the associated delay characteristics. A link experiencing anomalously long delays is judged to have a high probability of being a wormhole. We define B_1 as the event that link l is a wormhole and B_0 as the event that link l is valid. Furthermore, we let $w_l(t)$ denote the system's belief at time t that the link l is a wormhole, with $w_l(t) = Pr(B_1|r_l(t), p_l(t))$, where

$$p_l(t) = \begin{cases} f_l(r_l(t)), & l \text{ valid} \\ \beta_l(x) f(r_l), & l \text{ wormhole} \end{cases}$$

The effect of the detection process on the flow allocation is modeled as an increase in the link price, so that the price is increased by $K\mathbf{1}(w_l(t) > \overline{w})$, where K represents a penalty for routing packets through suspected wormhole links, $\mathbf{1}$ denotes the indicator function, and $\overline{w}$ is a predefined threshold.

A model of the wormhole delay dynamics, taking the derivative of the source rate $\dot{r}$ as input and giving the delay $p - p^*$ as output, is given by

$$(H_l) \begin{cases} \dot{r}_l(t) &= u(t) \\ \dot{x}(t) &= (-\beta'(x) - c_A)_+ \\ y_l(t) &= \beta_l(x) f(r_l) + K(\mathbf{1}(w_l(t) > \overline{w})) \end{cases}$$

The source rate dynamics are unchanged from Section 3.3, since detection is performed at the link instead of the source level. The steady-state behavior of the system is described as follows.

3.4.4 Steady-state and Stability Analysis for the In-Band Wormhole

In this section, we prove the stability of the in-band wormhole, enabling us to characterize the average delay due to the wormhole in steady state. Stability of the network in the presence of the in-band wormhole is a result of the following proposition, which establishes the passivity of the wormhole link price.

Proposition 3.6. *The wormhole link dynamics (H_l) are passive with input $\dot{r}_l$ and output y_l.*

Proof: To prove passivity when l is a wormhole link, we use the Lyapunov function $V_l(\cdot)$ defined by

$$\begin{aligned} V_l(r_l, x) = \int_{r_l^*}^{r_l} & \beta_l(x) f(s) - \beta_l(x^*) f(r_l^*) \\ & + K(\mathbf{1}(w_l(t) > \overline{w}) - \mathbf{1}(w_l^* > \overline{w}))\, ds \\ & + \int_{x^*}^{x} \left(\int_0^{r_l^*} f(v)\, dv \right) \beta_l'(s)\, ds. \end{aligned}$$

We have

$$\begin{aligned}\dot{V}_l(r_l, x) &= (\beta_l(x) f(r_l) - \beta_l(x^*) f(r_l^*) \\ &\quad + K(\mathbf{1}(w_l(t) > \overline{w}) - \mathbf{1}(w_l^* > \overline{w})))u_l \\ &\quad + \beta_l'(x) \left(\int_{r_l^*}^{r_l} f(s)\ ds + \int_0^{r_l^*} f(s)\ ds \right) \dot{x} \\ &= y_l u_l + \beta_l'(x) \left(\int_0^{r_l} f(s)\ ds \right) (-\beta_l'(x) - c_A)_+ \\ &\leq y_l u_l,\end{aligned}$$

where the final inequality follows from the the fact that $\beta_l(x)$ is nonincreasing (Proposition 3.5) and $f(s) \geq 0$. The fact that $V_l(r_l^*, x^*) = 0$ holds by inspection. It remains to show that $V_l(r_l, x) \geq 0$ for all r_l and x. This holds because f_l and $\mathbf{1}(w_l(t) > \overline{w})$ are assumed to be nondecreasing functions of r_l, while β_l' is an increasing funtion of x by Proposition 3.5. ■

The stability of the system under the in-band wormhole attack is established by the following theorem.

Theorem 3.2. *The source rate* $\mathbf{r}_i$ *satisfies* $\lim_{t\to\infty} \mathbf{r}_i(t) = \mathbf{r}_i^*$.

Proof: The proof follows from the passivity of the source rate (Theorem 3.1) and wormhole delay (Proposition 3.6), and the fact that they form a negative feedback interconnection. ■

Theorem 3.2 implies that the average delay converges to a stable point in the presence of in-band wormhole.

In what follows, using our framework, we show how complex wormhole attacks consisting of both in- and out-of band wormholes can be jointly modeled and mitigated.

3.5 Joint Modeling of Out-of-Band and In-Band Wormholes

At present, in the security literature, out-of-band wormholes and in-band-wormholes are treated using different methods. A more general wormhole that consists of in-band and out-of-band wormholes has not been identified or discussed, though such wormholes can be

conceived. Our framework can naturally model complex wormholes formed by composing in-band and out-of-band wormholes.

We consider a system with a set of out-of-band wormhole links $\mathcal{L}' = \{l'_1, \ldots, l'_w\}$ and in-band wormhole links $\mathcal{L}'' = \{l''_1, \ldots, l''_w\}$. The delay experienced by a valid link is an increasing function of r_l, the flow through the link. The delay experienced by an out-of-band wormhole link is defined by the propagation time and the packet dropping rate, as described in Section 3.3. For an in-band wormhole link, the delay experienced by the wormhole link is function of the expected number of hops in the wormhole tunnel, as described in Section 3.4. These delay characteristics are described by the following dynamics, where the input $u(t)$ is equal to the change in the source rate $\dot{r}(t)$:

$$(H_l) \begin{cases} \dot{r}_l(t) = u_l(t) & \\ y_l(t) = \frac{\alpha_l}{1-\Phi_l(r_l)} - \frac{\alpha_l}{1-\Phi_l(r_l^*)}, & l \in \mathcal{L}' \\ y_l(t) = \beta_l(x) f(r_l) - \beta_l(x^*) f(r_l^*), & l \in \mathcal{L}'' \\ y_l(t) = f_l(r_l) - f_l(r_l^*), & \text{else} \end{cases}$$

We assume that the network employs mitigation schemes for both the in- and out-of-band wormholes. The out-of-band wormhole mitigation mechanism increases the delay on valid and out-of-band wormhole links as discussed in Section 3.3. However, since the in-band wormhole contains colluding nodes that can modify the time stamps using valid cryptographic keys, the out-of-band wormhole mitigation is ineffective and hence adds no delay to in-band wormhole links. The in-band wormhole mitigation mechanism described in Section 3.4 is employed on the valid and in-band wormhole links. Since the out-of-band wormhole link is created using a high capacity, low-latency channel, the adversary can manipulate the delays in order to thwart the statistical mitigation mechanism. Hence our model of the

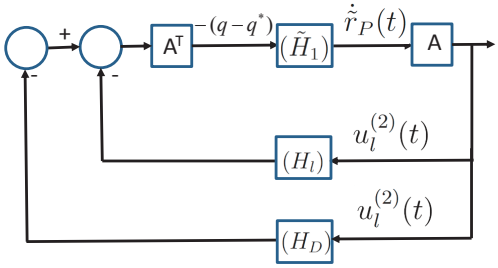


Figure 3.5: Illustration of the interconnection between flow allocation, link delay characteristics, and mitigation when multiple out-of-band and in-band wormholes are present. The system $(\tilde{H}_1)$ defines the flow allocation dynamics as a function of observed delays. The system (H_l) defines the delays experienced by valid, out-of-band, and in-band wormhole links as a function of the flow rates. The system (H_D) models the impact of mitigation mechanisms on the flow allocation dynamics.

impact of mitigation on the link delays is given by the following dynamics:

$$(H_D)\begin{cases} \dot{r}_l(t) = u_l(t) \\ y_l(t) = \left(\frac{1}{1-P_d} - 1\right) f_l(r_l) - \left(\frac{1}{1-P_d^*} - 1\right) f_l(r_l^*), & l \in \mathcal{L}' \\ y_l(t) = K(\mathbf{1}(w_l(t) > \overline{w}) - \mathbf{1}(w_l^* > \overline{w})), & l \in \mathcal{L}'' \\ y_l(t) = \left(\frac{1}{1-P_d} - 1\right) f_l(r_l) - \left(\frac{1}{1-P_d^*} - 1\right) f_l(r_l^*) \\ \qquad +K(\mathbf{1}(w_l(t) > \overline{w}) - \mathbf{1}(w_l^* > \overline{w})), & \text{else} \end{cases}$$

The flow allocation, delay, and mitigation models are illustrated in Figure 3.5. The following theorem characterizes the stability properties of the system when both in-band and out-of-band wormholes are present.

Theorem 3.3. *The interconnected system of Figure 3.5 is globally asymptotically stable.*

Proof: By Theorem 3.1, the top block of Figure 3.5 is strictly passive. The blocks (H_l) and (H_D) are passive by Theorem 3.1 (if l is an out-of-band wormhole) and Proposition

3.6 (if l is an in-band wormhole). Hence the negative feedback interconnection of Figure 3.5 is globally asymptotically stable. ■

Theorem 3.3 implies the passivity based framework enables us to compose in-band and out-of-band wormholes and characterize the overall delay and flow allocation.

3.6 Numerical Study

In this section, we conduct a numerical study using MATLAB. We use our passivity-based framework to answer the following questions for the out-of-band and in-band wormhole attacks: 1) What is the overall flow allocated and delays experienced by sources for a given adversary's strategy? and 2) How do the proposed mitigation methods affect the flow allocation and delays experienced by sources? 3) What is the impact of wormhole attack on a networked control system?

We consider a network which consists of two source nodes S_1, S_2 and a single destination node D shown in Figure 3.7. The source rates for sources 1 and 2 are given as 10 and 5, respectively. Each source allocates flows to three different paths. We denote the path which traverses links 4 and 5 as path 1, the path which traverses links 6 and 7 as path 2, and the path which traverses link 9 as path 3. We assume the propagation delays for valid links are equal and normalized to 1 time unit. The average delay is given as the propagation delay times the expected number of transmissions. The expected number of transmissions for a link is given as $\frac{1}{1-P_d}$ where P_d is the probability of a packet drop. For valid links, we assume the probability of packet drop is due to buffer overflow in an M/M/1/K queue [66]. We denote $\rho_l = \frac{r_l}{c_l}$, where r_l is the amount of traffic flowing into link l, and c_l is the capacity of link l. The probability of a packet drop is given as

$$P_d = \frac{\rho^K - \rho^{K+1}}{1 - \rho^{K+1}} \tag{3.8}$$

In this simulation, we assume the buffer size $K = 5$ for all links.

The propagation delay for the wormhole tunnel, α_l, is assumed to be 2. The clock skew

Δ is an exponential random variable with mean 1. $\Delta_{\max}$ is given as

$$\Delta_{\max} = \alpha_l - 1 + \frac{1}{r}, \tag{3.9}$$

which is a monotonic decreasing function in r.

3.6.1 Simulation of the Out-of-band Wormhole

In the out-of-band wormhole simulation, we assume that link 9 in Figure 3.7 is the wormhole link. The propagation delay for the wormhole link is denoted as α_l, where $\alpha_l > 1$ due to longer physical distance the packet traverses through the wormhole link. The delay for the wormhole link is given as $\frac{\alpha_l}{1-\Phi(r)}$ where $\Phi(r)$ is the dropping rate of packets that flow into the wormhole link. The function $\Phi(r)$ is given as $\Phi(r) = (1 - \frac{1}{r})\mathbf{1}_{(r>1)}$.

We illustrate the impact of the out-of-band wormhole by comparing the flow allocation without the wormhole (Figure 3.6(a)) with the flow allocation resulting from the wormhole (Figure 3.6(b)). In both cases, simulation result shows that our choice of dynamics results in the convergence to the stable equilibrium. Figure 3.6(a) shows that when path 3 contains a poor quality link with low capacity of 0.01 (link 9), both sources allocate negligible amount of flows to path 3 in equilibrium. Figure 3.6(b) shows that packet drops by the wormhole path result in increased delay on path 3, thus reducing the flow allocated to path 3. At the equilibrium, the wormhole drops half of the packets on average. As a result, the wormhole is able to attract only 2 units of flow from both source 1 and 2 combined.

Figure 3.6(d) shows that in order to attract flow, the wormhole has to provide a low-latency link whose performance is comparable to other links. Therefore, the average delay experienced by the sources is approximately the same regardless of the presence of the wormhole link. Figure 3.6(c) shows that when packet leash mitigation methods are employed, the amount of flow allocated to the wormhole link is reduced from 2 to 1.3 units. The overall delay, however, increases due to packet drops caused by the packet leash mitigation method.

3.6.2 Simulation of the In-band Wormhole

In the in-band wormhole simulation, we assume that link 9 is an in-band wormhole. Upon receiving packets allocated to path 3, the malicious node allocates λ fraction of traffic to path 1 and $1-\lambda$ fraction of traffic to path 2. This results in increased traffic to paths 1 and 2 and hence increased overall delay experienced by sources. The perceived delay for path 3 is given as $q(P_3) = \lambda q(r_{P_1} + \lambda r_{P_3}) + (1-\lambda)q(r_{P_2} + (1-\lambda)r_{P_3})$. The mitigation mechanism is based on the anomalous delay experienced at the wormhole link. The link will be avoided if the ratio of actual delay experienced at link l, denoted D_l, to the expected delay exceeds a predefined threshold. The penalty of $K = 10$ was added to the link price when $\log \frac{D_l}{f_l(r_l)} > 0$. The delay experienced at link l is modeled as an exponential random variable with mean $f_l(r_l)$.

We evaluate the impact of the in-band wormhole on flow allocation (Figure 3.8(a)). Packets allocated to path 3, which contains the wormhole link, are rerouted by the adversary to path 2 with probability 0.7. This results in longer delay experienced over path 2. Without mitigation, source 1 is unaware of packets flowing through wormhole tunnels, and allocates all its traffic through paths 1 and 3. Figure 3.8(b) shows the flow allocation when statistical mitigation method is used. Since the packets allocated to path 3 do not traverse a one-hop link with capacity 15 as advertised, but instead traverse a two-hop path with lower capacity, the delay will deviate significantly from its expected value. Hence the statistical mitigation mechanism will identify the wormhole link (link 9) with high probability. This results in an equilibrium point similar to the case without wormhole. Figure 3.8(c) shows the impact of mitigation on average delay. The average delay experienced by source 1 is reduced when mitigation is used. These results suggest that the sources become aware of the true topology of the network, which does not contain path 3, and achieve a Wardrop equilibrium consisting only of paths 1 and 2.

3.6.3 Simulation of Impact of Out-of-band Wormhole on a Physical System

We now study the impact of the out-of-band wormhole on a physical system. We consider a networked control system where the control loop is closed through the network shown in Figure 3.7. The physical plant considered is a single-input, single-output integrator with dynamics given in equation (3.10). We assume the state value $x(t)$ is measured, and sampled every $h = 0.3$ time units by node S_1 and relayed to the controller node D. Disturbance $w(t)$ is assumed to be white Gaussian noise with zero mean and variance 1. Control gain $G = 2$ is considered in the simulation.

$$\begin{aligned} \dot{x}(t) &= u(t) + w(t), \quad t \in [kh + \tau_k, (k+1)h + \tau_{k+1}] \\ u(t) &= -Gx(t - \tau_k), \quad t \in [kh + \tau_k, (k+1)h + \tau_{k+1}] \end{aligned} \tag{3.10}$$

We consider the same M/M/1/K queue model for valid links except the propagation delay α_l for valid links is now assumed to be 0.05 time units, and propagation delay for the out-of-band wormhole link (link 9) is assumed to be 0.1 time units. Adversary controlling the wormhole link provides a low-latency link with delay 0.1 when the flow rate traversing through the wormhole is less than 5 units of flow, and once the flow rate through the wormhole link exceeds 5 units of flow, the adversary drops packets with probability 0.9.

We evaluate the impact of out-of-band wormhole on the physical system in three different cases. In the first case, we assume no mitigation strategy is employed by the network. In the second and third cases, we assume packet leash defense is employed with $\Delta_{\max} = 0.04$ and $\Delta_{\max} = 0.1$ respectively. The clock skew Δ is assumed to be an exponential random variable with mean 0.05.

The impact of wormhole on the physical plant when no mitigation strategy is employed is illustrated in Figure 3.8(d). Adversary first starts providing a low-latency link, attracting a large amount of packets traversing through the wormhole. Once the flow rate through the wormhole exceeds the threshold, the adversary drops packets with high probability, resulting in large disturbance of the plant state $x(t)$. Source node S_1 reallocates flows to paths 1 and 2 once high delay is observed on path 3, and adversary starts attracting flows again by

providing low-latency link.

Figures 3.8(e) and (f) illustrate the effect of mitigation strategies on the physical plant. In both cases, flows allocated to path 3 quickly converges to 0 due to packet leash. However, as shown in Figure 3.8(e), a stringent packet leash with $\Delta_{\max} = 0.04$ results in growing oscillation of $x(t)$ due to overall increased delay. On the other hand, Figure 3.8(f) illustrates that when $\Delta_{\max}$ is chosen appropriately as $\Delta_{\max} = 0.1$, the plant stabilizes around the equilibrium point while successfully mitigating the wormhole attack. This case study shows that parameters of the defense mechanism need to be chosen and adjusted over time to mitigate the attack while maintaining the performance of the physical plant.

3.7 Conclusions and Future Work

In this chapter, we studied the wormhole attack on networked control systems, in which an adversary creates a link between two geographically distant network regions, either using a side channel, as in the out-of-band wormhole, or by colluding network nodes, as in the in-band wormhole. Using the wormhole attack, the adversary can cause violations of timing constraints in real-time systems, including dropping or delaying packets flowing into wormholes. We presented a passivity-based control-theoretic framework for modeling and mitigating the wormhole attack. Under our framework, the flow allocation of the valid nodes, the delays experienced on the wormholes, and the wormhole mitigation algorithms were modeled as distinct, interconnected passive dynamical systems. The passivity approach enabled us to prove stability and convergence of the system to a unique equilibrium, which satisfies the criteria for the well-known Wardrop equilibrium, under general assumptions on the adversary behavior and network mitigation mechanism. This allowed us to characterize the delays experienced by source nodes at the steady-state.

For the out-of-band wormhole attack, we quantified the increase in delay caused by the wormhole link and mapped the adversary's strategy to the optimization problem of selecting the packet-dropping rate. We also introduced an approach for dynamically adapting the parameters of packet leash-based defenses in response to the observed network delays. For

the in-band wormhole, we used spatial statistics to estimate the delays experienced by the wormhole tunnel as a function of the number of misbehaving network nodes. In addition, we identified a new class of complex wormhole attacks consisting of both in- and out-of band wormholes, which we modeled and analyzed using our framework.

Our simulation results illustrate the trade-off between the effectiveness of the network defense and the increase in delay for the out-of-band case. In particular, we found that out-of-band wormhole causes large disturbances in the physical system by selectively dropping packets, and the parameters of packet leash defense can be chosen to reduce flow allocation to the wormhole while satisfying the delay constraint of the physical system. For the in-band case, our simulation suggests that the network defense allows the system to reach the same flow allocation equilibrium regardless of the presence of wormhole.

In our future work, we will investigate whether the steady-state values of our passivity framework arise as equilibria of an equivalent dynamic game between the network and adversary.

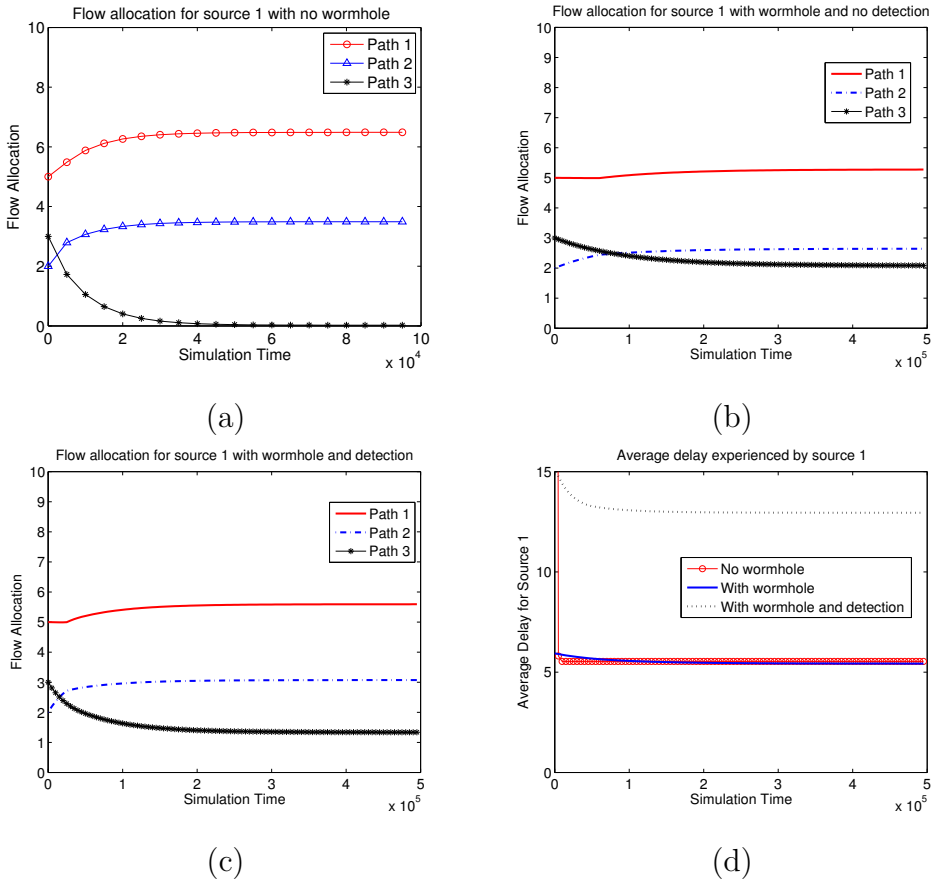


Figure 3.6: Simulation of our passivity framework for modeling the out-of-band wormhole. The time scales represent the number of iterations of the simulation. Each iteration represents a single update step of the wormhole dynamics. The source rates for sources 1 and 2 are given as 10 and 5. Initial flow allocation for source 1 is [5,2,3], and flow allocation for source 2 is [2,2,1] for paths 1, 2, and 3 respectively. (a) The convergence of flow allocation without the wormhole when link 9 has capacity 0.01. (b) The impact of the wormhole on flow allocation with no mitigation mechanisms. (c) The flow allocation when packet leashes method are used.

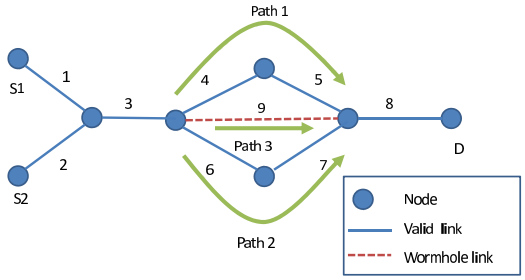


Figure 3.7: Network topology used in numerical study. Two sources send flows with total rate of 10 and 5 to destination D. Each source maintains a path through links 4 and 5 (path 1), a path through links 6 and 7 (path 2), and a path through the wormhole link 9 (path 3).

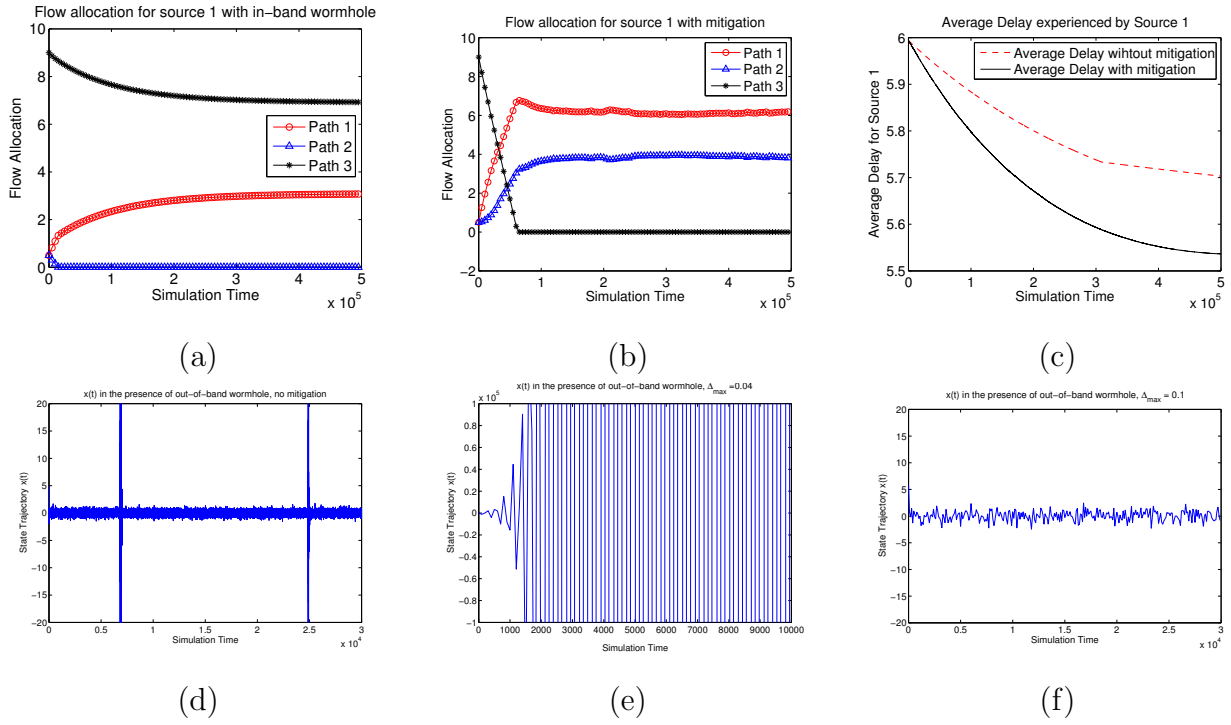


Figure 3.8: Simulation of our passivity framework for modeling the in-band wormhole and the effect of wormhole attacks on the networked control system. The time scales represent the number of iterations of the simulation. Each iteration represents a single update step of the in-band wormhole dynamics. The source rates for sources 1 and 2 are given as 10 and 5. Initial flow allocation for source 1 is [0.5,0.5,9], and flow allocation for source 2 is [0.5,0.5,4] for paths 1, 2, and 3 respectively. Link 9 is an wormhole link with falsely advertised capacity of 15. Packets allocated to path 3 will be rerouted to path 1 with probability 0.3 and to path 2 with probability 0.7. (a) The impact of an in-band wormhole on flow allocation with no mitigation mechanisms. (b) The flow allocation when mitigation method is used. (c) The impact of mitigation method on average delay. (d) No mitigation strategy employed (e) Packet-leash is employed with $\Delta_{\max} = 0.04$ (f) Packet-leash is employed with $\Delta_{\max} = 0.1$.

Chapter 4

PASSIVITY-BASED MODELING OF ROUTING ATTACKS

4.1 Introduction

Cyber-physical systems (CPS), including wide-area monitoring in the smart grid, require real-time information exchange between distributed components [30]. This information exchange is increasingly provided by wireless networks. The use of a shared medium, however, leaves wireless networks vulnerable to medium-exploiting attacks. In a jamming attack [62], an adversary broadcasts an interfering signal in the vicinity of a receiver, thus preventing transmitted packets from being correctly decoded. All network flows traversing a jammed link will experience lower throughput and increased end-to-end latency.

Network sources respond to increases in latency by reallocating flows to lower-latency paths [38]. This approach mitigates the attack by leveraging the spatial diversity provided by multiple disjoint paths. Intelligent adversaries may exploit this behavior, however, by jamming specific links in order to redirect traffic to nodes that collude with, or have been compromised by, an adversary [48, 9]. Once a sufficient amount of network flow traverses these compromised or colluding nodes, an adversary can mount effective, stealthy attacks on higher-layer services, including man-in-the-middle attacks [9, 37] that can violate the real-time constraints of cyber-physical systems [36]. We denote this as the *flow-redirecting jamming attack*.

Current models for the impact of jamming focus on jamming individual links [62, 84], while network flow redirection affects the overall end-to-end performance of source-destination pairs. Existing work on flow jamming considers an adversary whose main goal is to reduce throughput and increase delay [73], as opposed to redirecting network flows towards compromised links.

In this chapter, we develop a control-theoretic approach for modeling flow-redirecting jamming attacks on wireless networks. In our approach, from the adversary's perspective, the flow allocation by the network sources is modeled as a plant, while jamming at targeted network links acts as a control input. We formulate the adversary's goal of redirecting network flows to compromised links as introducing a control input to steer the system towards a desired equilibrium state, which represents a flow allocation where a desired rate of flow traverses compromised links. Modeling flow-redirection in a control-theoretic language enables integration of the attack into models of cyber-physical systems.

Developing a jamming strategy for flow redirection attacks poses two challenges. First, the network flow allocation by the sources in response to changes in network delays exhibits nonlinear dynamics [38]. Second, the feasible jamming strategies are limited by the power constraints of the adversary.

In order to resolve these challenges, we introduce passivity-based dynamic jamming strategies in which the adversary updates the jamming probability based on the rate of flow traversing each link. We show that our passivity-based jamming strategies guarantee convergence to the adversary's desired network flow under nonlinear flow allocation dynamics. We identify a class of physically relevant jamming strategies that can be represented as passive dynamical systems.

We formulate the optimal jamming strategy as the solution to a convex optimization problem. The power limitations of the adversary are mapped to constraints on the feasible jamming strategy. We prove that, if there exists a jamming strategy that satisfies a given power constraint and achieves a desired flow allocation, then a passivity-based jamming strategy can be constructed with the same power constraint, implying that the passivity-based approach is optimal in terms of power consumption. Our approach is illustrated through a numerical study.

The chapter is organized as follows. Section 4.2 describes the network and adversary models, and gives needed background on passivity. Section 4.3 presents a problem formulation for the flow redirection attack. Section 4.4 contains our passivity-based approach

to redirecting the flow to a desired operating point via jamming. Section 4.5 includes our numerical results. Section 4.6 concludes the chapter.

4.2 Model and Preliminaries

In this section, we present the network and adversary models.

4.2.1 Network Model

We consider a network with n source-destination pairs, indexed in the set $\{s_1, \ldots, s_n\}$. The set of network links is denoted $\mathcal{L}$, with $|\mathcal{L}| = L$. Each link $l \in \mathcal{L}$ has a capacity c_l. Each source s_i has a set of paths $\mathcal{P}_i$; we let $\mathcal{P} = \bigcup_{i=1}^{n} \mathcal{P}_i$, and $m_i = |\mathcal{P}_i|$, with $m = \sum_i m_i$. We define the $n \times m$ path matrix H by $H_{ip} = 1$ if path p is used by source i and $H_{ip} = 0$ otherwise. The $L \times m$ routing matrix A is defined by $A_{lp} = 1$ if link l belongs to path p and 0 otherwise. We let $x_p(t)$ denote the flow allocated to path p at time t, and $\mathbf{x}(t)$ denote the vector of flow allocations. Each source s_i chooses $x_p(t)$ for all $p \in \mathcal{P}_i$ at each time t. The vector $\mathbf{z} = A\mathbf{x}$ is the vector of flows allocated to each link, where z_l is the flow allocated to link l. The vector $\mathbf{y} = H\mathbf{x}$ is the total flow allocated to all sources. The link capacity constraints imply that $\mathbf{z} = A\mathbf{x} \leq \mathbf{c}$.

The limited capacities of the links leads to delays. For each link l, the function $\sigma_l : \mathbb{R} \to \mathbb{R}$ is defined such that $\sigma_l(z_l)$ is equal to the delay experienced on link l when the flow rate is equal to z_l. The delay function considered in this work is given as [38]

$$\sigma_l(z_l) = \left(\frac{z_l}{c_l}\right)^{\beta} \tag{4.1}$$

where $\beta > 1$.

4.2.2 Adversary Model

The network is assumed to be attacked by one or more distributed, coordinating jammers. Each jammer can eavesdrop on a link until a packet is observed and then broadcast an interfering signal in order to prevent the packet from being decoded (reactive jammer [62]).

We assume that the interfering signal has sufficient power to cause the packet to be jammed with probability 1. The adversary is assumed to have knowledge of the network topology, link capacities, and flow rates allocated to each link. Furthermore, the flow allocation algorithms of the sources are assumed to be known by the adversary, so that the adversary can predict how the sources will react to a jamming attack.

The adversary is assumed to be power-constrained, with total power budget P_j and cost α_l to jam one bit of flow on link l. The cost α_l is determined by the adversary's distance to the receiver, the path-loss of the environment, and the anti-jamming mechanisms employed by the nodes comprising the link. Letting v_l denote the number of times that each packet is jammed on link l (due to retransmissions), the adversary's power constraint is modeled as the inequality $\sum_{l\in\mathcal{L}} \alpha_l v_l z_l \leq P_j$.

The adversary is assumed to control a subset of links $\mathcal{L}' \subseteq \mathcal{L}$. A link is controlled by the adversary if one or both of the nodes comprising the links has been compromised by or colludes with the adversary. The goal of the adversary is to redirect the network flows to links in $\mathcal{L}'$, in order to mount higher-layer attacks [37, 55].

4.3 Control-Theoretic Framework for Flow Redirection

We assume that each source s_i has an associated utility function $U_{s_i}(y_{s_i})$ which is concave and monotonically increasing in y_{s_i}, the total transmission rate of s_i. Each source s_i observes the end-to-end path delay of path $r_i \in \mathcal{P}_i$ and updates flow rate per each path via the following dynamics

$$\dot{x}_{r_i} = \left(U'_{s_i}(y_{s_i}) - \sum_{l\in r_i} \sigma_l(z_l, v_l) \right)_+^{x_{r_i}} \tag{4.2}$$

where

$$(f(x))_+^{x_{r_i}} = \begin{cases} 0, & x_{r_i} = 0 \text{ and } f(x) < 0 \\ f(x), & \text{else} \end{cases}$$

Eq. (4.2) can be interpreted as a gradient ascent, where each source aims to maximize the utility function U_{s_i} subject to the capacity constraint of each link l. It was shown in [38] that

under the flow allocation dynamics (4.2), $\mathbf{x}(t)$ converges to the solution of an optimization problem

$$\max \sum_{i=1}^{n} U_{s_i}(y_{s_i}) - \sum_{l} \int_0^{z_l} \sigma_l(\tau) d\tau$$
$$\text{subject to } \mathbf{y} = \mathbf{A}\mathbf{x}, \mathbf{z} = \mathbf{H}\mathbf{x}$$

The impact of jamming on each link l is modeled as a reduction in capacity c_l, and the resulting increase of delay at link l. We assume that the delay at link l is written as

$$\sigma_l(z_l, v_l) = \left(\frac{z_l}{c_l}\right)^{\beta} (v_l + 1)$$

In the absence of any jamming at link l ($v_l = 0$), the delay function reduces to $\sigma_l(z_l)$.

The impact of jamming on flow allocation dynamics can be written as the following. For each route r_i,

$$\dot{x}_{r_i} = \left(U'_{s_i}(y_{s_i}) - \sum_{l \in r_i} \sigma_l(z_l) + \sum_{l \in r_i} \sigma_l(z_l) - \sum_{l \in r_i} \sigma_l(z_l, v_l) \right)_+^{x_{r_i}}$$

The flow allocation dynamics can be simplified to

$$\dot{x}_{r_i} = \left(U'_{s_i}(y_{s_i}) - \sum_{l \in r_i} \sigma_l(z_l) + \sum_{l \in r_i} \sigma_l(z_l)(v_l) \right)_+^{x_{r_i}}$$

The v_l can be interpreted as the adversarial control exerted by jammers at link l, and we define the parameter $u_l = v_l$. From the adversary's perspective, the flow allocation can be viewed as a state-space system defined by

$$(\Sigma) \begin{cases} \dot{\mathbf{x}}(t) = f(\mathbf{x}(t)) + g(\mathbf{x}(t))\mathbf{u}(t) \\ \mathbf{y}(t) = \mathbf{x}(t) \end{cases} \tag{4.3}$$

The goal of the jammer is to choose the signal $\mathbf{u}(t)$ in order to stabilize the system at the flow allocation $\mathbf{x}^*$.

4.4 Passivity Approach to Optimal Jamming Strategy

In this section, we present a passivity-based approach for optimal jamming by the adversary. The goal of the adversary is to introduce a control input $\mathbf{u}(t)$ that drives the network flow rates to the adversary's desired allocation $\mathbf{x}^*$, while satisfying the adversary's power constraints at each time t. In Section 4.4.1, we present a decomposition of the network flow allocation and link delay dynamics, and prove the passivity properties of each component of the decomposed model. In Section 4.4.2, we formulate a passivity-based jamming strategy of the adversary and prove that this jamming strategy drives the flow allocation to the desired equilibrium point. Section 4.4.3 incorporates the adversary's power constraint into our framework by presenting an efficient approach to designing a jamming strategy that guarantees the desired equilibrium point while satisfying the adversary's power constraints.

4.4.1 Decomposition of Flow Allocation and Jamming

We decompose the dynamical system of (4.3) into three components, the *flow allocation*, *congestion delay*, and *jamming delay* (Figure 4.1). The flow allocation component contains the flow allocation by the network sources, with state variables $x_{i,j}(t)$ representing the rate of flow allocated by sources s_i to path $p_j \in \mathcal{P}_i$. It takes as input the total delay $q_{i,j}$ on each path, and has state dynamics $\dot{x}_{i,j}(t) = [U'(\mathbf{1}^T\mathbf{x}_i) - q_{i,j}]^+_{x_{i,j}}$ as in Section 4.3. The output of the flow allocation is the rate of change of the flow allocation, $\dot{x}_{i,j}(t)$. This output is multiplied by the routing matrix A to yield the rate of change of the flow allocation on each link, $\tilde{w}_l(t) \triangleq \dot{z}_l(t)$. The signal $\tilde{w}_l(t)$ acts as input to the remaining components.

The second component consists of the delays due to congestion, and takes as input the rate of change in the flow allocation at each link, $\tilde{w}_l(t)$. The state is equal to the flow allocated to the link, $z_l(t)$, and hence the state is equal to the integral of the input. Since the delay is an increasing function σ_l of the incoming flow rate, the delay dynamics are given by $p_l(t) = \sigma_l(z_l(t))$.

The final component consists of the delays due to jamming by the adversary. In its

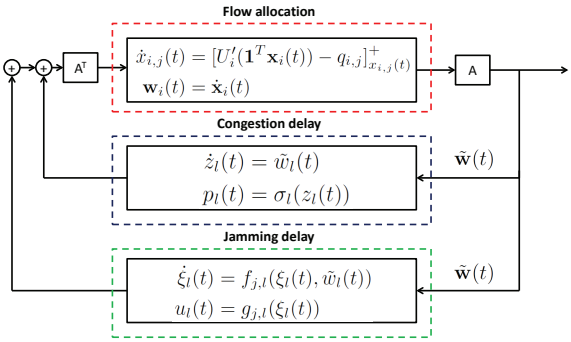


Figure 4.1: Decomposition of network flow dynamics under jamming attack into flow allocation, congestion delay, and jamming delay components. The decomposition enables passivity-based design of the optimal jamming strategy.

most general form, the adversary's jamming strategy has an internal state $\xi_l(t)$ for each link, with dynamics $\dot{\xi}_l(t) = f_{j,l}(\xi_l(t), \tilde{w}_l(t))$. The output is the additional delay in link l due to jamming, denoted $u_l(t)$, which is a function of the current state $\xi_l(t)$ and the input $\tilde{w}_l(t)$.

4.4.2 Passivity-Based Jamming Strategy

We now describe the passivity-based approach to designing the jamming strategy. Since the goal of the adversary's strategy is to drive the flow allocation to a desired point $\mathbf{x}^*$, we first introduce a sufficient condition for $\mathbf{x}^*$ to be a fixed point of the dynamics (Σ) in Figure 4.1.

Lemma 4.1. *Let $\boldsymbol{\xi}^*$ satisfy $f_{j,l}(\xi_l, 0) = 0$ for all $l \in \mathcal{L}$, and define $\mathbf{u}^* = g_j(\boldsymbol{\xi}^*)$, $p_l^* = \sigma_l(z_l^*)$, $\mathbf{p}^* = \{p_l^* : l \in \mathcal{L}\}$, and $\mathbf{q}^* = A^T(\mathbf{p}^* + \mathbf{u}^*)$. If $U_i'(\mathbf{1}^T\mathbf{x}_i^*) = q_{ij}^*$ for all $i = 1, \ldots, n$ and $j = 1, \ldots, m_i$, then $(\mathbf{x}^*, \boldsymbol{\xi}^*)$ is an equilibrium point of the dynamics in Figure 4.1.*

Proof. It suffices to show that all of the state variables of Figure 4.1 achieve equilibrium at the point $(\mathbf{x}^*, \boldsymbol{\xi}^*)$. By assumption, $U_i'(\mathbf{1}^T\mathbf{x}_i^*) = q_{ij}^*$ for all $i = 1, \ldots, n$ and $j = 1, \ldots, m_i$, and hence $\dot{x}_{i,j} = 0$ for all $i = 1, \ldots, n$ and $j = 1, \ldots, m_i$. Since $\tilde{\omega}_l(t) = A\dot{\mathbf{x}}(t) = 0$, $\dot{z}_l(t) = 0$ for all $l \in \mathcal{L}$, and hence z_l reaches a fixed point. Finally, since $f_{j,l}(\xi_l^*, 0) = 0$ for all $l \in \mathcal{L}$, the state $\boldsymbol{\xi}(t)$ is in equilibrium as well. □

Let $\mathbf{q}^*$ be the vector of path costs satisfying $q^*_{ij} = U_i'(\mathbf{1}^T\mathbf{x}^*_i)$ for all $i = 1, \ldots, n$, $j = 1, \ldots, m_i$. The following theorem defines a class of jamming strategies that are guaranteed to converge to the desired state $\mathbf{x}^*$.

Theorem 4.1. *Define a jamming strategy by $f_{j,l}(\xi_l, \tilde{w}_l) = \tilde{w}_l$. Choose $g_{j,l}(\xi_l) = \tilde{\sigma}_l(\xi_l) - \sigma_l(\xi_l)$, where $\tilde{\sigma}_l$ is an increasing function satisfying $\tilde{\sigma}_l(z^*_l) = u^*_l$ and $\mathbf{u}^*$ satisfies $A^T(\mathbf{u}^* + \mathbf{p}^*) = q^*$. Then $\lim_{t\to\infty} \mathbf{x}(t) = \mathbf{x}^*$.*

Proof. By Lemma 4.1, $\mathbf{x}^*$ is an equilibrium point. The remainder of the proof is in two parts. We first show that, for appropriate choice of input and output, each of the three blocks in Figure 4.1 is a passive dynamical system. We then leverage the fact that a negative feedback interconnection of passive systems is globally asymptotically stable to prove that the system converges to the equilibrium $\mathbf{x}^*$.

Consider the component (H_1). We show that (H_1) is passive from input $-(\mathbf{q} - \mathbf{q}^*)$ to output $\mathbf{w}$. Defining

$$V_1(\mathbf{x}) = \sum_{i=1}^{n} \left(U_i(\mathbf{1}^T\mathbf{x}^*_i) - U_i(\mathbf{1}^T\mathbf{x}_i)\right) + (\mathbf{q}^*)^T(\mathbf{x} - \mathbf{x}^*),$$

we have

$$\begin{aligned}
\dot{V}_1 &= -\left(\sum_{i=1}^{n} U_i'(\mathbf{1}^T\mathbf{x}_i)\right)^T \dot{\mathbf{x}}_i + (\mathbf{q}^*)^T\mathbf{x} \\
&= -\left(\sum_{i=1}^{n} U_i'(\mathbf{1}^T\mathbf{x}_i)\dot{\mathbf{x}}_i\right) + \mathbf{q}^T\dot{\mathbf{x}} + (\mathbf{q}^* - \mathbf{q})^T\dot{\mathbf{x}} \\
&= -||\dot{\mathbf{x}}||_2^2 + (\mathbf{q} - \mathbf{q}^*)^T\dot{\mathbf{x}} \leq -(\mathbf{q} - \mathbf{q}^*)^T\dot{\mathbf{x}}
\end{aligned}$$

implying passivity of (H_1).

We now show that the bottom two blocks can be viewed jointly as a passive system with input $\tilde{\mathbf{w}}$ and output $(\mathbf{p} + \mathbf{u} - \mathbf{p}^* - \mathbf{u}^*)$. Define a storage function equal to

$$V_2(\mathbf{z}, \boldsymbol{\xi}) = \sum_{l\in\mathcal{L}} \int_0^{z_l - z^*_l} \tilde{\sigma}_l(\tau_l + z^*_l) - \tilde{\sigma}_l(z^*_l)\, d\tau_l.$$

We then have

$$\begin{aligned}\dot{V}_2(\mathbf{z},\boldsymbol{\xi}) &= \sum_{l\in\mathcal{L}} (\tilde{\sigma}_l(z_l) - \tilde{\sigma}_l(z_l^*))\tilde{w}_l \\ &= \sum_{l\in\mathcal{L}} (\sigma_l(z_l) + g_{j,l}(\xi_l) - \sigma_l(z_l^*) - g_{j,l}(\xi_l^*))\tilde{w}_l \\ &= \tilde{\mathbf{w}}^T(\mathbf{p} + \mathbf{u} - \mathbf{p}^* - \mathbf{u}^*)\end{aligned}$$

establishing passivity of the joint dynamics of (H_2) and (H_3).

Hence, under these jamming dynamics, the overall system (4.3) illustrated in Figure 4.1 can be viewed as a negative feedback interconnection of passive systems, and hence is globally asymptotically stable, with equilibrium point $\mathbf{x}^*$. □

Theorem 4.1 provides a simple jamming strategy in which the adversary's control input at each link is an increasing function of the flow traversing the link. The jammer dynamics are sufficient to guarantee that the network flow reaches the desired allocation $\mathbf{x}^*$. The theorem, however, does not incorporate the power constraints of the adversary, and hence may provide an infeasible jamming strategy. In the following section, we present an approach to selecting the function $\tilde{\sigma}(\cdot)$ in order to satisfy the resource constraints of the adversary.

4.4.3 Incorporating Power Constraint of Adversary

When constructing the adversary's jamming strategy $\tilde{\sigma}_l$, we first observe that the function must be increasing in z_l. The next requirement is that the point $\mathbf{x}^*$ is an equilibrium. Define $\tilde{\boldsymbol{\sigma}}^* = \{\tilde{\sigma}_l^{(m_l)} : l \in \mathcal{L}\}$. The equilibrium requirement can then be stated as $\mathbf{q}^* = A^T\tilde{\boldsymbol{\sigma}}^*$, where $\mathbf{q}^*$ is defined as in Theorem 4.1.

The final requirement is the power constraint. As described in Section 5.2.1, the adversary's power constraint is given by

$$\sum_{l\in\mathcal{L}} \alpha_l v_l(z_l) z_l \leq P_j, \tag{4.4}$$

where α_l is the cost to jam each packet, v_l is the expected number of times to jam each packet, and z_l is the rate of flow traversing link l. In order to ensure feasibility of the

jamming strategy, we require that this constraint is satisfied for each feasible flow allocation, i.e., each $\mathbf{z}$ satisfying $\mathbf{z} = A\mathbf{x}$ and $\mathbf{z} \leq \mathbf{c}$. The following theorem defines a construction for the functions $\tilde{\sigma}_l$ that guarantees that all of the constraints are satisfied.

Theorem 4.2. *Suppose that there exists $\tilde{\boldsymbol{\sigma}}^*$ such that $A^T\tilde{\boldsymbol{\sigma}}^* = \mathbf{q}^*$, $\tilde{\sigma}_l^* \geq \sigma_l(z_l^*)$, and*

$$\sum_{l\in\mathcal{L}} \left(\left(\frac{c_l}{z_l^*} \right)^{\beta} \tilde{\sigma}_l^* - 1 \right) \alpha_l z_l < P_j. \tag{4.5}$$

Then there exists a set of functions $\{\sigma_l : l \in \mathcal{L}\}$ that satisfies the conditions of Theorem 4.1 and the power constraint (4.4).

Proof. We prove that a function exists of the form

$$\tilde{\sigma}_l(z_l) = \begin{cases} \sigma_l(z_l), & z_l \in [0, z_l^* - \epsilon) \\ \frac{\tilde{\sigma}_l^* - \sigma_l(z_l^* - \epsilon)}{\epsilon}(\sigma_l - \sigma_l^*) + \tilde{\sigma}_l^*, & z_l \in [z_l^* - \epsilon, z_l^*] \\ \max\left\{\sigma_l(z_l), \tilde{\sigma}_l^* + \epsilon(z_l - z_l^*)\right\}, & z_l \in (z_l^*, \infty) \end{cases} \tag{4.6}$$

for some $\epsilon > 0$. We observe that the function $\tilde{\sigma}_l$ is increasing as a function of z_l for all $l \in \mathcal{L}$. By construction, $\tilde{\sigma}_l(z_l^*) = \tilde{\sigma}_l^*$ for all $l \in \mathcal{L}$ and $A^T\tilde{\boldsymbol{\sigma}}^* = \mathbf{q}^*$. Hence, the conditions of Theorem 4.1 are satisfied and convergence to the desired flow allocation $\mathbf{x}^*$ is guaranteed. It suffices to prove that the power constraints are satisfied.

Our approach is to bound $\alpha_l v_l(z_l) z_l$ on each link for all $z_l \in [0, c_l]$. First, suppose that $z_l \in [0, z_l^* - \epsilon)$. We have $\tilde{\sigma}_l(z_l) = \sigma_l(z_l)$, and hence $v_l(z_l) = 0$.

Now, suppose that $z_l \in [z_l^* - \epsilon, z_l^*]$. Define

$$R_l(\epsilon) = \sup\left\{\alpha_l v_l(z_l) z_l : z_l \in [z_l^* - \epsilon, z_l^*]\right\}.$$

The function $R_l(\epsilon)$ is continuous as a function of ϵ and satisfies

$$\lim_{\epsilon\to 0} R_l(\epsilon) = \left(\left(\frac{c_l}{z_l^*} \right)^{\beta} \tilde{\sigma}_l^* - 1 \right) \alpha_l z_l^*.$$

Defining δ as

$$\delta \triangleq \frac{P_j - \sum_{l\in\mathcal{L}} \left(\left(\frac{c_l}{z_l^*} \right)^{\beta} \tilde{\sigma}_l^* - 1 \right) \alpha_l z_l^*}{L} > 0,$$

we can choose ϵ sufficiently small such that

$$R_l(\epsilon) < \sum_{l \in \mathcal{L}} \left(\left(\frac{c_l}{z_l^*} \right)^{\beta} \tilde{\sigma}_l^* - 1 \right) \alpha_l z_l^* + \delta$$

for all $l \in \mathcal{L}$.

Finally, if $z_l > z_l^*$, we have two cases. If $\sigma_l(z_l) > \tilde{\sigma}_l^* + \epsilon(z_l - z_l^*)$, then $v_l = 0$. Otherwise,

$$v_l = \left(\frac{c_l}{z_l} \right)^{\beta} (\tilde{\sigma}_l^* + \epsilon(z_l - z_l^*)) - 1$$

and

$$\alpha_l v_l z_l = \left(c_l^{\beta} z_l^{(1-\beta)} (\tilde{\sigma}_l^* + \epsilon(z_l - z_l^*)) - z_l \right) \alpha_l.$$

Dividing by α_l and differentiating with respect to z_l yields

$$c_l(1-\beta) z_l^{-\beta} (\tilde{\sigma}_l^* + \epsilon(z_l - z_l^*)) + c_l^{\beta} z_l^{(1-\beta)} \epsilon - 1. \tag{4.7}$$

When $\epsilon = 0$, Eq. (4.7) is equal to $c_l(1-\beta) z^{-\beta} \tilde{\sigma}_l^* - 1$, which is negative since $\beta > 1$. Hence ϵ can be chosen sufficiently small such that Eq. (4.7) is negative for all $z_l \leq c_l$. This analysis implies that $\alpha_l v_l(z_l) z_l$ is a decreasing function of z_l when $z_l > z_l^*$ and ϵ is chosen appropriately.

Taking these conditions together, we have that (4.4) holds for all $\mathbf{z} \leq \mathbf{c}$, and hence for all feasible flow allocations, completing the proof. □

Theorem 4.2 provides a jamming strategy (4.6) that can be interpreted as not jamming until the flow rate z_l exceeds the desired flow rate z_l^*, and then jamming at the equilibrium rate determined by $\tilde{\sigma}_l^*$. Since there may be multiple feasible jamming strategies $\tilde{\boldsymbol{\sigma}}^*$, we formulate the problem of selecting the minimum-energy jamming strategy as

$$\begin{array}{ll} \text{minimize} & \sum_{l \in \mathcal{L}} \left(\left(\frac{c_l}{z_l^*} \right)^{\beta} \tilde{\sigma}_l^* - 1 \right) \alpha_l z_l^* \\ \tilde{\boldsymbol{\sigma}}^* & \\ \text{s.t.} & A^T \tilde{\boldsymbol{\sigma}}^* = \mathbf{q}^* \\ & \tilde{\sigma}_l^* \geq \sigma_l(z_l^*) \ \forall l \in \mathcal{L} \end{array} \tag{4.8}$$

Eq. (4.8) defines a linear program in $\tilde{\boldsymbol{\sigma}}^*$, and hence can be solved in polynomial time. If the solution of (4.8) satisfies (4.5), then redirecting the network flow to allocation $\mathbf{x}^*$ is feasible.

In fact, a converse result can also be shown, implying that any feasible flow allocation can be achieved using the passivity-based approach.

Proposition 4.1. *Suppose that*

$$\sum_{l\in\mathcal{L}} \left(\left(\frac{c_l}{z_l^*} \right)^{\beta} \tilde{\sigma}_l^* - 1 \right) \alpha_l z_l^* \tag{4.9}$$

for any $\tilde{\boldsymbol{\sigma}}^*$ satisfying the constraints of (4.8). Then there is no energy-feasible jamming strategy that guarantees global asymptotic stability of $\mathbf{x}^*$.

Proof. Let $\dot{\xi}_{j,l}(t) = f_{j,l}(\xi_{j,l}(t), \tilde{w}_l(t))$ and $u_{j,l}(t) = g_{j,l}(\xi_{j,l}(t))$ define a jamming strategy that guarantees global asymptotic stability of $\mathbf{x}^*$. Since $\mathbf{x}^*$ is globally asymptotically stable, $\lim_{t\to\infty} ||\dot{\mathbf{x}}(t)|| = 0$ and

$$\lim_{t\to\infty} ||U'(\mathbf{x}(t)) - \mathbf{q}(t)|| = 0.$$

Furthermore, since $\lim_{t\to\infty} \mathbf{x}(t) = \mathbf{x}^*$ and $U'(\mathbf{1}^T\mathbf{x}^*) = \mathbf{q}^*$, we have that $\lim_{t\to\infty} ||\mathbf{q}^* - \mathbf{q}(t)|| = 0$.

Since $\mathbf{q}(t) = A^T(\mathbf{p}(t) + \mathbf{u}(t))$, there exists $\tilde{\boldsymbol{\sigma}}^*$ such that $A^T\tilde{\boldsymbol{\sigma}}^* = \mathbf{q}^*$, $\tilde{\sigma}_l^* \geq \sigma_l(z_l^*)$, and $||\mathbf{p}(t) + \mathbf{u}(t) - \tilde{\boldsymbol{\sigma}}^*|| < \epsilon$ for any $\epsilon > 0$ and t sufficiently large. Eq. (4.9) then implies that, for t sufficiently large, $\sum_{l\in\mathcal{L}} v_l(t) z_l(t) \alpha_l > P_j$, and hence the jamming strategy violates the power constraint and is infeasible. □

Proposition 4.1 implies that, if there exists a feasible jamming strategy of any type that guarantee convergence to a desired equilibrium point $\mathbf{x}^*$, then there exists a passivity-based jamming strategy of the form described in Theorems 4.1 and 4.2 that guarantees convergence to the desired equilibrium point. Equivalently, Proposition 4.1 implies that the passivity-based jamming strategies are optimal from a power consumption perspective.

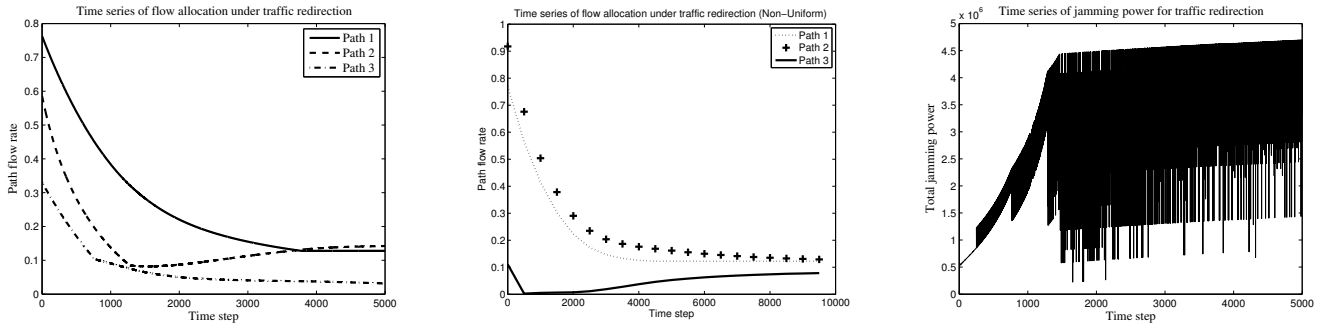
4.5 Numerical Study

We evaluated our approach through a Matlab numerical study. We considered two networks of 200 nodes, one deployed uniformly at random over a square area of width 1200 meters, and the other network deployed non-uniformly such that the average position of each node is at $(500, 500)$ instead of $(600, 600)$. A link was created between two nodes if and only if they were within 300 meters of each other. Three source-destination pairs were selected. Three disjoint paths were chosen for each source-destination pair. Each link was assumed to have unit capacity. Nodes were assumed to have logarithmic utility function, so that $U_{s_i}(\mathbf{y}_i) = \log y_i$ for each node i. The cost function for each link $l \in \mathcal{L}$ was chosen as $\sigma_l(z_l) = \left(\frac{z_l}{c_l}\right)^{\beta}$.

The number of jammers was equal to 3 and locations of jammers were placed uniformly at random. The power required to jam a link was given by the path-loss model $||p_j - p_r||^{\alpha}$, where p_j is the position of the jammer and p_r is the position of the receiver. Each link was assumed to be compromised by the adversary with probability 0.15. In our study, the goal of the jammer was to ensure that at least fraction $\gamma = 0.2$ of flow traversed the compromised links. A candidate flow allocation of this type was chosen by solving the convex program

$$\begin{aligned} \text{minimize} \quad & \mathbf{1}^T\mathbf{q} \\ \mathbf{q}, \mathbf{x}, \mathbf{y}, \mathbf{z} \quad & \\ & q_p = q_{p'} \ \forall p, p' \in \mathcal{P}_i \\ & \mathbf{z} = A\mathbf{x}, \mathbf{z} \leq \mathbf{c} \\ & \mathbf{y} = H\mathbf{x} \\ & U_i'(y_i) \leq q_p \ \forall p \in \mathcal{P}_i \\ & q_p \geq \textstyle\sum_{l \in p} \sigma_l(z_l) \end{aligned} \tag{4.10}$$

In this formulation, the constraints $q_p = q_{p'}$ for all paths p assigned to a given node were chosen so that $\mathbf{q}$ could define an equilibrium point of the source rate allocation dynamics. The constraint $\mathbf{z} \leq \mathbf{c}$ ensured that the chosen rate satisfied the capacity constraint, while the constraint $U_i'(y_i) \leq q_p$ was chosen as a relaxation of the equilibrium equation $U_i'(y_i) = q_p$. The constraint $q_p \geq \sum_{l \in p} \sigma_l(z_l)$ ensured that the price due to jamming at the equilibrium



(a) (b) (c)

Figure 4.2: A numerical study of flow redirection attacks via jamming on network with 200 nodes deployed uniformly at random over a square area of width 1200 meters. Links were created between nodes within 300 meters of each other. Three source-destination pairs with three disjoint paths each were considered. The goal of the jammer was to cause a fraction $\gamma = 0.2$ of flow to traverse compromised links. (a) Rate of flow allocated to each of the three disjoint paths by source 1 over time. Due to jamming, the rate of flow allocated to paths 1 and 3 decreases, causing more flow to be allocated to path 2, which contains compromised links.(b) Rate of flow allocated to each of the three disjoint paths by source 1 over time in the non-uniform deployment case. In this case, path 3 contained compromised links, and flow increases to path 3 due to jamming on paths 1 and 2. This again resulted in $\gamma = 0.2$ fraction of total flow rate being allocated to path 3. (c) Power consumption of the jammer over time. In order to conserve power, the passivity-based jamming strategy only jams packets when the rate over a link exceeds a certain threshold, resulting in oscillations in the jamming power.

was greater than the price without jamming. Finally, minimizing over $\mathbf{1}^T\mathbf{q}$ ensured that the program chose $\mathbf{q}$ as small as possible, making the constraint $q_p \geq U'_{s_i}(y_i)$ tight. Since this program was used as a heuristic, we manually verified that the points $\mathbf{x}$ were valid equilibria of the flow allocation dynamics.

The goal of our simulation was to observe the impact of the jamming attack on the network flow allocation, and in particular observe the time required for the passivity-based jamming strategy to cause convergence to the adversary's desired allocation. We also investigated the temporal dynamics of the jamming power.

Figure 4.2(a) shows the temporal progression of the flow rate on each path for source 1. In this case, source 1 maintained three disjoint paths to the destination. Paths 1 and 3 contained only non-compromised links, while path 2 contained one compromised link. Over time, the fraction of flow allocated to paths 1 and 3 is reduced, as the adversary jams those paths in order to ensure that additional packets traverse the compromised path 2.

Figure 4.2(b) shows the temporal progression of the flow rate in the non-uniform network case. In this case, path 3 contained compromised links, and jammers were able to redirect the flow to the compromised path by jamming paths 1 and 2. However, because the network was clustered around upper-left corner of the deployed area, the average distances between jammers links increased compared to the uniform deployment case. It was numerically verified that the total power budget P_j required to redirect the flow increases compared to uniform deployment case on average.

The jamming power required to achieve this outcome is illustrated in Figure 4.2(c). The adversary expends jamming power on links that have not been compromised. When the flow traversing a non-compromised link l exceeds the adversary's desired flow rate z_l^*, the adversary increases the probability of jamming, and hence the average jamming power. These increases in power are represented by the peaks in Figure 4.2(b). When the flow is reduced below the level z_l^*, the adversary reduces the jamming probability, causing the local minima in Figure 4.2(b).

4.6 Conclusions and Future Work

We considered flow redirection attacks on wireless networks, in which an adversary jams a set of communication links in order to redirect network flow towards compromised links. The redirected flows are then exposed to higher-layer man-in-the-middle attacks. We studied the problem from the adversary's perspective, and formulated the flow redirection within a control-theoretic framework. In this framework, the network flow allocation by source nodes is viewed as a plant, while the changes in link delays introduced by jamming are modeled as a control input.

We developed a passivity-based approach for selecting a jamming strategy. Based on the passivity framework, we derived a class of dynamic jamming strategies that guarantee convergence to a desired flow allocation. Intuitively, these are threshold-based strategies in which the adversary begins jamming the network flow on a given link after the flow exceeds the desired rate. We proved that, in addition to guaranteeing convergence, these strategies are energy optimal, i.e., if there exists a jamming strategy with a given power constraint that results in a desired flow allocation, then a passivity-based jamming strategy can be derived that satisfies the same power constraint. We characterized the set of feasible flow allocations as the solution to a convex optimization problem.

While our approach assumed that the network protocols, and hence the flow rate dynamics, are known to the adversary, in practice the parameters of higher-layer protocols may be unknown or uncertain. We will investigate robust techniques that incorporate these uncertainties while guaranteeing convergence to a desired flow allocation. Robustness of the attack against external disturbances including changes in network topology will also be analyzed and incorporated. In future work, we will also investigate efficient mitigation strategies against flow redirection attack including detection and identification of colluding nodes and jammers in the network. We will extend our approach to other denial-of-service attacks in wired networks including the Coremelt attack [71].

Chapter 5

PASSIVITY FRAMEWORK FOR COMPOSING AND MITIGATING MALWARE PROPAGATION

5.1 Introduction

The growing reliance on computer networks for communication creates a corresponding increase in the threat of computer malware. Computer malware is an application that infects and installs itself on a host, and then uses the resources of that host to attempt to infect other devices. Infected hosts often form large botnets that are controlled by one or more malicious adversaries and used to mount attacks including denial of service and spam campaigns [27]. Malware has been growing in sophistication, with new attack vectors targeting social networks [86] and mobile devices [88].

A variety of defense mechanisms have been developed for thwarting the spread of malware. The standard approach is to periodically patch hosts against known malware, thus removing the infection and, depending on the type of malware, preventing reinfection in the future. Proactive defenses include scanning network traffic with intrusion detection systems to identify malware signatures and quarantine infected hosts [91].

While each defense mechanism mitigates the spread of malware, there is also an associated performance cost, including host downtime during patching, delays due to packet filtering, and allocation of system resources to decoy networks. In order to determine appropriate parameters (e.g., patching rate) of a mitigation strategy that balance removal of malware with system performance, propagation models have been proposed that describe the rate of malware propagation, the impact of the attack, and the effectiveness of mitigation [90, 13]. These models provide an analytical framework for designing a malware defense strategy.

Standard malware propagation models are based on epidemic dynamics such as Susceptible-

Infected-Susceptible (SIS), which depend on the network topology, scanning rate of the malware, and probability that a scanned host becomes infected. In general, however, propagation characteristics such as the scanning rate are unknown *a priori*, leading to uncertainties in the design of mitigation parameters. Such a mitigation strategy could incur unnecessarily large overhead or fail to control the spread of malware [31].

These uncertainties are especially pronounced when multiple malware strains propagate through a network simultaneously. The interactions between different strains are complex and inherently unpredictable. In the case of *competing* malware, one malware strain may install anti-virus software in order to remove or block other malware from compromising the same host [7]. *Co-existing* or *colluding* malware, in contrast, may reside together on a single host, and the presence of one malware can facilitate other infections, e.g., by disabling firewalls and anti-virus. At present, however, defense mechanisms that incorporate uncertainties in the propagation of a single malware, let alone multiple co-existing or competing malwares, are in the early stages.

In this chapter, we develop a passivity-based approach to modeling and mitigating multiple malware propagations, using both static and adaptive defenses. By modeling the multi-virus propagation, patching, and filtering as *passive dynamical systems*, we develop intuitive rules for updating the probability of packet inspection in order to guarantee removal of the viruses while minimizing performance overhead. Our specific contributions are as follows:

- We develop a passivity framework for modeling multi-virus propagation and mitigation under SIS malware propagation dynamics. We derive mean-field dynamical models of multi-virus propagation Markov process and prove that the multi-virus propagation and mitigation can be viewed as coupled passive dynamical systems, and show that the required patching rate is characterized by the passivity index of the system. In the case when the propagation rates are known to the defender, we formulate the convex optimization problem of selecting the minimum-cost mitigation strategy to remove multiple viruses at a desired rate.

- When the propagation rates are *not known to the defender apriori*, we consider the class of adaptive patching and filtering based defenses. We propose two adaptive patching-based defenses. In the first defense, we derive an update rule that is guaranteed to ensure asymptotic removal of all viruses in this network. In the second defense, we derive a rule that can drive the probability of infection to be arbitrarily low in the single-virus case while minimizing the performance overhead of mitigation.

- We analyze two performance characteristics of our patching and filtering strategies, namely the convergence rate of the network to the state where all viruses are removed, and the total cost of mitigation. We derive bounds on both characteristics as functions of the update parameters.

- We evaluate our approach via a numerical study. We numerically verify the accuracy of the mean-field approximation by comparing it to the underlying Markov stochastic model via Monte-Carlo method. In addition, we compare the convergence rates under coexisting and competing malware propagation and verifies convergence of the adaptive patching and filtering dynamics to the desired steady-state.

5.2 Model and Preliminaries

This section presents the model and assumptions of the adversary and network defense.

5.2.1 Adversary Model

We consider an undirected network with N hosts. We say there exists an edge (i, j) if hosts $i, j \in N$ can directly communicate with each other. The set of edges are denoted as E. A host j is a neighboring host of i if there exists an edge (i, j) between i and j. The set of neighboring hosts of host i is denoted as N_i. Given a network topology, we define the adjacency matrix A as $|N| \times |N|$ matrix with 0 on the diagonal entries and $A_{ij} = 1$ if $(i, j) \in E$ and $A_{ij} = 0$ otherwise for the off-diagonal entries.

A set of malwares V attempts to infect network hosts. Once a host has been compromised by malware $v \in V$, that host will send malware traffic (e.g., embedded in email, social media, or other data flows) to non-infected neighboring hosts. We model the arrival process of malware traffic of virus v as a Poisson process with rate μ^v. In other words, the interarrival times of malware traffic are independent exponential random variables with mean $\frac{1}{\mu^v}$. The receiving host becomes infected by each malware packet with probability $p^{S,v}$, depending on the set of malwares S currently infecting that host. This dependence is due to the fact that malwares may either install or disable anti-virus software onto a host, thus changing the difficulty of re-infection by a different malware.

A pair of malwares v and w can either be *co-existing* or *competing*. If v and w are co-existing, then both can be present on the same host at any time. If v and w are competing, then malware v will attempt to remove malware w if it is successfully installed on a host; hence, malwares v and w will never reside on the same host. We let C_v denote the set of malwares that compete with malware v.

5.2.2 Network Defense Model

We consider two types of defense mechanisms, namely, *patching* and *packet filtering*. In the patching-based defense, each host is taken offline according to a random process and is inspected for any potential infection. When an infection is detected, the system administrator removes the infection and brings the host back online. The drawback of this defense mechanism is it could induce unnecessary cost of taking hosts offline since the patching process will continue even when all malwares are removed from the network since the inspection and cleaning process is independent from the state of the hosts. On the other hand, in the filtering-based mitigation, each packet that is sent from one host to the other is randomly forwarded according to an independent Bernoulli process to an *intrusion detection system* (IDS), which inspects the packet for malware signatures. If such signatures are detected, all malwares are removed from the host that sent the malware packet. Since a host is taken offline only when a packet that contains malware is detected, filtering-based mitigation avoids

unnecessary cost. However, since the infected host will only send malware traffic to uninfected hosts, the filtering will not be able to detect any infection when all hosts are infected.

In this chapter, we consider susceptible-infected-susceptible (SIS) model [81]. In the patching defense, each host i is taken offline according to a Poisson process with rate β_i, and patched against *all* known malwares. That is, the times between two consecutive patching for host i are modeled as independent exponential random variables with mean $\frac{1}{\beta_i}$. In the packet filtering defense, we assume each packet that is sent from host i to host j is randomly forwarded with probability q to an IDS. The parameters β_i and q vary over time, and are assumed to be set by a centralized entity, which is notified when a malware packet or infected host is detected.

5.3 Multi-Virus Propagation Dynamics

In this section, a Markov model for malware propagation and mitigation is formulated. A state-space dynamical model is derived using a mean-field approximation of the Markov propagation model. We then prove that the propagation model is output feedback passive, as a first step towards a passivity-based approach to designing a mitigation strategy. We formulate the problem of selecting a static patching rate when the propagation parameters are known.

5.3.1 Markov Model and Mean-Field Approximation

The time-varying components of the system model defined in Section 5.2 consist of the set of malwares infecting each host i at time t, denoted $S_i(t) \subseteq V$, as well as the patching rate $\beta_i(t)$ of each host i and the probability of packet filtering, denoted $q(t)$. The quantities $\beta_i(t)$ and $q(t)$ vary over time due to the adaptive defense. Taken together, $\mathcal{S}(t) = (S_1(t), \ldots, S_n(t), \beta_1(t), \ldots, \beta_n(t), q(t))$ comprises the state of the system.

Due to the Poisson assumption on the infection and patching rates, the state $\mathcal{S}(t)$ defines a continuous-time Markov chain with the following transition rates. For malware v, each infected host sends malware packets to each uninfected neighbor with rate μ^v. When a host

i receives a packet infected with malware v at time t, host i becomes infected with malware v and all competing viruses (i.e., $S_i(t) \cap C_v$) are removed with probability $p(S_i(t), v)$. Host i's transition rate from being infected with a set of viruses $S_i(t)$ to being infected with $S_i(t) \setminus C_v \cup \{v\}$ due to a single neighbor infected with virus v is denoted $\lambda^{S,v} \triangleq p(S, v)\mu^v$. Throughout this chapter, we define $\lambda_{\max} = \max_{S,v} \lambda^{S,v}$ and $\lambda_{\min} = \min_{S,v} \lambda_{S,v}$.

Transitions due to the filtering process are described as follows. For any malware v with $v \in S_i(t) \setminus S_j(t)$ with $j \in N_i$, host i sends malware packets to j with rate μ^v, which are inspected with probability $q(t)$. If the malware packet is forwarded to IDS, then the host i is taken offline and all malwares in $S_i(t)$ are removed, resulting in a transition from $S_i(t)$ to $\emptyset$ with rate $\overline{\lambda}^v(t) \triangleq q(t)\mu^v$. The last type of transition occurs due to the patching process. This results in a transition from $S_i(t)$ to $\emptyset$ with rate $\beta_i(t)$.

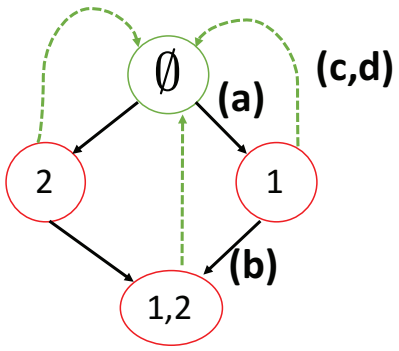


Figure 5.1: Illustration of possible transitions with two malwares 1 and 2 that are coexisting. If $S = \{1\}$, then (a) is the transition into set S by being infected with malware 1, (b) is the transition away from S by being additionally infected with malware 2, and $(c), (d)$ is the transition away from set S due to patching and filtering respectively.

The Markov model defined in this fashion has a number of states that is exponential in the number of hosts and malwares. Instead of dealing directly with all possible combinations of states $S_i(t)$, which is computationally infeasible for large networks, we consider the *average* probability of infection for the tractability of the analysis by applying mean-field approximation analogous to [39, 75, 83]. The mean-field model is described by the states

$\{x_i^S(t) : i \in N, S \subseteq V\}$, defined as the probability that host i is infected with a set of viruses S at time t. In describing the mean-field dynamics, we first observe that the set of subsets of V that can transition to a set S is given by

$$\bigcup_{v \in S} \{(S \setminus \{v\}) \cup R : R \subseteq C_v\} \subset 2^V$$

where 2^V is the power set of the set V. Using the Kolmogorov forward equation [66], the net transitions into state S_i are described by

$$\begin{aligned}
&\dot{x}_i^S(t) \\
&= \sum_{v \in S} \sum_{R \subseteq C_v} \sum_{j \in N_i} \sum_{T \subset V : T \ni v} \big[\lambda^{(S \setminus \{v\} \cup R, v)} && (5.1)\\
&\quad \times Pr(S_i(t) = S \setminus \{v\} \cup R, S_j(t) = T)] \\
&\quad - \sum_{v \notin S} \sum_{j \in N_i} \sum_{T \ni v} \big[\lambda^{S,v}\ Pr(S_i(t) = S, S_j(t) = T)] && (5.2)\\
&\quad - \sum_{v \in S} \sum_{j \in N_i} \sum_{T : v \notin T} \overline{\lambda}^v(t) Pr(S_i(t) = S, S_j(t) = T) && (5.3)\\
&\quad - \beta_i(t) x_i^S(t). && (5.4)
\end{aligned}$$

In the above, Eq. (5.1) describes transitions to S due to infection, while Eq. (7.22) describes transitions from S due to infection with viruses not in S. Eqs. (5.3) and (5.4) describe the impact of filtering and patching, respectively (Transitions (a), (b) and (c,d) respectively in Figure 5.1).

Independence Approximation and its Implication

Throughout this chapter, we make an independence assumption that $Pr(S_i(t) = S, S_j(t) = T) = x_i^S x_j^T$ for all i, j, S, and T. With this assumption, the dynamics of $x_i^S(t)$ are rewritten

as

$$\dot{x}_i^S(t) = \sum_{v\in S}\sum_{R\subseteq C_v}\sum_{j\in N_i}\sum_{T\ni v}\lambda^{(S\setminus\{v\}\cup R,v)}x_i^{S\setminus\{v\}\cup R}x_j^T \tag{5.5}$$

$$-\sum_{v\notin S}\sum_{j\in N_i}\sum_{T\ni v}\lambda^{S,v}x_i^S x_j^T \tag{5.6}$$

$$-\sum_{v\in S}\sum_{j\in N_i}\sum_{T:v\notin T}\overline{\lambda}^v(t)x_i^S x_j^T - \beta_i(t)x_i^S(t). \tag{5.7}$$

This independence assumption is common in models of malware propagation [75, 81]. In the case of single virus propagation, this assumption is known to overestimate the mean-field propagation dynamics [75] under the assumption

$$Pr(S_i = \emptyset | S_j = \{v\}) \leq Pr(S_i = \emptyset). \tag{5.8}$$

In other words, conditioned on the event that a neighboring host j of host i is infected, it cannot increase the probability that i is clean. Since the independence assumption overestimates the propagation dynamics, it implies that any mitigation strategy that is sufficient to remove all malwares with the independence assumption is also sufficient to remove all malwares for the underlying mean-field dynamics. Recently, in the case of competing multi-virus propagation, it was shown [81] that the independence assumption does not systematically over or under estimate the propagation dynamics of *individual* malware propagation (equations (5.5) and (5.6)). On the other hand, if the goal of the defender is to remove *all* malwares, not the individual malware, then it suffices to consider the dynamics of $\bar{x}_i(t) = \sum_{S\subset V:S\neq\emptyset} x_i^S$, the probability that host i is infected with at least one malware at time t. The following theorem shows that the conditional probability assumption (5.8) results in over-estimation of mean field dynamics of $\bar{x}_i(t)$.

Theorem 5.1. *Consider the propagation dynamics of $\bar{x}_i(t)$ in the absence of mitigation strategy given as*

$$\dot{\bar{x}}_i = (1-\bar{x}_i)\sum_{j\in N_i}\sum_{v\in V}\lambda^{\emptyset,v}\,\bar{x}_j^v. \tag{5.9}$$

The dynamics (5.9) provides an upperbound on the mean-field dynamics of $\bar{x}_i$.

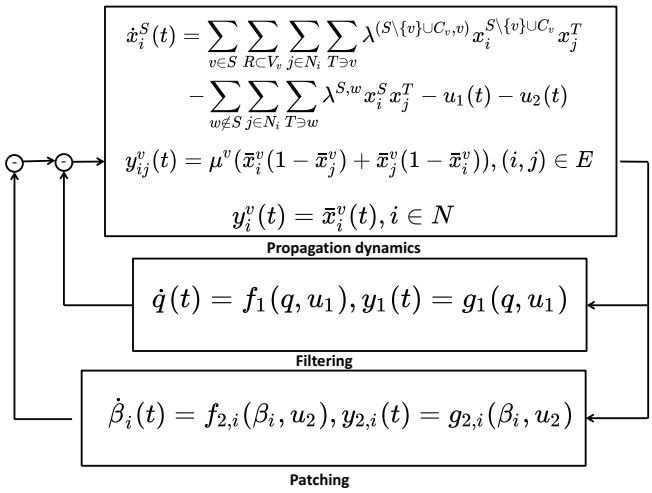


Figure 5.2: Representation of our passivity-based approach, consisting of coupled dynamical systems representing propagation, filtering, and patching.

Proof: Define $\bar{x}_i^v = \sum_{S\ni v} x_i^S$, the probability that host i is infected with malware v at time t, and $\gamma_i^{S\to S'}(t)$ as the transition rate of being infected with set of viruses S' from being infected with S. $\mathbf{1}_{S_i(t)=S}$ is an indicator which equals to 1 if node i is infected with set of viruses S and 0 otherwise. Then from equations (5.5), (5.6), we have

$$\begin{aligned}
\dot{\bar{x}}_i(t) &= \sum_{S\subset V:S\neq\emptyset}\mathbb{E}[\sum_{S'\neq S}\mathbf{1}_{S_i(t)=S'}\gamma_i^{S'\to S}(t)] \\
&- \mathbb{E}[\sum_{S'\neq S:S'\neq\emptyset}\mathbf{1}_{S_i(t)=S}\gamma_i^{S\to S'}(t)] \\
&= \sum_{v\in V}\mathbb{E}[\mathbf{1}_{S_i(t)=\emptyset}\sum_{j\in N_i}\sum_{S\ni v}\lambda^{\emptyset,v}\mathbf{1}_{S_j(t)=S}] \\
&= \mathbb{E}[\mathbf{1}_{S_i(t)=\emptyset}\sum_{j\in N_i}\sum_{v\in V}\sum_{S\ni v}\lambda^{\emptyset,v}\mathbf{1}_{S_j(t)=S}] \\
&\leq (1-\bar{x}_i(t))\sum_{j\in N_i}\sum_{v\in V}\lambda^{\emptyset,v}\bar{x}_j^v
\end{aligned}$$

where the last inequality is from the assumption (5.8). ■

5.3.2 Passivity Analysis of Malware Propagation

Our passivity-based analysis of malware propagation and mitigation decomposes the propagation model into three coupled dynamical systems, namely, multi-virus propagation, filtering-based mitigation, and patching based mitigation (Figure 5.2). The first step in developing our approach is to prove that the propagation dynamics (top block) are output feedback passive.

As a preliminary, we have the following result that provides a storage function for systems characterized by continuous-time Markov chains.

Lemma 5.1. *Consider a finite set V, and the set of state dynamics given as*

$$\dot{x}^S = \sum_{T \neq S} \gamma_{S \to T}(t) x^S(t) - \sum_{S \neq T} \gamma_{T \to S}(t) x^T(t)$$

for $S, T \subset V$. Given a quadratic function $W = \frac{1}{2} \sum_{S \subset (V \setminus \emptyset)} (x^S)^2$, we have

$$\dot{W} = \sum_{T \neq S} \sum_{S \subset (V \setminus \emptyset)} \gamma_{S \to T}(t) \left(-(x^S)^2(t) + x^S(t) x^T(t) \right).$$

In what follows, we analyze the storage function

$$W_i(\mathbf{x}) = \frac{1}{2} \sum_{S \neq \emptyset} (x_i^S)^2$$

using the results of Lemma 5.1.

Lemma 5.2. *Define $\mathbf{u}_i = -\beta_i \mathbf{x}_i$, and $\mathbf{x}_i$ as a column vector of length $2^{|V|} - 1$ where entries enumerate $\{x_i^S\}$ for all possible subset $S \subset V \setminus \emptyset$. The time derivative of $W_i(\mathbf{x})$ is given by*

$$\dot{W}_i \leq \mathbf{x}_i^T Q_i \mathbf{x}_i + \sum_{j \in N_i} \mathbf{x}_j^T Q \mathbf{x}_j + \mathbf{u}_i^T \mathbf{x}_i,$$

where Q_i is a diagonal matrix with diagonal entry corresponding to host i's state being S. The diagonal entries of Q_i are written as

$$Q_i(S, S) = \frac{|N_i|}{6} \sum_{v \in S} \sum_{R \subseteq C_v} 2^{|V \setminus C_v| - 1} \lambda^{S \setminus \{v\} \cup R, v},$$

and $Q = H\Lambda H^T$. *Here* H *is a* $2^{|V|} \times |V|$ *0-1 matrix where each entry* $H_{S,v}$ *corresponds to set* S *(row) and malware* v *(column), which equals to 1 if* $v \in S$ *and 0 otherwise, and* Λ *is a* $|V| \times |V|$ *diagonal matrix with*

$$\Lambda_{vv} = \frac{1}{12} \sum_{S: v \notin S} \lambda^{S,v}.$$

Proof: Let $\mathcal{R}$ be the set of realizable sets where for $S \in \mathcal{R}$, if $v \in S$ then for any $u \in C_v$, $u \notin S$. By Lemma 5.1, $\dot{W}_i(\mathbf{x})$ is equal to

$$\begin{aligned}
\dot{W}_i &= \sum_{S \in \mathcal{R}} \sum_{v \in S} \sum_{R \subseteq C_v} \Big[\gamma_{S \setminus \{v\} \cup R \to S}(t) (-(x_i^{S \setminus \{v\} \cup R})^2 \\
&\quad + x_i^{S \setminus \{v\} \cup R} x_i^S) \Big] \\
&\leq \frac{1}{4} \sum_{S \in \mathcal{R}} \sum_{v \in S} \sum_{R \subseteq C_v} \left[\gamma_{S \setminus \{v\} \cup R \to S}(t) (x_i^S)^2 \right],
\end{aligned}$$

where the inequality follows from the identity $(2x_i^{S \setminus \{v\} \cup R} - x_i^S)^2 \geq 0$. Since $\gamma_{S \setminus \{v\} \cup R \to S}(t) = \sum_{n_j \in N_i} \lambda^{S \setminus \{v\} \cup R, v} \overline{x}_j^v$, we have

$$\begin{aligned}
\dot{W}_i &\leq \frac{1}{4} \sum_{S \in \mathcal{R}} \sum_{v \in S} \sum_{R \subseteq C_v} \sum_{n_j \in N_i} \lambda^{S \setminus \{v\} \cup R, v} \, \overline{x}_j^v (x_i^S)^2 \\
&\leq \frac{1}{12} \sum_{S \in \mathcal{R}} \sum_{v \in S} \sum_{R \subseteq C_v} \sum_{j \in N_i} \lambda^{S \setminus \{v\} \cup R, v} \, (\overline{x}_j^v)^2 \\
&\quad + \frac{1}{6} \sum_{S \in \mathcal{R}} \sum_{v \in S} \sum_{R \subseteq C_v} \sum_{j \in N_i} \lambda^{S \setminus \{v\} \cup R, v} \, (x_i^S)^2
\end{aligned}$$

by the inequality $abc \leq \frac{1}{3}(a^2 + b^2 + c^2)$. We can simplify the the first term as follows:

$$\begin{aligned}
&\sum_{S \in \mathcal{R}} \sum_{v \in S} \sum_{R \subseteq C_v} \sum_{j \in N_i} \lambda^{S \setminus \{v\} \cup R, v} \, (\overline{x}_j^v)^2 \\
= \; &\sum_{v \in S} \sum_{\substack{S \in \mathcal{R}: \\ v \in S}} \sum_{R \subseteq C_v} \sum_{j \in N_i} \lambda^{S \setminus \{v\} \cup R, v} \, (\overline{x}_j^v)^2 \\
= \; &\sum_{v \in S} \sum_{j \in N_i} \left[(\overline{x}_j^v)^2 \left(\sum_{S \in \mathcal{R}: v \notin S} \lambda^{S \setminus \{v\}, S} \right) \right].
\end{aligned}$$

The last equivalence relationship follows from the observation that each set $T \in \mathcal{R}$ with $v \notin T$ appears exactly once in the collection $\mathcal{C} = \{(S \setminus \{v\} \cup R : S \in \mathcal{R}, R \subseteq C_v\}$. To see

this, let $T \in \mathcal{R}$ be a set with $v \notin T$. Let $S = (T \setminus C_v) \cup \{v\}$ and $R = T \cap C_v$. We have $T = S \cup R \setminus \{v\}$, which appears in the collection $\mathcal{C}$.

Now, suppose that there exist S' and R' with $v \in S'$, $S' \in \mathcal{R}$, $R' \subseteq C_v$, $T = S' \cup R' \setminus \{v\}$, and $S' \neq S$ or $R' \neq R$. We have four cases. First, if $S' \neq S$ and there exists $u \in S' \setminus S$, then we must have $u \in R$. However, $u \in R \subseteq C_v$, and hence u and v are both in S', contradicting the assumption that $S' \in \mathcal{R}$.

Second, suppose that $u \in S \setminus S'$. By a similar argument, we must have $u' \in R' \subseteq C_v$, creating a contradiction by the same argument.

Third, suppose that there exists $u \in R' \setminus R$. We must have $u \in S$, however, $u \in C_v$, creating a contradiction since $u, v \in S$ and $S \in \mathcal{R}$. Finally, the case where there exists $u \in R \setminus R'$ is similar.

This yields

$$\dot{W}_i \;\leq\; \frac{1}{12} \sum_{j \in N_i} \sum_{v \in V} \left[\left(\sum_{S : v \notin S} \lambda^{S,v} \right) \left(\sum_{T : v \in T} x_j^T \right)^2 \right] + \frac{|N_i|}{6} \sum_{S \in \mathcal{R}} \left(\sum_{v \in S} \sum_{R \subseteq C_v} \lambda^{S \setminus \{v\} \cup R, v} \right) (x_i^S)^2.$$

■

Two special cases are a set of *competing viruses*, in which $C_v = V \setminus \{v\}$ for all $v \in V$, and *coexisting viruses*, in which $C_v = \emptyset$ for all $v \in V$. In the coexisting virus case,

$$Q_i(S, S) = \frac{|N_i|}{6} \sum_{v \in S} 2^{|V|-1} \lambda^{S \setminus \{v\}, v},$$

while in the competing case

$$Q_i(S, S) = \frac{|N_i|}{6} \left[\sum_{u \neq v} \lambda^{u,v} + \lambda^{\emptyset, v} \right].$$

In general, the passivity index in the competing case will be less than the passivity index in the coexisting case since the exponential term $2^{|V|-1}$ will increase exponentially as the number of malwares increase.

The following theorem implies that the multi-virus propagation is output-feedback passive, and hence that passivity-based techniques can be developed to design a mitigation strategy.

Theorem 5.2. *The mean-field approximation (5.5)–(5.7) of the multi-virus propagation dynamics without filtering ($\bar{\lambda}^v = 0$) is output feedback passive from input ($\mathbf{u}_i = -\beta_i \mathbf{x}_i : i \in N$) to output ($\mathbf{x}_i : i \in N$), with passivity index ρ bounded by*

$$\rho \leq \max_i \left\{ \mu_1(Q_i + |N_i|Q) \right\},$$

where $\mu_1(\cdot)$ denotes the largest eigenvalue of a matrix.

Proof: Select the storage function $W(\mathbf{x}) = \sum_{i \in N} W_i(\mathbf{x})$. By Lemma 5.2,

$$\begin{aligned}
\dot{W}(\mathbf{x}) = \sum_{i \in N} \dot{W}_i &\leq \sum_{i \in N} \mathbf{x}_i^T Q_i \mathbf{x}_i + \sum_i \sum_{j \in N_i} \mathbf{x}_j^T Q \mathbf{x}_j + \sum_{i \in N} \mathbf{u}_i^T \mathbf{x}_i \\
&= \sum_{i \in N} \mathbf{x}_i^T Q_i \mathbf{x}_i + \sum_i |N_i| \mathbf{x}_i^T Q \mathbf{x}_i + \sum_{i \in N} \mathbf{u}_i^T \mathbf{x}_i \\
&= \sum_{i \in N} \mathbf{x}_i^T (Q_i + |N_i|Q) \mathbf{x}_i + \sum_{i \in N} \mathbf{u}_i^T \mathbf{x}_i,
\end{aligned}$$

implying that the system is OFP with passivity index $\max_i \{\mu_1(Q_i + |N_i|Q)\}$. ■

This completes the first step of proving passivity of the propagation dynamics in order to design the patching strategy to remove all malwares at a desired rate.

5.3.3 Design of Static Patching Strategies

If the compromise rates $\lambda^{S,v}$ are known for all S and v, then the results of Lemma 5.2 and Theorem 5.2 can be used to select the patching rates $\{\beta_i : i \in N\}$ while minimizing a desired cost function. The following proposition provides a sufficient condition for removal of all viruses at a desired rate ϵ.

Proposition 5.1. *Let $B_i = \beta_i I_{(2^{|V|}-1)\times(2^{|V|}-1)}$, where I denotes the identity matrix, and let B be a block diagonal matrix with the B_i's as diagonal entries. Define $\overline{Q}$ by*

$$\overline{Q} = A \otimes Q + \begin{pmatrix} Q_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & Q_n \end{pmatrix}.$$

where A is the adjacency matrix of the network, and $\otimes$ is Kronecker product. If $B - \overline{Q} \geq \epsilon I$, where "$\geq$" denotes inequality in the semidefinite cone, then all viruses will be removed in steady-state and $||\mathbf{x}(t)||_2 \leq \sqrt{|N|}e^{-\epsilon t}$ for all $t \geq 0$.

Proof: Using the storage function $W(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T\mathbf{x}$, Theorem 5.2 implies that

$$\dot{W}(\mathbf{x}) \leq \mathbf{x}^T\overline{Q}\mathbf{x}^T - \mathbf{x}^T B\mathbf{x}^T \leq -\epsilon\mathbf{x}^T\mathbf{x}.$$

Therefore, from Theorem 2.1, we have

$$||\mathbf{x}(t)||_2 \leq e^{-\epsilon t}||\mathbf{x}(0)||_2 \leq \sqrt{|N|}e^{-\epsilon t},$$

since $\sum_S x_i^S(0) \leq 1$. ■

Proposition 5.1 implies that an optimal patching strategy can be selected using semidefinite programming, with the problem formulation

$$\begin{aligned} \text{minimize} \quad & \textstyle\sum_{i\in N} c_i(\beta_i) \\ \text{s.t.} \quad & B \geq \overline{Q} + \epsilon I \\ & \beta_i \geq 0 \ \forall i, \end{aligned} \tag{5.10}$$

where the cost function of patching for host i, c_i is an increasing, convex function in β_i.

When the infection parameters $\lambda^{S,v}$ are known, the optimization problem (5.10) can be used to select an efficient mitigation strategy. In general, however, these parameters will be unknown. One approach to incorporating unknown infection rates is through robust variations on (5.10), which would select the minimum-cost mitigation strategy over a set of possible mitigation strategies. Alternatively, an adaptive approach can be designed that dynamically adjusts the patching rate based on previously observed infections. Developing such an approach is the focus of the next section.

5.4 Patching-Based Adaptive Mitigation

This section presents two adaptive strategies for tuning the patching rate based on previous detections of infected hosts. The convergence of the patching rate and infection probability are analyzed for both rules.

5.4.1 Adaptive Patching Strategy

As in the previous section, we take a passivity-based approach to designing the patching strategy; the approach, however, is based on an equivalent representation of the malware propagation dynamics with different input and output. We define the probability that host i is infected with at least one malware at time t as $\bar{x}_i(t)$ and the probability that host i is infected with virus v as $\bar{x}_i^v = \sum_{S \ni v} x_i^S$. We use the state dynamics of $\overline{x}_i = \sum_S x_i^S$ under the independence assumption derived in Theorem 5.1 as

$$\dot{\overline{x}}_i = (1 - \overline{x}_i) \sum_{j \in N_i} \sum_{v \in V} \lambda^{\emptyset, v} \, \overline{x}_j^v - \beta_i \overline{x}_i.$$

Proposition 5.2. *The dynamics of $\overline{x}_i$ are passive from input $\mathbf{u}$ where $u_i = (|N_i|\hat{\lambda} - \beta_i)$ to output $\mathbf{y}$ where $y_i = (\overline{x}_i)^2$.*

Proof: Define the storage function $W(\mathbf{x}) = \frac{1}{2} \sum_{i \in N} (\overline{x}_i)^2$ and $\hat{\lambda} = \sum_{v \in V} \lambda^{\emptyset, v}$. Differentiating with respect to time gives

$$\begin{aligned}
\dot{W}(\mathbf{x}) &= \sum_{i \in N} \overline{x}_i (1 - \overline{x}_i) \sum_{v \in V} \sum_{j \in N_i} \lambda^{\emptyset, v} \, \overline{x}_j^v - \sum_{i \in N} \beta_i (t) (\overline{x}_i)^2 \\
&\leq \sum_{i \in N} \overline{x}_i (1 - \overline{x}_i) \sum_{j \in N_i} \hat{\lambda} \overline{x}_j - \sum_{i \in N} \beta_i (\overline{x}_i)^2 \\
&\leq \sum_{i \in N} \sum_{j \in N_i} \hat{\lambda} \overline{x}_i \overline{x}_j - \sum_{i \in N} \beta_i (\overline{x}_i)^2 \\
&\leq \sum_{(i,j) \in E} \frac{\hat{\lambda}}{2} ((\overline{x}_i)^2 + (\overline{x}_j)^2 - \sum_{i \in N} \beta_i (\overline{x}_i)^2 \\
&= \sum_{i \in N} (|N_i| \hat{\lambda} - \beta_i) (\overline{x}_i)^2,
\end{aligned}$$

Thus proving passivity. ■

The passivity of the propagation dynamics implies that, in order to ensure convergence to the state where all viruses are removed, it suffices to select an update rule $\dot{\beta}_i(t)$ that is passive from input $(\overline{x}_i)^2$ to output $(|N_i|\hat{\lambda} - \beta_i)$ by Theorem 2.2. One such adaptive rule is given by

$$\dot{\beta}_i(t) = \alpha \overline{x}_i, \tag{5.11}$$

for some $\alpha > 0$. This patching strategy can be implemented by incrementing the patching rate by $\frac{\alpha}{\beta_i(t)}$ when an infection is detected. This is because the rate of this patching update process is $\beta_i(t)\bar{x}_i(t)$ at time t, which leads to the rate of change in the patching rate being equal to $\frac{\alpha}{\beta_i(t)}\beta_i(t)\bar{x}_i(t) = \alpha x_i(t)$. The adaptive patching does not require the knowledge of the propagation rate λ^v, but requires that $\beta_i(0) > 0$.

Theorem 5.3. *Under the patching update rule* $\dot{\beta}_i(t) = \alpha\overline{x}_i(t)$, $\lim_{t\to\infty}\overline{x}_i(t) = 0$ *for all* $i \in N$, *implying that all malwares are removed asymptotically from the network.*

Proof: Let $\mathbf{x}$ be the vector enumerating $\bar{x}_i^v$ for all $i \in N$ and $v \in V$. The proof is via the LaSalle Invariance Principle (Theorem 2.3). Define the storage function $W(\mathbf{x}, \beta)$ by

$$W(\mathbf{x}, \boldsymbol{\beta}) = \frac{1}{2}\sum_{i\in N}(\overline{x}_i)^2 + \sum_{i\in N}\Gamma_i(\beta_i),$$

where

$$\Gamma_i(\beta_i) = \begin{cases} \frac{1}{2\alpha}(|N_i|\hat{\lambda} - \beta_i)^2, & \beta_i \le |N_i|\hat{\lambda} \\ 0, & \text{else.} \end{cases}$$

By inspection, W is positive semidefinite, and continuously differentiable, and therefore is a valid storage function. We now show that $\dot{W}(\mathbf{x}, \boldsymbol{\beta}) \le 0$. By Proposition 5.2,

$$\begin{aligned} \dot{W}(\mathbf{x}, \boldsymbol{\beta}) &\le \sum_{i\in N}(|N_i|\hat{\lambda} - \beta_i)(\overline{x}_i)^2 + \sum_{i\in N}\dot{\Gamma}_i(\beta_i) \\ &= \sum_{i\in N}\left[(|N_i|\hat{\lambda} - \beta_i)(\overline{x}_i^2 - \bar{x}_i)\right]. \end{aligned}$$

We show that each term of the inner summation is bounded above by zero. If $\beta_i \le |N_i|\hat{\lambda}$, then, the corresponding term is given by

$$(|N_i|\hat{\lambda} - \beta_i)((\overline{x}_i)^2 - \overline{x}_i) \le 0,$$

since $(\overline{x}_i)^2 \le \overline{x}_i$ for $\overline{x}_i^v \in [0, 1]$. On the other hand, if $\beta_i > |N_i|\hat{\lambda}$, then the corresponding term is simply $(|N_i|\hat{\lambda} - \beta_i)(\overline{x}_i)^2 \le 0$.

By the LaSalle's Invariance Principle, all trajectories of $(\mathbf{x}, \boldsymbol{\beta})$ converge to $\{(\mathbf{x}, \boldsymbol{\beta}) : \dot{W}(\mathbf{x}, \boldsymbol{\beta}) = 0\}$. We show that this set is equal to $\{(\mathbf{x}, \boldsymbol{\beta}) : \mathbf{x} = 0\}$. Since

$$\dot{W}(\mathbf{x}, \boldsymbol{\beta}) = \sum_{i \in N} \overline{x}_i (1 - \overline{x}_i) \sum_{v \in V} \sum_{j \in N_i} \lambda^{\emptyset, v} \overline{x}_j^v - \sum_{i \in N} \beta_i(t) (\overline{x}_i)^2 + \sum_{i \in N} \dot{\Gamma}_i(\beta_i),$$

we have $\dot{W}(\mathbf{0}, \boldsymbol{\beta}) = \sum_{i \in N} \dot{\Gamma}_i(\beta_i)$. However $\dot{\Gamma}_i(\beta_i) = -(|N_i|\hat{\lambda} - \beta_i)\bar{x}_i$ for $\beta_i < |N_i|\hat{\lambda}$ and 0 for $\beta_i \geq |N_i|\hat{\lambda}$, resulting in $\dot{\Gamma}_i(\beta_i) = 0$ if $x_i = 0$. Moreover, suppose there exists $(\mathbf{x}, \boldsymbol{\beta})$ such that $\dot{W}(\mathbf{x}, (\beta)) = 0$ and $\bar{x}_i^v > 0$ for some i and v. Since $\bar{x}_i \geq x_i^v > 0$, we have $\dot{\beta}_i = \alpha \bar{x}_i > 0$. Thus β_i will increase at $(\mathbf{x}, \boldsymbol{\beta})$, and hence such $(\mathbf{x}, \boldsymbol{\beta})$ cannot stay in the set where $\dot{W} = 0$. Therefore, $\dot{W}(\mathbf{x}, \boldsymbol{\beta})$ is identically 0 if and only if $\mathbf{x} = 0$.

■

5.4.2 Analysis of Adaptive Patching Rate

We now analyze the time required for the adaptive patching rate to converge to $\beta_i(t) = |N_i|\hat{\lambda}$. As an approximation, we assume that the malware propagation $\overline{x}_i^v(t)$ instantaneously converges to a fixed point, denoted $s_i^v(\beta)$, and that $\overline{x}_i^v$ instantaneously converges to fixed point s_i. The reasoning behind this assumption is that when the patching update parameter α is small, then the dynamics of patching and filtering update will be on a much slower timescale than the timescale of the malware propagation. This assumption is made in the adaptive control literature [6] for the tractability of analysis. Under this assumption, we have $\dot{\beta}_i(t) = \alpha \sum_{v \in V} s_i^v(\beta)$. In order to bound the convergence rate, we derive a lower bound on s_i^v as follows. We have that $(1 - s_i) \sum_v \sum_{n_j \in N_i} \lambda^{\emptyset, v} s_j^v = \beta_i s_i$, and hence the union bound $\sum_v s_j^v \geq s_j$ implies that $(1 - s_i) \sum_{n_j \in N_i} \lambda_{min} s_j \leq \beta_i s_i$. Summing over i and rearranging terms yields

$$\begin{aligned} \sum_{i \in N} \lambda_{min} |N_i| s_i &\leq 2 \sum_{(i,j) \in E} \lambda_{min} s_i s_j + \sum_{i \in N} \beta_i s_i \\ &\leq \sum_{i \in N} |N_i| \lambda_{min} (s_i)^2 + \sum_{i \in N} \beta_i s_i. \end{aligned}$$

We then arrive at the lower bound

$$\sum_{i\in N} s_i(\lambda_{min}|N_i| - \beta_i - |N_i|\lambda_{min}s_i) \leq 0.$$

Based on this inequality, we take the approximation $s_i \geq \frac{|N_i|\lambda_{min}-\beta_i}{|N_i|\lambda_{min}}$, leading to the dynamics

$$\dot{\beta}_i(t) = \alpha \sum_{v\in V} s_i^v \geq \alpha \sum_{v\in V} \frac{1}{|N_i|\lambda_{min}}(|N_i|\lambda_{min} - \beta_i).$$

The resulting lower bound on $\beta_i(t)$ is then given by

$$\beta_i(t) \geq \frac{|V||N_i|}{\overline{\lambda}} + \left(\beta_i(0) - \frac{|V||N_i|}{\overline{\lambda}}\right) \exp\left(-\alpha \frac{|V|}{|N_i|\lambda_{\min}} t\right).$$

Next, we consider the final value of β_i that is reached after the infection rates converge to zero. The approach is to upper bound $\overline{x}_i(t)$, leading to an upper bound on $\dot{\beta}_i(t)$ and hence on $\beta_i(t)$. Since β_i is nondecreasing over time, we have

$$\dot{\overline{x}}_i(t) \leq \sum_{j\in N_i} \lambda_{max}(1-\overline{x}_i)\overline{x}_j - \beta_i\overline{x}_i \leq \lambda_{max} \sum_{j\in N_i} \overline{x}_j - \beta_i(0)\overline{x}_i,$$

which can be expressed in matrix form as $\dot{\overline{\mathbf{x}}}(t) = (\lambda_{max}A - B_0)\mathbf{x}(t)$ where A denotes the adjacency matrix of the network and B_0 is a diagonal matrix with $\beta_i(0)$ on the i-th diagonal entry. Hence

$$\dot{\overline{\mathbf{x}}}(t) \leq e^{(\lambda_{\max}A - B_0)t}\overline{\mathbf{x}}(t) \leq e^{(\lambda_{\max}A - B_0)t}\mathbf{1}.$$

Applying this bound gives

$$\begin{aligned}\sum_{i\in N} \dot{\beta}_i(t) &\leq \sum_{i\in N}\sum_{v\in V} \alpha e^{(\lambda_{\max}A - B_0)t}\mathbf{1} \\ &= \alpha \mathbf{1}^T e^{(\lambda_{\max}A - B_0)t}\mathbf{1} \leq \alpha|N|e^{\mu_1(\lambda_{\max}A - B_0)t},\end{aligned}$$

where $\mu_1(\lambda A - B_0)$ denotes the maximum eigenvalue of the matrix $(\lambda A - B_0)$. Integrating yields

$$\begin{aligned}&\sum_{i\in N} \beta_i(t) - \sum_{i\in N} \beta_i(0) \\ &\leq \frac{|N|\alpha}{|\mu_1(\lambda_{\max}A - B_0)|}(1 - \exp\left(-|\mu_1(\lambda_{\max}A - B_0)|t\right))\end{aligned}$$

giving a final value $\sum_{i\in N}\beta_i^* \leq \sum_{i\in N}\beta_i(0) + \frac{|N|\alpha}{|\mu_1(\lambda_{\max}A-B_0)|}$.

This bound depends on the value of $\beta_i(0)$, and is valid whenever $\beta_i(0) > \lambda_{max}|N_i|$. We therefore have

$$\sum_{i\in N}\beta_i^* \leq \min_{\epsilon_1,\ldots,\epsilon_N}\left\{\frac{|N|\alpha}{|\mu_1(\lambda_{\max}A-B_0)|} + \sum_{i\in N}(\lambda_{\max}|N_i| + \epsilon_i)\right\},$$

where $\epsilon_i = \beta_i(0) - \lambda_{\max}|N_i|$. We apply the Greshgorin Circle Theorem [32] to obtain a lower bound

$$|\mu_1(\lambda_{\max}A - B_0)| \geq \min\{\epsilon_i : i = 1,\ldots,n\}.$$

We have that

$$\sum_{i\in N}\beta_i^* \leq \min_{\epsilon}\left\{\frac{|N|\alpha}{\epsilon} + \lambda_{\max}|E| + |N|\epsilon\right\} = \lambda_{\max}|E| + 2|N|\sqrt{\alpha}.$$

This gives an average β_i^* value of approximately $\lambda_{\max}d_{avg} + 2\sqrt{\alpha}$, where d_{avg} is the average degree of the network.

5.4.3 Homogeneous Patching Strategy

This section presents the proposed adaptive patching strategy where the patching rate is dynamically updated based on previously detected infections. We characterize an equilibrium point of the propagation dynamics (7.8) and prove the global asymptotic convergence to the equilibrium point under the proposed adaptive patching strategy via passivity analysis.

Homogeneous Patching Update

Our proposed adaptive patching strategy is as follows. The patching rate applied to host i is dynamically updated based on detected infections of host i and its neighboring hosts $j \in N_i$. When an infection is detected at host i, the patching rate $\beta_i(t)$ is incremented by a factor of $\frac{\alpha}{\beta_i(t)}$. Similarly, if the inspection of node i reveals that no malware is present, then the patching rate is decremented by a factor of $\frac{\gamma}{\beta_i(t)}$.

Under the proposed patching update rule, the dynamics of the patching rate $\beta_i(t)$ is given as

$$\dot{\beta}_i(t) \quad = \quad \{\alpha x_i(t) - \gamma(1 - x_i(t))\}^+_{\beta_i}. \tag{5.12}$$

where $\{\cdot\}^+_{\beta_i}$ is the positive projection defined as

$$\{p(x)\}^+_{\beta_i} = \begin{cases} 0, & \beta_i = 0 \text{ and } p(x) < 0 \\ p(x), & \text{else} \end{cases}$$

We say the positive projection is active when $\beta_i = 0$ and $p(x) < 0$, and inactive otherwise. We will now characterize an equilibrium point of the joint dynamics of (7.8) and (5.12).

Theorem 5.4. *Let $x^* = \frac{\gamma}{\alpha+\gamma}$ and $\beta_i^* = \lambda d_i \frac{\alpha}{\alpha+\gamma}$. There exist two unique equilibria of the patching dynamics (5.12) with the propagation dynamics (7.8). The first equilibrium is (x_i^*, β_i^*) for all i, and the second equilibrium is $(x_i, \beta_i) = (0, 0)$ for all i.*

Proof. A necessary condition for $(\bar{\mathbf{x}}, \bar{\beta})$ to be an equilibrium is given as either $\bar{\beta}_i = 0$ and $\bar{x}_i < x^*$ for all i or $\bar{x}_i = x_i^*$, which is a condition to ensure $\dot{\beta}_i = 0$ for all i. Suppose $\bar{x}_i$ is a value in $0 < \bar{x}_i < x^*$, and $\bar{\beta}_i = 0$ Since $\bar{\mathbf{x}}$ is an equilibrium, the following equation is true.

$$\lambda(1 - \bar{x}_i) \sum_{j \in N_i} \bar{x}_j = 0. \tag{5.13}$$

Since $1 - \bar{x}_i > 0$, this condition implies that $\bar{x}_j = 0$ for all j. This in turn, implies that $\bar{x}_k = 0$ for all $k \in N_j$ since $\dot{x}_j = 0$. However since $i \in N_j$, this is a contradiction because $\bar{x}_i > 0$ from assumption. Therefore, $\bar{x}_i$ can either be 0 or $\bar{x}_i = x^*$ for all i.

Suppose that a host i has an equilibrium $\bar{x}_i = 0$. This implies that $\bar{x}_j = 0$ for all $j \in N_i$. Making the same argument for all neighbors of j inductively, we conclude that $\bar{\mathbf{x}} = \mathbf{0}$ for all hosts. Moreover, since $\beta_i(t)$ is a strictly decreasing function if $x_i = 0$, $\beta_i(t)$ will converge to 0 when the positive projection becomes active.

For the non-zero equilibrium (x_i^*, β_i^*), we verify by substituting x^* as x_i for all i and

$\beta_i = \beta_i^*$ in the propagation and patching dynamics. We obtain

$$\dot{x}_i(t) = \lambda(1 - x^*)d_i x^* - \beta_i^* x^* = 0$$
$$\dot{\beta}_i(t) = \{(\alpha + \gamma)\frac{\gamma}{\alpha + \gamma} - \gamma\}_{\beta_i}^+ = 0$$

for all i.

□

While (x^*, β^*) is an equilibrium point of the joint patching and propagation dynamics, this equilibrium point is not unique. The other equilibrium point is when $x_i = 0$ and $\beta_i = 0$ for all i. In what follows, we will prove that the proposed patching dynamics guarantee convergence to (x^*, β^*) when at least one host is initially infected with non-zero probability.

5.4.4 Passivity-Based Analysis of Homogeneous Patching

We prove convergence to (x^*, β^*) by formulating the joint propagation-defense dynamics as a negative feedback interconnection between the propagation dynamics and the adaptive patching rate update. We show that the propagation dynamics are strictly passive from input $-(\beta - \beta^*)$ to $(\mathbf{x} - \mathbf{x}^*)$. We then prove that the overall system dynamics converge to the equilibrium (x^*, β^*), guaranteeing the global asymptotic stability of the overall system as illustrated in Figure 7.1.

Lemma 5.3. *For all $x^* \in (0, 1)$, and for all $x_i, x_j \in (0, 1]$,*

$$(x_i - x^*)(\frac{x_j}{x_i} - x_j - 1 + x^*) + (x_j - x^*)(\frac{x_i}{x_j} - x_i - 1 + x^*) \leq 0$$

with equality achieved only when $x_i = x_j = x^*$.

Proof. Let $g(x_i, x_j) = (x_i - x^*)(\frac{x_j}{x_i} - x_j - 1 + x^*) + (x_j - x^*)(\frac{x_i}{x_j} - x_i - 1 + x^*)$. Expanding and rearranging $g(x_i, x_j)$ yields

$$g = -2x_i x_j + 2x^*(1 - x^* + x_i + x_j) - x^*(\frac{x_i}{x_j} + \frac{x_j}{x_i})$$

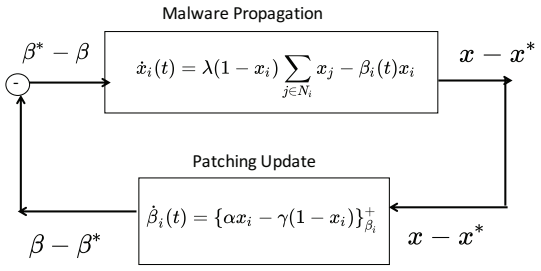


Figure 5.3: Figure illustrating passivity approach for proving convergence to the equilibrium $\mathbf{x}^*, \beta^*$. The malware propagation and patching dynamics are passive dynamical systems coupled by negative feedback interconnection.

Let $t = \frac{x_j}{x_i}$, then $g(x_i, x_j)$ can be rewritten as

$$g = 2x^*(1+t)x_i - x^*(t + \frac{1}{t}) - 2tx_i^2 + 2x^*(1 - x^*)$$

To derive the upper bound on $g(x_i, x_j)$, we will first maximize over x_i for a fixed t and then maximize over t. The upper bound obtained by this procedure will be an upper bound on

$$\max_{x_i, x_j \geq 0} g(x_i, x_j) \tag{5.14}$$

To see this, define $U(t) = \max\{g(x_i, tx_i) : x_i \geq 0\}$. Suppose that $(\bar{x}_i, \bar{x}_j)$ is the optimal solution to (5.14), and let $\bar{t} = \frac{\bar{x}_j}{\bar{x}_i}$. Then

$$U(\bar{t}) \geq g(\bar{x}_i, \bar{t}\bar{x}_i) = g(\bar{x}_i, \bar{x}_j),$$

and hence

$$\max_t U(t) \geq U(\bar{t}) \geq \max_{x_i, x_j \geq 0} g(x_i, x_j).$$

For any fixed t, $g(x_i, tx_i)$ is a concave function in x_i that is maximized when $x_i = \frac{1}{2}x^*(\frac{1}{t} + 1)$. Substituting this expression into the formula for g yields

$$g = x^* \left((t + \frac{1}{t})(\frac{1}{2}x^* - 1) + 2 - x^* \right)$$

For $0 < x^* < 1$, the term $\frac{1}{2}x^* - 1 < 0$. Since $t + \frac{1}{t}$ is a strict convex function in t, g is a strict concave function in t. Therefore, the t at which the maximum is achieved is unique and the function is maximized when $t = 1$, i.e., when $x_i = x_j$. Therefore,

$$g \leq x^*(x^* - 2 + 2 - x^*) = 0$$

This completes the proof. □

Theorem 5.5. *The propagation dynamics is strictly passive from input* $-(\beta - \beta^*)$ *to* $(\mathbf{x} - \mathbf{x}^*)$.

Proof. Consider the storage function $V_1(\mathbf{x})$ as

$$V_1(\mathbf{x}) = \sum_i \left(x^* \log \frac{x^*}{x_i} + (x_i - x^*) \right) \tag{5.15}$$

This storage function is a convex function in $\mathbf{x}$ since the Hessian of V_1 is

$$\nabla^2_{\mathbf{x}} V_1 = diag(\frac{x^*}{x_i^2}) > 0 \tag{5.16}$$

Due to convexity, the global minimum of V_1 is achieved when $\nabla_{\mathbf{x}} V_1 = \mathbf{0}$. However, the gradient of V_1 is a vector whose ith entry is given as $1 - \frac{x^*}{x_i}$. Therefore, $V_1(\mathbf{x}) \geq 0$ which is equal to 0 only when $\mathbf{x} = \mathbf{x}^*$.

In addition, $\dot{V}_1$ is given as

$$\begin{aligned} \dot{V}_1 &= \sum_i (1 - \frac{x^*}{x_i}) \dot{x}_i \\ &= \sum_i (x_i - x^*) \left(\lambda (\frac{1}{x_i} - 1) \sum_{j \in N_i} x_j - \beta_i \right) \end{aligned}$$

By adding and subtracting β_i^* term inside the parenthesis, and rearranging the terms, we obtain

$$\dot{V}_1 = -\sum_i (x_i - x^*)(\beta_i - \beta_i^*) + \lambda \sum_i (x_i - x^*) \left((\frac{1}{x_i} - 1) \sum_{j \in N_i} x_j - (1 - x^*) d_i \right)$$

Therefore, in order to prove passivity, it suffices to prove that

$$\sum_i (x_i - x^*) \left((\frac{1}{x_i} - 1) \sum_{j \in N_i} x_j - (1 - x^*) d_i \right) < 0$$

This term can further be rewritten as

$$\sum_i (x_i - x^*) \left((\frac{1}{x_i} - 1) \sum_{j \in N_i} x_j - (1 - x^*) d_i \right) \tag{5.17}$$

$$= \sum_i (x_i - x^*) \left(\sum_{j \in N_i} (\frac{x_j}{x_i} - x_j - 1 + x^*) \right) \tag{5.18}$$

$$= \sum_{(i,j) \in \mathcal{E}} [(x_i - x^*)(\frac{x_j}{x_i} - x_j - 1 + x^*) \tag{5.19}$$

$$+ (x_j - x^*)(\frac{x_i}{x_j} - x_i - 1 + x^*)] \tag{5.20}$$

However, each term of (5.20) is less than 0 for all $(i,j) \in \mathcal{E}$ due to Lemma 5.3, implying that $\dot{V}_1 < -\sum_i (x_i - x_i^*)(\beta_i - \beta_i^*)$ and the system is passive. □

Theorem 5.5 establishes the passivity of the propagation dynamics. We will now prove the passivity of homogeneous patching dynamics.

Theorem 5.6. *The patching dynamics is passive from* $(\mathbf{x}(t) - \mathbf{x}^*)$ *to* $(\beta(t) - \beta^*)$.

Proof. We first show that

$$(\beta_i - \beta_i^*)\dot{\beta}_i \leq (\beta_i - \beta_i^*)((\alpha + \gamma)x_i - \gamma)$$

If the positive projection is inactive, then the inequality holds with equality. If the positive projection is active, then $\beta_i = 0$ and $\dot{\beta}_i = 0$. Therefore, the left hand side of the inequality is 0, and the right hand side is equal to $-\beta_i^*((\alpha + \gamma)x_i - \gamma)$ which is greater than or equal to 0 since $\beta_i^* > 0$ and $(\alpha + \gamma)x_i - \gamma < 0$ by the definition of positive projection.

Let the storage function V_2 be given as

$$V_2(\beta) = \frac{1}{2(\alpha + \gamma)} (\beta - \beta^*)^T (\beta - \beta^*) \tag{5.21}$$

which is a positive definite function which equals to 0 only when $\beta = \beta^*$. Moreover,

$$\begin{aligned} \dot{V}_2 &= \frac{1}{(\alpha + \gamma)} (\beta - \beta^*)^T \dot{\beta} \\ &\leq \frac{1}{(\alpha + \gamma)} (\beta - \beta^*)^T (\alpha + \gamma)(\mathbf{x} - \mathbf{x}^*) \\ &= (\beta - \beta^*)^T (\mathbf{x} - \mathbf{x}^*) \end{aligned}$$

and hence the passivity property is satisfied for the homogeneous patching dynamics. □

Theorems 5.5 and 5.6 show the passivity of both propagation 7.8 and patching dynamics 5.12. Using these results, we now show that $x_i(t)$ will converge to x^* for all i.

Theorem 5.7. *The probability of infection at time t, $x_i(t)$ will converge to $x^* = \frac{\gamma}{\alpha+\gamma}$ for all i. The patching rate $\beta_i(t)$ will converge to β_i^* for all t.*

Proof. Using the storage functions $V_1(\mathbf{x})$ and $V_2(\beta)$ from Theorems 5.5 and 5.6 respectively, we can construct a Lyapunov function $V(\mathbf{x}, \beta) = V_1(\mathbf{x}) + V_2(\beta)$, which is a positive definite function. Moreover,

$$\dot{V} = \sum_{(i,j)\in\mathcal{E}} g(x_i, x_j) \leq 0$$

where $g(x_i, x_j)$ is the function defined in Lemma 5.3. From Lemma 5.3, it was shown that $\sum_{(i,j)\in\mathcal{E}} g(x_i, x_j) = 0$ if and only if $x_i = x_j = x^*$ for all (i, j).

By LaSalle's theorem [40], the $\mathbf{x}(t)$ will converge to the largest positive invariant subset of

$$\{(\mathbf{x}, \beta) : \dot{V}(\mathbf{x}, \beta) = 0\} = \{(\mathbf{x}, \beta) : \mathbf{x} = x^*\mathbf{1}\}.$$

Let R denote this largest positive invariant subset. Suppose $(x^*\mathbf{1}, \beta) \in R$ and $\beta \neq \beta^*$. Let $\mathbf{x}(0) = x^*\mathbf{1}$ and $\beta(0) = \beta^*$. Since $\beta_i \neq \beta_i^*$ for some i, there exists $\delta > 0$ such that $\dot{x}_i(t) \neq 0$ for $t \in [0, \delta)$. Hence $\mathbf{x}(t) \neq x^*\mathbf{1}$ when t is in a neighborhood of 0, contradicting the assumption that R is a positive invariant subset of $\{(\mathbf{x}, \beta) : \mathbf{x} = x^*\mathbf{1}\}$. Thus $(\mathbf{x}, \beta)$ converges to $(x^*\mathbf{1}, \beta^*)$ from any initial state where $\mathbf{x}(0) \neq 0$. □

5.4.5 Heterogeneous Patching Strategy

In Section 5.4.3, we considered a homogeneous patching strategy where the same patching update rule is applied to every host in the network. However, different host may have varying costs for patching efforts as well as different impact on the overall system when

infected. Under this scenario, it is preferable to have a heterogeneous patching strategy where each host will be infected with different probability of infection at the equilibrium.

In this section, we introduce a heterogeneous patching strategy where the patching update rule can differ for each host. We characterize the equilibrium under this dynamics and prove local convergence using the linearized dynamics. In addition, we formulate an optimization problem to trade-off the patching effort and the impact of infection.

Heterogeneous Patching Update

In the heterogeneous patching update rule, the patching rate is updated based on previous infections as in the homogeneous case. However, the increment and decrement factors α_i and γ_i vary for each host. Similarly as in (5.12), the heterogeneous patching dynamics is given as

$$\dot{\beta}_i(t) = \{\alpha_i x_i(t) - \gamma_i(1 - x_i(t)\})^+_{\beta_i} \tag{5.22}$$

Theorem 5.8. *An equilibrium of heterogeneous patching dynamics together with the propagation dynamics (7.8) is given as*

$$x_i^* = \frac{\gamma_i}{\alpha_i + \gamma_i}, \quad \beta_i^* = \lambda(\frac{1}{x_i^*} - 1) \sum_{j \in N_i} x_j^* \text{ for all } i \tag{5.23}$$

Proof. The patching dynamics is at equilibrium when $x_i^* = \frac{\gamma_i}{\alpha_i + \gamma_i}$. Substituting x_i^* in the (7.8), we obtain

$$\dot{x}_i(t) = \lambda(1 - x_i^*) \sum_{j \in N_i} x_j^* - \beta_i(t) x_i^*$$

and $\dot{x}_i = 0$ when $\beta_i = \beta_i^*$. □

We will now prove the local convergence to the characterized equilibrium (x_i^*, β_i^*).

Theorem 5.9. *The equilibrium point (x_i^*, β_i^*) is asymptotically stable.*

Proof. Linearizing the propagation dynamics (7.8) around the equilibrium point (x_i^*, β_i^*), we obtain

$$\dot{\bar{\mathbf{x}}} = A\bar{\mathbf{x}} + B\bar{\beta} \tag{5.24}$$

where the diagonal entries of A are given as $A_{ii} = -\lambda \sum_{j \in N_i} x_j^* - \beta_i^*$. For $j \neq i$, A_{ij} is given as

$$A_{ij} = \begin{cases} \lambda(1 - x_i^*), & \text{if } j \in N_i \\ 0, & \text{else} \end{cases}$$

The B matrix is a diagonal matrix with $B_{ii} = -x_i^*$. Linearizing the patching dynamics (5.22) around the equilibrium point, we obtain

$$\dot{\bar{\beta}} = K\bar{\mathbf{x}} \tag{5.25}$$

where K is a diagonal matrix with $K_{ii} = \alpha_i + \gamma_i$.

Since all off-diagonal entries of A are positive, from [61], if there exists a diagonal matrix $\bar{D}$ such that $A^T\bar{D}$ has negative row sums for all rows, then there exists a positive diagonal matrix D such that $A^TD + DA$ is negative definite.

Let $\bar{D}$ be a diagonal matrix where $\bar{D}_{ii} = x_i^*$. Then the sum of ith row element of $A^T\bar{D}$ is given as

$$\begin{aligned} (A^T\bar{D}\mathbf{1})_i &= A_{ii}x_i^* + \sum_{j \in N_i} \lambda(1 - x_j^*)x_j^* \\ &= -\lambda \sum_{j \in N_i} x_j^* + \sum_{j \in N_i} \lambda(1 - x_j^*)x_j^* < 0 \end{aligned}$$

since $0 < 1 - x_j^* < 1$ for all j. Therefore, there exists a positive diagonal matrix D such that $A^TD + DA < 0$.

Define the Lyapunov function

$$V(\bar{\mathbf{x}}, \bar{\beta}) = \frac{1}{2}\bar{\mathbf{x}}^T D\bar{\mathbf{x}} + \frac{1}{2}\bar{\beta}^T(-B)DK^{-1}\bar{\beta}$$

which is a positive definite function since D is a positive diagonal matrix, and $-B, D, K^{-1}$ are all positive diagonal matrices. The time derivative of V is given as

$$\begin{aligned} \dot{V} &= \frac{1}{2}\bar{\mathbf{x}}^T(A^TD + DA)\bar{\mathbf{x}} + \bar{\beta}^T BD\bar{\mathbf{x}} \\ &\quad + \bar{\beta}^T(-B)DK^{-1}K\bar{\mathbf{x}} \\ &\leq \bar{\beta}^T BD\bar{\mathbf{x}} - \bar{\beta}^T(B)D\bar{\mathbf{x}} = 0 \end{aligned}$$

with equality only if $\bar{\mathbf{x}} = \mathbf{0}$. This proves that heterogeneous dynamics guarantees asymptotic convergence around the equilibrium (x_i^*, β_i^*). □

Given that the equilibrium is asymptotically stable for arbitrary values of $\alpha_i, \gamma_i > 0$, a defense strategy can be designed to choose the equilibrium x_i^* which minimizes the trade-off between the probability of infection and the patching cost.

The patching rate at the equilibrium β_i^* is not a convex function in $\mathbf{x}^*$. However, if we assume that $x_i^* \ll 1$ for all i then the patching rate β_i^* can be approximated as

$$\beta_i^* \approx \frac{\lambda \left(\sum_{j \in N_i} x_j^* \right)}{x_i^*}$$

which provides an upper bound of β_i^*. The optimization problem of minimizing a trade-off between the probability of infection and the patching cost at the equilibrium can be formulated as

$$\begin{array}{ll} \text{minimize} & \sum_i c_i x_i^* + \lambda \sum_i \sum_{j \in N_i} x_j^* (x_i^*)^{-1} \\ \text{s.t.} & x_i^* \in (0, 1] \end{array} \tag{5.26}$$

where $c_i > 0$ is a positive constant to trade-off the probability of infection at host i. The optimization problem (5.26) is is a geometric program [14], and hence can be solved efficiently using convex optimization algorithms for a large network. Note that the objective function of (5.26) includes parameter λ, which is assumed to be unknown. Hence, a nominal value or probability distribution over λ can be used in the objective function. While an inaccurate estimate of λ will lead to suboptimal values of x^*, it will not impact the convergence properties of the adaptive update rule.

Analysis of Convergence Rate

We now analyze the convergence of the adaptive patching dynamics in the case of heterogeneous infection probabilities. Our convergence analysis is based on the linearization around the equilibrium point (x^*, β^*). As a convergence rate metric, we investigate the eigenvalue of the Jacobian whose real part has the smallest eigenvalue.

In what follows, we assume that the value of $\gamma_i = \gamma$ for all nodes, for some $\gamma > 0$. This can be assumed without loss of generality because any desired x_i^* can still be achieved by varying the parameter α_i. Letting J denote the Jacobian, we first introduce the matrix decomposition

$$J = \left(\begin{array}{c|c} A & B \\ \hline C & 0 \end{array}\right),$$

where A and B are defined as in the proof of Theorem 5.9, and C is a diagonal matrix with $C_{ii} = \alpha_i + \gamma_i$. As a preliminary, we have the following lemma that relates the eigenvalues of J to the eigenvalues of A.

Lemma 5.4. *Let Λ denote the set of eigenvalues of A. The eigenvalues of the Jacobian J are given as*

$$\overline{\Lambda} = \left\{ \frac{\eta \pm \sqrt{\eta - 4\gamma}}{2} : \eta \in \Lambda \right\}. \tag{5.27}$$

Proof. The characteristic polynomial of J is given by

$$\Delta_J(\rho) = \det \begin{pmatrix} A - \rho I & B \\ C & -\rho I \end{pmatrix}.$$

The matrices C and $-\rho I$ commute, and hence the characteristic polynomial is equivalent to $\Delta_J(\rho) = \det((A - \rho I)(-\rho I) - BC)$. The product BC is equal to $-\gamma I$, and hence

$$\begin{aligned} \Delta_J(\rho) &= \det(-\rho A + \rho^2 I + \gamma I) = \rho^n \det(A - (\rho + \frac{\gamma}{\rho})I) \\ &= \rho^n \Delta_A(\rho + \frac{\gamma}{\rho}). \end{aligned}$$

Thus the eigenvalues of J at values of ρ where $\rho + \frac{\gamma}{\rho} = \eta$ for some eigenvalue η of A. Solving for ρ gives the desired result. □

We now derive bounds on the eigenvalues of A.

Lemma 5.5. *Let η be an eigenvalue of A. Then*

$$|\eta| \geq \frac{\lambda \min_i \{(x_i^*)^2\}}{\max_i x_i^*}.$$

Proof. Define a diagonal matrix D by $D_{ii} = x_i^*$. Then the matrix AD satisfies

$$(AD)_{ij} = \begin{cases} -\lambda x_i^* \sum_{l \in N_i} x_l^*, & i = j \\ \lambda(1 - x_i^*)x_j^*, & j \in N_i \\ 0, & \text{else} \end{cases}$$

By the Gershgorin Circle Theorem, the magnitudes of the eigenvalues of AD are bounded below by

$$\min_i \left\{ \lambda x_i^* \sum_{j \in N_i} x_j^* \right\} \geq \lambda \min_i (x_i^*)^2.$$

Furthermore, for any vector v, we have that

$$\begin{aligned} ||D^{-1}ADv||_2 &\leq ||D^{-1}||_2 ||ADv||_2 \leq \frac{1}{\max_i D_{ii}} ||AD||_2 ||v||_2 \\ &\leq \frac{1}{\max_i x_i^*} \lambda \min_i (x_i^*)^2 ||v||_2 \end{aligned}$$

Since $D^{-1}AD$ and A have the same eigenvalues, we have the desired result. □

We remark that, in the homogeneous case (all x_i^* values are equal), this bound reduces to $|\eta| \geq \lambda x_i^*$. Combining the results of Lemmas 5.4 and 5.5 yields the following.

Theorem 5.10. *The magnitudes of the real parts of the eigenvalues of J are bounded below by*

$$\rho^* = \frac{\eta^* - \sqrt{(\eta^*)^2 - 4\gamma}}{2}, \tag{5.28}$$

where $\eta^* = \lambda \min_i (x_i^*)^2 / \max_i x_i^*$. If γ satisfies $4\gamma > (\eta^*)^2$, then the magnitudes of the real parts are bounded below by $\eta^*/2$.

Proof. By Lemma 5.4, the eigenvalues of J are defined by Eq. (5.27). The eigenvalue with smallest real part occurs when $|\eta|$ is minimized. Substituting the bound η^* from Lemma 5.5 yields Eq. (5.28). □

From Theorem 5.10, we observe that convergence rate is increasing in γ and η^*. The value of η^*, in turn, is increasing in $\min_i x_i^*$, increasing in λ, and decreasing in $\max_i x_i^*$.

Hence the convergence rate is maximized when γ is chosen to be large, all nodes have the same infection probability, and a higher infection probability is permitted. This suggests a trade-off between achieving a low infection probability and maximizing the rate of malware removal.

5.5 Adaptive Packet Filtering-Based Mitigation

This section presents an adaptive rule for packet filtering-based mitigation. Under the rule, the probability of filtering each packet q is increased with each malware packet that is detected. We first formally define the adaptive filtering-based mitigation strategy, and then analyze the convergence rate and overhead. A joint analysis of patching and filtering-based mitigation is also presented.

5.5.1 Adaptive Filtering Strategy

The first step in developing the adaptive filtering strategy is to analyze the passivity of the propagation dynamics when the output is equal to the information available to the packet filtering defense, namely, the rate of packets exchanged between hosts i and j. These passivity properties are analyzed in the following proposition. As a preliminary, define $\overline{\lambda}^v = q\mu^v$.

Proposition 5.3. *The multi-virus propagation dynamics are passive from input* $((\lambda^v_{max} - \overline{\lambda}^v) : v \in V)$ *to output* $(y^v(t) : (i,j) \in E, v \in V)$*, where*

$$y^v(t) = \sum_{(i,j)\in E} \mu^v(\overline{x}^v_i(1-\overline{x}^v_j) + \overline{x}^v_j(1-\overline{x}^v_i))$$

and μ^v *is the rate at which malware* v *sends packets to neighboring nodes.*

Proof: Define a storage function by

$$W(\mathbf{x}) = \frac{1}{2}\sum_{i=1}^{n}\sum_{v\in V}(\overline{x}^v_i)^2.$$

We then have

$$\dot{W}(\mathbf{x}) \leq \sum_{v\in V}\sum_{i=1}^{n}\left[\overline{x}_i^v\left(\sum_{j\in N(i)}\lambda_{max}^v(1-\underline{x}_i^v)\overline{x}_j^v - \sum_{v\in S}\sum_{j\in N(i)}u_{ij}^{(1)}\mu^v x_i^S(1-\overline{x}_j^v)\right)\right],$$

where $\lambda_{max}^v = \max\{\lambda^{S,v} : v \notin S\}$. Furthermore, we have that

$$\sum_{w\in S}\mu^w x_i^S(1-\overline{x}_j^w) \geq \mu^v x_i^S(1-\overline{x}_j^v)$$

for any $v \in S$, and hence

$$\dot{W}(\mathbf{x}) \leq \sum_{v\in V}\sum_{(i,j)\in E}\lambda_{max}^v(\overline{x}_i^v\overline{x}_j^v(1-\overline{x}_i^v) + \overline{x}_i^v\overline{x}_j^v(1-\overline{x}_j^v)) - \sum_{v\in V}\sum_{(i,j)\in E}q\mu^v((\overline{x}_i^v)^2(1-\overline{x}_j^v) + (\overline{x}_j^v)^2(1-\overline{x}_i^v)).$$

Now, since $2\overline{x}_i^v\overline{x}_j^v \leq (\overline{x}_i^v)^2 + (\overline{x}_j^v)^2$, we have that

$$\dot{W}(\mathbf{x}) \leq \sum_{v\in V}\sum_{(i,j)\in E}(\lambda_{max}^v - \overline{\lambda}^v)\left((\overline{x}_i^v)^2(1-\overline{x}_j^v) + (\overline{x}_j^v)^2(1-\overline{x}_i^v)\right).$$

This completes the proof of passivity. ■

Proposition 5.3 implies that the propagation dynamics are passive from input $(\lambda - \overline{\lambda})$ to output y^v. We consider the filtering probability update rule

$$\dot{q}(t) = \gamma\left\{\sum_{(i,j)\in E}\sum_{v\in V}\mu^v(\overline{x}_i^v(1-\overline{x}_j^v) + \overline{x}_j^v(1-\overline{x}_i^v))\right\}_{q<1} \tag{5.29}$$

where $\{f(\mathbf{x})\}_{q<1} = f(\mathbf{x})$ if $q < 1$ and 0 otherwise. This update rule can be implemented by incrementing $q(t)$ by $\frac{\gamma}{q(t)}$ whenever a malware packet is detected, since $q(t)$ and γ are known parameters at each time t. To show that this update rule results in (5.29), we observe that the rate of the filtering update process is given as

$$q(t)\left(\sum_{(i,j)\in E}\sum_{v\in V}\mu^v(\overline{x}_i^v(1-\overline{x}_j^v) + \overline{x}_j^v(1-\overline{x}_i^v))\right).$$

Therefore, by the same logic as the derivation of (5.11), incrementing the filtering probability by $\frac{\gamma}{q}$ when $q < 1$ results in the dynamics (5.29), which does not require the knowledge of the propagation rate λ^v.

Theorem 5.11. *The update rule (5.29) guarantees convergence of* $\overline{x}_i^v$ *to* 0 *for all* $i \in N$ *and* $v \in V$.

Proof: Define a storage function $W(\mathbf{x}, q)$ by

$$W(\mathbf{x}, q) = \begin{cases} \frac{1}{2}\sum_{i\in N}\sum_{v\in V}(\overline{x}_i^v)^2 \\ +\frac{1}{2}(q-\bar{p})^2, & q < \bar{p} \\ \frac{1}{2}\sum_{i\in N}\sum_{v\in V}(\overline{x}_i^v)^2, & q \geq \bar{p}. \end{cases}$$

Then $\dot{W}(\mathbf{x}, q)$ is bounded by

$$\begin{aligned} &\dot{W}(\mathbf{x}, q) \\ &\leq \sum_{v\in V}\sum_{(i,j)\in E}\mu^v(p^v - q)((1-\overline{x}_i^v)(\overline{x}_j^v)^2 + (1-\overline{x}_j^v)(\overline{x}_i^v)^2) \\ &\quad + \sum_{v\in V}\sum_{(i,j)\in E}\mu^v(q - p^v)((1-\overline{x}_i^v)\overline{x}_j^v + (1-\overline{x}_j^v)\overline{x}_i^v) \\ &\quad - \sum_{i\in N}\sum_{v\in V}\beta_i(\overline{x}_i^v)^2 \leq -\sum_{i\in N}\sum_{v\in V}\beta_i(\overline{x}_i^v)^2 < 0 \end{aligned}$$

when $q < \bar{p}$ and $\dot{W}(\mathbf{x}, q) < 0$ when $q \geq \bar{p}$ as well. Hence, the function W is strictly decreasing and converges to the set $\{\dot{W} = 0\}$, which occurs exactly when $\overline{x}_i^v = 0$ for all $i \in N$ and $v \in V$. ■

5.5.2 Convergence Rate Analysis

The convergence rate of the filtering probability to a sufficiently large value will determine how quickly the network defense is able to mitigate the malware propagation. In order to analyze the convergence rate, we divide the time required for all viruses to be removed into two intervals. The first time interval is the time for $q(t)$ to increase until it approaches p_{max}^v; this can be interpreted as the time required to "learn" the correct filtering strategy. The

second time interval is the time required for all viruses to be removed after $q(t)$ has reached this threshold value.

For simplicity, we define $\underline{\beta} = \min_{i\in N} \beta_i$, $\bar{\beta} = \max_{i\in N} \beta_i$ and $\bar{p} = \max_{S,v} p^{S,v}$, $\underline{p} = \min_{S,v} p^{S,v}$. Similarly $\bar{p}^v = \max_S p^{S,v}$ and $\underline{p}^v = \min_S p^{S,v}$. We analyze the time required for $q(t)$ to approach $(p^v_{max} - \beta_i)$. Let $\{r^v_i(q) : i \in N, v \in V\}$ denote a fixed point of $\overline{x}^v_i$ when $q(t)$ is constant and equal to q; when q is small, there exists such a fixed point with $r^v_i > 0$ for all $i \in N$ and $v \in V$. In order to analyze the convergence rate of $q(t)$, we adopt an approximation where the dynamics of $\overline{x}^v_i$ converge instantaneously to r^v_i for all i and v.

Under this approximation, the dynamics of $q(t)$ are

$$\dot{q}(t) \qquad \approx \qquad \gamma\{\sum_{v\in V}\sum_{(i,j)\in E} \mu^v \left((1 - r^v_i(q))r^v_j(q) \; + (1 - r^v_j(q))r^v_i(q)\right)\}_{q<1}. \quad (5.30)$$

A lower bound on the convergence time is described as follows.

Proposition 5.4. *The filtering probability $q(t)$ satisfies*

$$\dot{q}(t) \le \frac{\gamma|V|\bar{\beta}}{\underline{p} - q}\left(\min_{i\in N}|N_i| + \frac{(|N| - \min_{i\in N}|N_i|)\lambda_{max} - \underline{\beta}}{\mu_{min}(\underline{p} - q)}\right) \quad (5.31)$$

when $q(t) \le \underline{p}$.

Proof: We have that

$$\dot{q}(t) = \sum_{v\in V}\gamma\sum_{(i,j)\in E}\mu^v(r^v_i(1 - r^v_j) + r^v_j(1 - r^v_i)),$$

which can be bounded as

$$\begin{aligned}
\dot{q}(t) &= \sum_{v\in V}\left[\frac{\gamma}{\underline{p}^v - q}\sum_{(i,j)\in E}\mu_v(\underline{p}^v - q)(r^v_i(1 - r^v_j) + r^v_j(1 - r^v_i))\right] \\
&\le \sum_{v\in V}\left[\frac{\gamma}{\underline{p}^v - q}\sum_{(i,j)\in E}\left(\sum_{S:v\notin S} p^{S,v}\mu^v(r^S_i(1 - r^v_j) + r^S_j(1 - r^v_i))\right)\right] \\
&= \sum_{v\in V}\frac{\gamma}{\underline{p}^v - q}\sum_{i\in N}\beta_i r^v_i,
\end{aligned}$$

where (5.32) follows from the fact that r^v_i is a fixed point of the dynamics of $\overline{x}^v_i$.

Next, an upper bound on $\sum_{i\in N}\beta_i r_i^v$ is derived. At the fixed point,

$$\begin{aligned}\beta_i r_i^v &= \sum_{S:v\notin S}\sum_{n_j\in N(n_i)}\lambda^{S,v}r_i^S r_j^v - \sum_{S\ni v}\sum_{w\in S}\sum_{n_j\in N(n_i)} q\mu^w r_i^S(1-r_j^w)\\ &\le \lambda_{max}^v(1-r_i^v)r_j^v - \sum_{S\ni v}\sum_{w\in S}\sum_{n_j\in N(n_i)} q\mu^w r_i^S(1-r_j^w)\\ &\le (1-r_i^v)\lambda_{max}^v\sum_{n_j\in N(n_i)} r_j^v - q\mu^v r_i^v\sum_{n_j\in N(n_i)}(1-r_j^v)\end{aligned}$$

Rearranging terms yields

$$\begin{aligned}r_i^v &\le \frac{\lambda_{max}^v\sum_{n_j\in N(n_i)} r_j^v}{\beta_i+\lambda_{max}^v\sum_{n_j\in N(n_i)} r_j^v + q\mu^v\sum_{n_j\in N(n_i)}(1-r_j^v)}\\ &= \frac{\lambda_{max}^v\sum_{n_j\in N(n_i)} r_j^v}{\beta_i+(\lambda_{max}^v-q\mu^v)\sum_{n_j\in N(n_i)} r_j^v + q\mu^v d_i}\\ &\le \frac{\lambda_{max}^v\sum_{j\in N} r_j^v}{\beta_i+(\lambda_{max}^v-q\mu^v)\sum_{j\in N} r_j^v + q\mu^v d_i}\end{aligned}$$

Summing over i then gives

$$\sum_{i\in N} r_i^v \le \frac{n\lambda_{max}^v-(\underline{\beta}+q\mu^v d_{min})}{\lambda_{max}^v-q\mu^v}.$$

Combining with (5.32), we have

$$\begin{aligned}\dot{q}(t) &\le \sum_{v\in V}\left[\frac{\gamma\bar{\beta}}{\underline{p}^v-q}\cdot\frac{n\lambda_{max}^v-(\underline{\beta}+q\mu^v d_{min})}{\mu^v\bar{p}^v-q\mu^v}\right]\\ &\le \sum_{v\in V}\left[\frac{\gamma\bar{\beta}}{\underline{p}^v-q}\cdot\frac{n\lambda_{max}^v-(\underline{\beta}+q\mu^v d_{min})}{\mu^v\underline{p}^v-q\mu^v}\right]\\ &\le \frac{\gamma\bar{\beta}m}{\underline{p}-q}\left(d_{min}+\frac{(n-d_{min})\lambda_{max}-\underline{\beta}}{\mu_{min}(\underline{p}-q)}\right),\end{aligned}$$

completing the proof. ■

The upper bound on $q(t)$ can be used to analyze the time required for the filtering probability to converge to $\underline{p}$.

Lemma 5.6. *If $\underline{p}\ll 1$, then the time required for the filtering probability $q(t)$ to equal $\underline{p}$ is bounded below by*

$$\frac{\underline{p}^3\min_{v\in V}\mu^v}{3\gamma\bar{\beta}|V|((|N|-\min_{i\in N}|N_i|)\lambda_{max}-\underline{\beta})}.$$

We briefly remark on the tightness of the bound for a special case. Consider a network with a complete graph topology and a single propagating virus, in which all nodes have an identical patching rate β. At the equilibrium r_i, we have

$$\beta \sum_i r_i = (p-q)\mu \sum_{(i,j)} [r_i(1-r_j) + r_j(1-r_i)].$$

By symmetry, there exists r such that $r_i = r$ for all $i \in N$. Hence the approximation (5.30) is equivalent to $\dot{q}(t) = \frac{\beta\gamma|N|r}{p-q}$. By symmetry, we have

$$r = \frac{(p-q)(|N|-1)\mu - \beta}{(p-q)(|N|-1)\mu},$$

which implies that

$$\dot{q}(t) \geq \gamma \frac{|N|\beta}{p} \left(\frac{\mu(|N|-1)p - \beta}{\mu(|N|-1)} - q \right).$$

This bound agrees exactly with (5.31).

5.5.3 Final Value of Filtering Probability

The filtering probability $q(t)$ is a monotone increasing function that is bounded above by 1, and hence converges to a value $q^* = \lim_{t\to\infty} q(t)$. If this final value is approximately equal to $\bar{p}$, then the network will filter just enough packets to ensure that all viruses are removed. On the other hand, if q^* is approximately equal to 1, then almost all packets (including non-malware packets) will be inspected, increasing the delays experienced by legitimate network traffic. In what follows, we analyze the value of q^* as a function of the parameters γ and β.

Proposition 5.5. *The final value of $q(t)$ satisfies*

$$q^* \leq \min \left\{ \bar{p} + |V|\gamma \sum_{i\in N} \frac{|N_i|}{\beta_i}, 1 \right\}. \tag{5.32}$$

Proof: By inspection of (5.29) and the fact that $(1-\overline{x}_i^v) \leq 1$, we have that

$$\dot{q}(t) \leq \gamma \left\{ \sum_{v \in V} \sum_{(i,j) \in E} (\overline{x}_i^v + \overline{x}_j^v) \right\}_{q<1} \tag{5.33}$$

$$= \gamma \left\{ \sum_{v \in V} \sum_{i \in N} |N_i| \overline{x}_i^v \right\}_{q<1} \tag{5.34}$$

$$\leq \gamma \left\{ \sum_{v \in V} \sum_{i \in N} |N_i| e^{-\beta_i t} \right\}, \tag{5.35}$$

where (5.35) follows from the upper bound $\overline{x}_i^v(t) \leq e^{-\beta_i t}$ when $q > \bar{p}$. This yields

$$q(t) \leq q(0) + \sum_{v \in V} \sum_{i \in N} \frac{|N_i|\gamma}{\beta_i} \left(1 - e^{-\beta_i t}\right).$$

The expression can be simplified by noting that $q(0) = \bar{p}$ and the inner summation of the second term has no dependence on v. The fact that $\dot{q}(t) = 0$ when $q = 1$ then implies (5.32). ■

The following Corollary shows that when both adaptive patching and filtering are employed, all malwares are removed independent of the initial values of $\beta_i(0), q(0)$ and update parameters α, γ as long as these parameters are positive.

Corollary 5.1. *Joint adaptive patching and filtering guarantee convergence of $\bar{x}_i = 0$ for all $i \in N$ for any $q(0) > 0$, and $\beta_i(0) > 0$.*

Proof: Define the dynamics of $\bar{x}_i$ with only adaptive patching as $\dot{\bar{x}}_i^{(p)}$ and the dynamics of joint adaptive patching and filtering as $\dot{\bar{x}}_i^{(p),(f)}$. Since

$$\dot{\bar{x}}_i^{(p),(f)} = \dot{\bar{x}}_i^{(p)} - \sum_{v \in V} q(t) \mu^v \bar{x}_i^v \sum_{j \in N_i} (1 - \bar{x}_j^v),$$

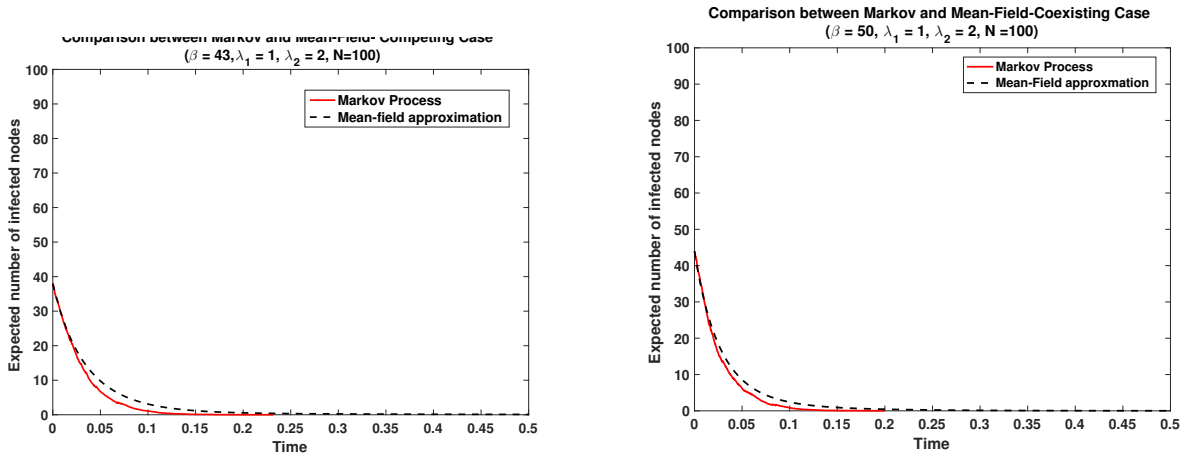
and $\sum_{v \in V} q(t) \mu^v \bar{x}_i^v \sum_{j \in N_i} (1 - \bar{x}_j^v) \geq 0$ for all $\bar{x}_i^v$ and $q(t) > 0$, we have $\dot{\bar{x}}_i^{(p),(f)} \leq \dot{\bar{x}}_i^{(p)}$. Since $q(t) > 0$ for all t for $q(0) > 0$ since $q(t)$ is a monotonic non-decreasing function in t. Therefore, for the same initial point $\bar{x}_i(0)$, the trajectory of $\bar{x}_i^{(p),(f)}(t)$ with joint patching and filtering will be upper bounded by the trajectory of $\bar{x}_i^{(p)}(t)$ with only filtering. However, Theorem 5.3 shows that under $\dot{x}_i^{(p)}$, $\bar{x}_i(t)$ will converge to 0 for all initial points $\bar{x}_i(0) \in [0, 1]$. Therefore, the joint adaptive patching and filtering guarantee convergence to $\bar{x}_i = 0$. ■

5.6 Numerical Study

In this section, we conduct a numerical study via Matlab. We conduct three numerical studies. First, we compare the mean-field approximation with the underlying Markov process by comparing the trajectories in the static patching case. Second, we simulate the adaptive patching strategy where the patching rate for host i is incrementally increased when the infection of host i is detected, as well as the adaptive filtering strategy jointly employed with static patching. Finally, we conduct a numerical study for the non-monotonic increasing adaptive patching strategy proposed in Section 5.4.3.

We assume there are two viruses v_1, v_2 propagating through the network, and the infection rates are given as $\lambda^{S,\{v_1\}} = \lambda_1 = 1$ and $\lambda^{S,\{v_2\}} = \lambda_2 = 2$ for all sets $S \subset \{v_1, v_2\}$ in the coexisting case, and the same infection rates are given as $\lambda^{\emptyset,v_1} = \lambda^{v_2,v_1} = 1$, $\lambda^{\emptyset,v_2} = \lambda^{v_1,v_2} = 2$ in the competing case. For the comparison between Markov process and mean-field approximation, we considered a Erdos-Renyi graph with 100 hosts and probability of connection $p = 0.2$. We assume that initially, each host is infected with either malware 1 or 2 with probability 0.4. To simulate the underlying Markov process, we used Monte-Carlo methods with 100 trials. Figure 5.4 validates that mean-field approximation provide good approximation of the underlying Markov chain for both the competing and coexisting cases. It also shows that mean-field approximation with independence assumption provides an upper bound on the trajectories of $\bar{x}_i(t)$ as proved in Theorem 5.1. Figure 5.4 also illustrates that when β values are chosen to satisfy the passivity index conditions shown in Theorem 5.2, it is sufficient to remove all malwares at desired rates.

The convergence of patching rates for the non-decreasing adaptive patching strategy for different α values are shown in Figure 5.5 (a) for both competing and coexisting cases. The network configuration is same as the static patching rate case, and the initial β values were set to 10 for all hosts. Figure 5.5 (b) validates the assumption of the instantaneous convergence to the fixed point in Section 5.4.2. The errors introduced by the instantaneous convergence assumption is negligible from the actual trajectory $\beta_i(t)$.



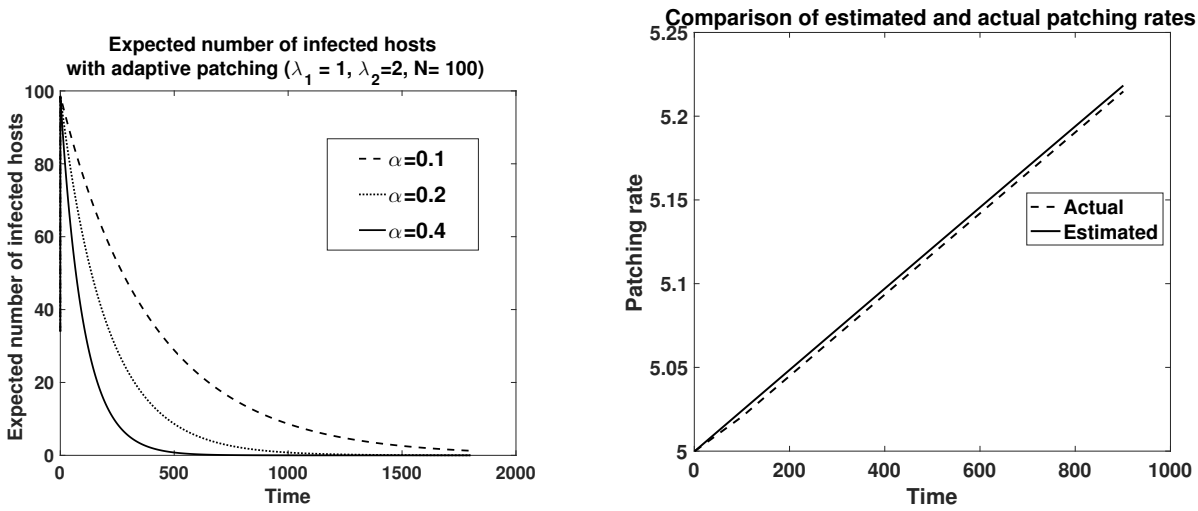
(a) (b)

Figure 5.4: Figure comparing the Markov process and the mean-field approximation with independence assumption. In both competing and coexisting cases, mean-field approximation provide good approximation while providing upper bounds on the trajectory of $\bar{x}_i(t)$ which is consistent with Theorem 5.1.

The effectiveness of the adaptive filtering strategy with static patching rate of $\beta_i = 10$ for all hosts are illustrated in Figure 5.6. Propagation rates λ_1, λ_2 are same as the static patching rate and the network was chosen to be a Erdos-Renyi random graph with $p = 0.2$. Initially, each host is infected with either virus 1 or 2 with probability 0.3. Figure 5.6 (a) shows that all malwares are eventually removed from the network. Smaller update parameter γ results in low final values of $q(t)$ (Figure 5.6 (b)) at the cost of longer time to remove all malwares.

Figure 5.6 (a) verifies that the adaptive patching strategy in Section 5.4.2 removes all malwares from the network. Large update parameter α ensures faster convergence to the desired steady state at the cost of higher final average patching rate at the equilibrium, resulting in unnecessarily high patching rates.

The non-monotone adaptive patching rule (Figure 5.6 (b)) was evaluated as follows. We considered propagation of a single virus in an Erdos-Renyi random graph with 100 hosts and $p = 0.05$. The propagation rate was $\lambda = 1$, while $\alpha = 1$ and $\gamma = 0.1$. For each host, the



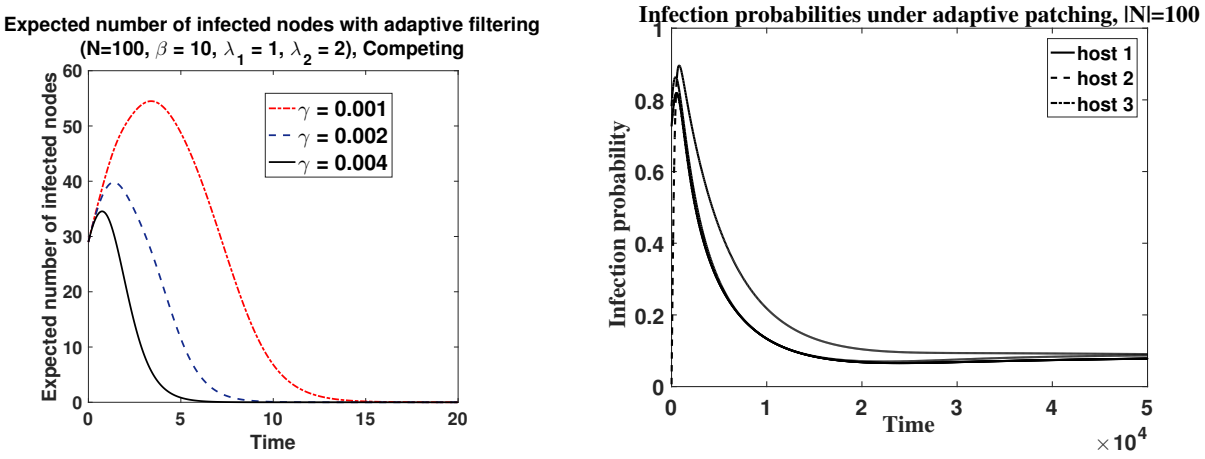
(a) (b)

Figure 5.5: (a): illustration of the effectiveness of adaptive patching strategy. Higher values of α ensures faster convergence rate to the final value at the cost of higher final patching rates at the equilibrium. (b) Comparison between the estimated patching rate with the instantaneous convergence assumption in Section 5.4.2 and the actual trajectory of β.

initial infection probabilities and patching rates were chosen independently and uniformly at random from $[0, 1]$ and $[0, 0.2]$, respectively. The trajectory of $x_i(t)$ for $i = 1, 2, 3$ is shown in Figure 5.6(b). Each of the three trajectories converges to the fixed point $\frac{\gamma}{\alpha+\gamma}$ from the initial state.

5.7 Conclusions and Future Work

In this chapter, we investigated static and adaptive mitigation strategies against propagation of multiple competing and coexisting malwares. We developed a passivity-based framework, and proved that patching and filtering-based defenses can be analyzed and designed jointly by modeling them as coupled dynamical systems. In the case where the malware propagation rates are known *a priori*, we characterized the needed patching rate as a passivity index of the dynamical model. We formulated the problem of selecting the minimum-cost mitigation strategy to remove all viruses at a desired rate by leveraging the derived passivity index.



(a) (b)

Figure 5.6: (a) Figure illustrating the effectiveness of adaptive filtering strategy. Adaptive filtering strategy is employed jointly with a static patching strategy with rate $\beta_i = 10$ for all hosts. Smaller values of γ results lower final values of q at the cost of higher peak number of infected hosts and longer time till all malwares are removed. (b) Effectiveness of non-monotone patching strategy. Probability of infection asymptotically converges to the equilibrium point computed in Theorem 5.4

When the propagation rates are not known *a priori*, we presented adaptive mitigation strategies that vary the rate of patching a host, or the probability of filtering a packet, in response to the observed malware infections. We developed two adaptive patching strategies, namely, a monotone increasing patching rate that guarantees removal of all viruses in steady-state, as well as a non-monotone patching rate that can approximate the propagation rate to any desired accuracy by varying the mitigation parameters. We also presented an adaptive packet filtering strategy for removing all viruses.

The adaptive update strategies presented in this chapter involve each host updating its own patching rate based on its observed infection probability. In future work, We will investigate generalizations to other propagation models, such as Susceptible-Infected-Recovered. Also, while we showed that joint adaptive patching and filtering remove all malwares, finding the optimal tradeoff between two mitigation strategies by tuning the update parameters is

an open research problem.

Chapter 6

PASSIVITY-BASED DISTRIBUTED STRATEGIES FOR PATROLLING GAMES

6.1 Introduction

Intelligent and persistent adversaries typically observe a targeted system and its security policies over a period of time, and then mount efficient attacks tailored to the weaknesses of the observed policies. These attacks have been analyzed within the framework of Stackelberg Security Games (SSG), where the defender (leader) selects a policy in order to maximize its utility under the best response strategy of the adversary (follower) [58, 52]. Applications of SSGs include defense of critical infrastructures [60, 68] and intrusion detection in computer networks [18]. In both of these applications, the security policy corresponds to defending a set of targets, including ports, checkpoints, or computer network nodes.

The security of the system targeted in an SSG can be further improved through randomized policies, in which the set of nodes or locations that are guarded varies over time with a probability distribution that is chosen by the defender [52, 60, 68, 35]. An attacker with knowledge of the probability distribution, but not the outcome of the randomized policy at each time step, will have greater uncertainty of the system state and reduced effectiveness of the attack.

Current work in SSGs focuses on centralized computation of the Stackelberg equilibria against different types of attackers, including rational, min-max, and bounded rational [35] attackers, under complete, incomplete, or uncertain information. In scenarios including patrolling and intrusion defense, however, security policies are implemented by distributed agents (e.g., multi-robot patrols, or malware filters in intrusion detection). These agents have limitations on computation, communication, and ability to move between targets. Currently,

however, computationally efficient distributed strategies for resource-constrained defenders to achieve the same Stackelberg equilibria as centralized mechanisms are lacking.

In this chapter, we develop distributed strategies for multiple defenders that guarantee convergence to a stochastic Stackelberg equilibrium distribution while minimizing the cost of movement. We propose a distributed strategy in which each defender first checks if a neighboring target is undefended, and then transitions to defending that with a certain probability if it is undefended. Since each defender only needs to know whether the neighboring targets are defended, the proposed policy can be implemented with only local communication. We analyze our approach by introducing nonlinear continuous dynamics, where each state variable is equal to the probability that a corresponding target is guarded by at least one defender, that approximate our proposed strategy. We show that, under this mapping, the Stackelberg equilibrium is achieved if and only if the continuous dynamics converge to a fixed point corresponding to the Stackelberg equilibrium. We develop sufficient conditions for convergence of these nonlinear dynamics via a passivity-based approach.

We derive bounds on the utility of an adversary with partial information as a function of the convergence rate of the dynamics, which we characterize as a passivity index. We then formulate the problem of maximizing the convergence rate, subject to mobility constraints, and prove that the formulation is convex, leading to efficient algorithms for computing the optimal policy. Our approach is validated and compared with an existing integer programming-based approach via numerical study.

The chapter is organized as follows. In Section 6.2, the defenders and attacker models are introduced, and a zero-sum game is formulated between multiple defenders and an attacker. In Section 6.3, we propose a distributed defender strategy and prove convergence to the desired Stackelberg equilibrium. Section 6.4 bounds the utility of the attacker using the convergence rate of the dynamics and presents a convex optimization approach for maximizing the convergence rate. Section 6.5 presents our simulation results. Section 6.6 concludes the chapter.

6.2 Model and Preliminaries

In this section, we present the defender and adversary models. We then formulate a Stackelberg game modeling the behavior of the adversary and defenders.

6.2.1 Defender Model

We assume that there are n targets and m defenders where $m \leq n$. The targets are represented as nodes on a complete graph, and each defender is located at one node in the graph at each time t. We model the constrained mobility of defenders and physical distances between nodes by assigning a cost d_{ij} of traversing from target i to target j. The cost of traversing may not be symmetric ($d_{ij} \neq d_{ji}$). Each defender is able to communicate with other defender to obtain information regarding whether any target is currently occupied by another defender. We define S_t to be the set of targets that is defended at time t.

6.2.2 Adversary Model

We consider an adversary whose goal is to successfully penetrate the system by attacking one or more targets over time. If the adversary attacks target i at time t, the adversary will collect the reward $r_i \geq 0$ if no defender is present at the target at time t. If at least one defender is present at target i at time t, the adversary will pay the cost $c_i \geq 0$. Both reward and cost values are known to the defenders and the adversary.

We consider two types of adversaries with different levels of available information. The first type of adversary is able to observe the fraction of time that a target is occupied by at least one defender for all targets but is unable to observe the current locations of defenders. The second type of adversary is able to observe exact location of one or more defenders at a sequence of times $t_1 < t_2 < \cdots < t_k$ and plan the attack strategy at time $t > t_k$ based on these observations.

6.2.3 Game Formulation

We consider a Stackelberg game where the defenders first choose the fraction of time that each target will be occupied by at least one defender. The adversary then observes the chosen fraction of time and decides to either attack a specific target, or not attack any target. The goal of the adversary is to maximize its expected utility, defined as the expected reward minus the expected cost of detection. The goal of the defender is to minimize the best-case expected utility of the adversary, leading to a zero-sum formulation.

To formally define the game, we denote x_i as the fraction of time that target i is occupied by at least one defender. If the adversary decides to attack target i, then the expected utility of attacking i, denoted $U_{adv}(i)$, is given as

$$U_{adv}(x_i) = (1 - x_i)r_i - x_i c_i = -(r_i + c_i)x_i + r_i \tag{6.1}$$

Let z_i be the adversary's chosen probability of attacking target i. Writing $\mathbf{x}$ and $\mathbf{z}$ as the vectors of defender and adversary probabilities, respectively, the expected utility of the adversary can be written as

$$U_{adv}(\mathbf{x}, \mathbf{z}) = -\mathbf{x}^T(C + R)\mathbf{z} + \mathbf{1}^T R\mathbf{z} \tag{6.2}$$

where C and R are $n \times n$ diagonal matrices with $C_{ii} = c_i$ and $R_{ii} = r_i$. Given $\mathbf{x}$, the adversary obtains the best-response strategy $\mathbf{z}$ by solving the linear program

$$\begin{aligned} &\text{maximize} \quad -\mathbf{x}^T(C + R)\mathbf{z} + \mathbf{1}^T R\mathbf{z} \\ &\mathbf{z} \\ &\text{s.t.} \qquad\quad \mathbf{1}^T\mathbf{z} \leq 1, 0 \leq z_i \leq 1,\ i = 1, \ldots, n \end{aligned} \tag{6.3}$$

We note that the adversary can maximize its utility by selecting $z_i = 1$ for some i satisfying

$$i \in \arg\max \{(\mathbf{x}^T(C + R) + \mathbf{1}^T R)_j : j = 1, \ldots, n\}$$

and $z_j = 0$ otherwise. Hence, without loss of generality we assume that the adversary selects a best-response strategy $\mathbf{z}^*$ with this structure, implying that the expected utility of the

adversary is given by

$$U^*_{adv}(\mathbf{x}) = \max\{\max_{i=1,\dots,n}\{-(r_i + c_i)x_i + r_i\}, 0\} \tag{6.4}$$

which is a piecewise linear function in $\mathbf{x}$.

The Stackelberg equilibrium $\mathbf{x}^*$ of the defender can then be obtained as the solution to the optimization problem

$$\begin{aligned} &\text{minimize} \quad U^*_{adv}(\mathbf{x}) \\ &\mathbf{x} \\ &\text{s.t.} \qquad \mathbf{1}^T\mathbf{x} \leq m, x_i \in [0,1] \end{aligned} \tag{6.5}$$

where the constraint $\mathbf{1}^T\mathbf{x} \leq m$ reflects the fact that there are m defenders. Eq. (6.5) is a piecewise linear optimization problem, and hence is convex. In the following section, we will discuss how to design the mobility patterns of defenders to achieve the computed $\mathbf{x}^*$ in a distributed manner.

6.3 Passivity-Based Distributed Defense Strategy

In this section, we present the proposed distributed patrolling strategy of the defenders. We define continuous dynamics that approximate the probability that each target is defended at time t, and show that convergence of the continuous dynamics to the distribution $\mathbf{x}^*$ is equivalent to convergence of the time-averaged defender positions to the Stackelberg equilibrium. We formulate sufficient conditions for convergence of the continuous dynamics via a passivity-based approach.

6.3.1 Distributed Defender Strategy

Our proposed distributed patrolling strategy is as follows. Each defender decides whether to move to a different target according to an i.i.d. Poisson process with rate γ. At time t, the defender at target i selects a target $j \neq i$ uniformly at random and sends a query message to determine if there is already a defender at target j. If so, then the defender remains at target i. If not, the defender moves to target j with probability p_{ij}.

This defender strategy can be modeled via nonlinear continuous dynamics. Let $x_i(t)$ denote the probability that at least one defender guards target i at time t. For $\delta > 0$ sufficiently small, we then have

$$x_i(t+\delta) = x_i(t) + (1 - x_i(t)) \sum_{j \neq i} \gamma \delta p_{ji} x_j(t) - \sum_{j \neq i} \gamma \delta p_{ij} x_i(t)(1 - x_j(t)).$$

This approximation makes the simplifying assumption that the events $i \in S_t$ and $j \notin S_t$ are independent for $i \neq j$. Dividing by δ and taking the limit as $\delta \to 0$ yields

$$\dot{x}_i(t) = (1 - x_i(t)) \sum_{j \neq i} Q_{ji} x_j(t) - x_i(t) \sum_{j \neq i} Q_{ij}(1 - x_j(t)), \tag{6.6}$$

where $Q_{ij} = p_{ij}\gamma$. The following lemma establishes that under the dynamics (6.6), the number total expected number of defended targets is equal to m at each time step, and the probability that each target is defended is within the interval [0,1].

Lemma 6.1. *If $x_i(0) \in [0,1]$ for all i and $\mathbf{1}^T\mathbf{x}(0) = m$, then $x_i(t) \in [0,1]$ and $\mathbf{1}^T\mathbf{x}(t) = m$ for all $t \geq 0$.*

Proof. To show that $x_i(t) \in [0,1]$ for all $t \geq 0$ when $x_i(0) \in [0,1]$, let

$$t^* = \inf \{ t : x_i(t) \notin [0,1] \text{ for some } i \}.$$

By continuity, $x_i(t^*) \in \{0,1\}$ for some i and $x_j(t) \in [0,1]$ for all $j \neq i$. Suppose without loss of generality that $x_i(t^*) = 0$. Then

$$\dot{x}_i(t^*) = \sum_{j \neq i} Q_{ji} x_j(t) \geq 0,$$

implying that $x_i(t) \in [0,1]$ within a neighborhood of t^* and contradicting the definition of t^*. Hence $x_i(t) \in [0,1]$ for all i and $t \geq 0$.

Now, we have that

$$\begin{aligned} \mathbf{1}^T\dot{\mathbf{x}}(t) &= \sum_{i=1}^{n} \left[(1 - x_i(t)) \sum_{j \neq i} Q_{ji} x_j(t) - x_i(t) \sum_{j \neq i} Q_{ij}(1 - x_j(t)) \right] \\ &= \sum_{i=1}^{n} \left[\sum_{j \neq i} (Q_{ji} x_j(t) - Q_{ij} x_i(t)) + \sum_{j \neq i} (Q_{ij} x_i(t) x_j(t) - Q_{ji} x_i(t) x_j(t)) \right] = 0, \end{aligned}$$

implying that $\mathbf{1}^T\mathbf{x}(t)$ is constant. □

6.3.2 Passivity-Based Convergence Analysis

We now derive conditions on the matrix Q to ensure that, for any initial distribution $\mathbf{x}(0)$, the dynamics (6.6) satisfy $\lim_{t\to\infty} \mathbf{x}(t) = \mathbf{x}^*$. If this condition holds, then the time-averaged distribution satisfies $\frac{1}{T}\int_0^T \mathbf{x}(t)\, dt \to \mathbf{x}^*$, and hence the Stackelberg equilibrium is achieved.

By inspection of (6.6), convergence to $\mathbf{x}^*$ occurs only if

$$(1 - x_i^*) \sum_{j \neq i} Q_{ji} x_j^* = x_i^* \sum_{j \neq i} Q_{ij}(1 - x_j^*)$$

for all i. Defining D^* to be a diagonal matrix with $D^*_{ii} = x_i^*$, this necessary condition can be written in matrix form as

$$(D^*(Q - Q^T) + Q^T)\mathbf{x}^* = D^* Q \mathbf{1}. \tag{6.7}$$

In order to develop sufficient conditions for convergence to $\mathbf{x}^*$, we introduce a decomposition of the dynamics (6.6) into a negative feedback interconnection between two passive dynamical systems. Recall that a dynamical system Σ is *output feedback passive* if there exists a positive semidefinite function V such that

$$\dot{V}(t) \leq \rho y(t)^T y(t) + u(t)^T y(t) \tag{6.8}$$

for all input u and output y for all time t. If $\rho = 0$, then the system is called passive, and the system is called strictly passive if $\rho < 0$. The parameter ρ is defined as the output feedback passivity index of the system [40].

Define $\hat{\mathbf{x}}(t) = \mathbf{x}(t) - \mathbf{x}^*$, and let two input-output dynamical systems be given by

$$(\Sigma_1) \qquad \begin{cases} \dot{\hat{x}}_i(t) = -(R_{in}(i) + R_{out}(i))\hat{x}_i(t) + u_i^{(1)}(t) \\ y_i^{(1)}(t) = \hat{x}_i(t) \end{cases} \tag{6.9}$$

$$(\Sigma_2): \qquad \mathbf{y}^{(2)}(t) = -(D^*(Q - Q^T) + Q^T)\mathbf{u}^{(2)}(t) \tag{6.10}$$

where $R_{in}(i) = \sum_{j\in N(i)} Q_{ji} x_j(t)$ and $R_{out}(i) = \sum_{j\in N(i)} Q_{ij}(1 - x_i(t))$. By inspection, the trajectory of $\hat{x}_j(t)$ in the negative feedback interconnection between (Σ_1) and (Σ_2), shown in Figure 6.1, is equivalent to the trajectory of $\hat{x}_j(t)$ under the dynamics (6.6).

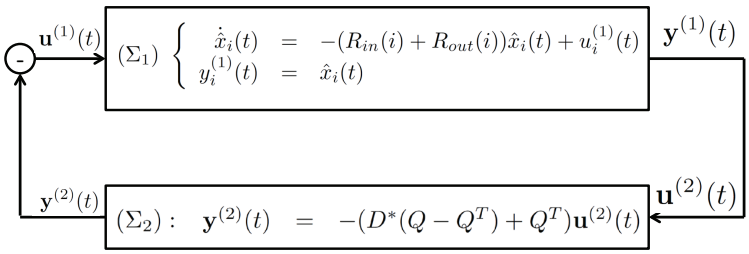


Figure 6.1: Decomposition of the patrol dynamics as negative feedback interconnection between passive systems.

The decomposition of Figure 6.1 can be interpreted as follows. The top block represents the change in the probability that each target i is defended, based on the current probability that target i is defended. The input signal from the bottom block can be interpreted as the rate at which defenders from other targets move to target i.

A standard result states that the negative feedback interconnection between two strictly passive systems is globally asymptotically stable [40], which in this case implies that $\mathbf{x}(t)$ converges asymptotically to $\mathbf{x}^*$. Hence, it suffices to derive conditions under which systems (Σ_1) and (Σ_2) are strictly passive. We now present sufficient conditions for strict passivity of (Σ_1) and (Σ_2), starting with (Σ_1).

Proposition 6.1. *The system* (Σ_1) *is passive from input* $\mathbf{u}^{(1)}(t)$ *to output* $\mathbf{y}^{(1)}(t)$.

If $\max_j \{\min\{Q_{ji}, Q_{ij}\}\} > 0$ *for all* i, *then* (Σ_1) *is strictly passive.*

Proof. Consider the storage function $V(\hat{\mathbf{x}}) = \frac{1}{2}\hat{\mathbf{x}}^T\hat{\mathbf{x}}$. We have

$$\dot{V}(\hat{\mathbf{x}}) = -\sum_i (R_{in}(i) + R_{out}(i))\hat{x}_i^2 + (\mathbf{u}^{(1)})^T\hat{\mathbf{x}}.$$

Since the output $\mathbf{y}^{(1)}$ is given by $\mathbf{y}^{(1)}(t) = \hat{\mathbf{x}}$, it suffices to show that $R_{in}(i) + R_{out}(i) > 0$ for all feasible $\mathbf{x}$. We have

$$R_{in}(i) + R_{out}(i) = \sum_i [Q_{ji}x_j + Q_{ij}(1 - x_j)]. \tag{6.11}$$

Since $x_j \in [0,1]$, each term of (6.11) is bounded below by $\min\{Q_{ji}, Q_{ij}\} \geq 0$. Hence the system (Σ_1) satisfies $\dot{V}(\hat{\mathbf{x}}) \leq (\mathbf{u}^{(1)})^T\mathbf{y}$, implying passivity. Furthermore, if the condition $\max_j \{\min\{Q_{ji}, Q_{ij}\}\} =: k > 0$ holds for all i, then

$$\dot{V}(\hat{\mathbf{x}}) < -k\hat{\mathbf{x}}^T\hat{\mathbf{x}} + (\mathbf{u}^{(1)})^T\mathbf{y},$$

implying strict passivity. □

The condition $\max_j \{\min\{Q_{ji}, Q_{ij}\}\} > 0$ implies that, for target i, there exists at least one target j such that defenders will transition to target i from target j, and vice versa, with positive probability.

For the system (Σ_2), define matrix $K = (D^*(Q - Q^T) + Q^T)$, so that $\mathbf{y}^{(2)} = -K\mathbf{u}^{(2)}$. If $-\mathbf{u}^T K\mathbf{u} \geq 0$ for all $\mathbf{u}$, then passivity of the bottom block would be guaranteed. On the other hand, since the diagonal entries of K are all 0, the matrix K is neither positive- nor negative-definite. The following proposition gives a weaker sufficient condition.

Proposition 6.2. *Define* $P = I - \frac{1}{n}\mathbf{1}\mathbf{1}^T$. *If* $PKP \leq 0$ *for all* $\mathbf{u}$, *then the system* (Σ_2) *satisfies* $\mathbf{u}^T\mathbf{y} \geq 0$ *for all* $\mathbf{u}$ *satisfying* $\mathbf{1}^T\mathbf{u} = 0$.

Proof. Suppose that $\mathbf{1}^T\mathbf{u} = 0$. Then $P\mathbf{u} = \mathbf{u}$, since P projects any vector onto the subspace orthogonal to $\mathbf{1}$, and hence $\mathbf{u}^T K\mathbf{u} = \mathbf{u}^T PKP\mathbf{u}$. The inequality $PKP \leq 0$ then implies that $\mathbf{u}^T\mathbf{y} = \mathbf{u}^T K\mathbf{u} \leq 0$. □

Combining the conditions for passivity of (Σ_1) and (Σ_2) with the fact that $\mathbf{1}^T\hat{\mathbf{x}}(t) = 0$ (Lemma 6.1) yields the following sufficient condition for convergence to the desired distribution $\mathbf{x}^*$.

Theorem 6.1. *If the conditions*

$$K\mathbf{x}^* = D^*Q\mathbf{1} \tag{6.12}$$

$$\max_j \{\min\{Q_{ji}, Q_{ij}\}\} > 0 \ \forall i \tag{6.13}$$

$$P^T\frac{K + K^T}{2}P \leq 0 \tag{6.14}$$

hold, then the vector of probabilities $\mathbf{x}(t)$ *converges to* $\mathbf{x}^*$ *as* $t \to \infty$. *There exists at least one realization of* Q *with* $Q_{ij} \geq 0$ *for all* $i \neq j$ *and* $Q_{ii} = 0$ *that satisfies (6.12)–(6.14).*

Proof. Condition (6.12) implies that the equilibrium of the dynamics (6.6) corresponds to the Stackelberg equilibrium $\mathbf{x}^*$. Conditions (6.13) and (6.14) establish strict passivity of (Σ_1) (Proposition 6.1) and passivity of (Σ_2) (Proposition 6.2), respectively, when the trajectory satisfies $\mathbf{1}^T\hat{\mathbf{x}}(t) = 0$ and $x_i(t) \in [0,1]$ for all i and t, which is guaranteed by Lemma 6.1. Hence the overall system is globally asymptotically stable with equilibrium $\mathbf{x}^*$. It remains to show that there is a feasible matrix Q that satisfies the conditions (6.12)–(6.14).

The proof constructs a matrix Q such that $\frac{K+K^T}{2} = \zeta(\frac{1}{n}\mathbf{1}\mathbf{1}^T - I)$ for some $\zeta \geq 0$. By construction, $\frac{1}{2}P(K+K^T)P = -\zeta P^3 \leq 0$, since $P \geq 0$.

For this choice of $\frac{K+K^T}{2}$, the identities $\frac{K+K^T}{2} = \zeta(\frac{1}{n}\mathbf{1}\mathbf{1}^T - I)$ and $K\mathbf{x}^* = D^*Q\mathbf{1}$ are equivalent to

$$\begin{aligned} x_i^*Q_{ij} + (1-x_j^*)Q_{ij} + x_j^*Q_{ji} + (1-x_i^*)Q_{ji} &= \zeta \ \forall i \neq j & (6.15)\\ \sum_j x_i^*(1-x_j^*)Q_{ij} &= \sum_j x_j^*(1-x_i^*)Q_{ji} \ \forall i & (6.16) \end{aligned}$$

Define

$$\tau_{ij} = \frac{1}{1-x_j^*} + \frac{1}{x_i^*} + \frac{1}{1-x_i^*} + \frac{1}{x_j^*},$$

and let $Q_{ij} = \frac{\zeta}{\tau_{ij}x_i^*(1-x_j^*)}$. Substitution of Q_{ij} and Q_{ji} into (6.15) yields

$$\frac{x_i^*\zeta}{\tau_{ij}x_i^*(1-x_j^*)} + \frac{(1-x_j^*)\zeta}{\tau_{ij}x_i^*(1-x_j^*)} + \frac{x_j^*\zeta}{\tau_{ij}x_j^*(1-x_i^*)} + \frac{(1-x_i^*)\zeta}{\tau_{ij}x_j^*(1-x_i^*)} = \zeta,$$

implying that (6.15) holds. Furthermore,

$$x_i^*(1-x_j^*)Q_{ij} = \frac{\gamma}{\tau_{ij}}x_j^*(1-x_i^*)Q_{ji},$$

and hence (6.16) holds as well.

Observe that under this choice of Q, $Q_{ij} \geq 0$ for all i, j, and condition (6.13) is satisfied as well. □

While there may be multiple matrices Q satisfying conditions (6.12)–(6.14), and hence guaranteeing convergence to $\mathbf{x}^*$, the corresponding dynamics of each defender may lead to a high cost associated with moving between distant targets. The problem of selecting the values of Q that minimize the total movement can be formulated as

$$\begin{aligned} \text{minimize} \quad & \textstyle\sum_{i=1}^{n}\sum_{j=1}^{n} d_{ij}Q_{ij}x_i^*(1-x_j^*) \\ Q, K & \\ \text{s.t.} \quad & K = D^*(Q-Q^T)+Q^T \\ & P(K+K^T)P \leq 0 \\ & K\mathbf{x}^* = D^*Q\mathbf{1} \\ & Q_{ij} \geq 0 \ \forall i \neq j, \ Q_{ii} = 0 \ \forall i \\ & \max_j \{\min\{Q_{ji}, Q_{ij}\}\} > 0 \ \forall i \end{aligned} \tag{6.17}$$

The objective function $\sum_{i=1}^{n}\sum_{j=1}^{n} d_{ij}Q_{ij}x_i^*(1-x_j^*)$ can be interpreted as the total movement cost to maintain the Stackelberg equilibrium $\mathbf{x}^*$ once the equilibrium is reached. Eq. (6.17) can be reformulated as a standard-form semidefinite program and solved in polynomial time. Furthermore, the procedure described in Theorem 6.1 can be used to construct a feasible solution to (6.17) in $O(n^2)$ time when the number of targets is large.

6.4 Mitigating Side Information of Adversary

In this section, we analyze the performance of our approach against an adversary with knowledge of the defender positions at a previous time period. We first bound the deviation between the utility of an adversary with partial information and the Stackelberg equilibrium utility. Our bound is a function of the convergence rate of the dynamics (6.6). We then formulate the problem of maximizing the convergence rate subject to mobility constraints, as well as the problem of selecting the least-costly patrolling strategy to achieve a desired convergence rate.

6.4.1 Deviation from Stackelberg Equilibrium

An adversary who observes the defender positions at time t' can estimate the probability $x_i(t)$ that target i is defended at time $t > t'$ via the dynamics (6.6). The adversary then computes the optimal strategy $\mathbf{z}(t)^*$, where $z_i(t)^*$ is the probability of attacking target i at time t, by solving the optimization problem $\max\{-\mathbf{x}(t)^T(C+R)\mathbf{z} + \mathbf{1}^T R\mathbf{z} : \mathbf{1}^T\mathbf{z} = 1, \mathbf{z} \geq 0\}$.

The deviation of the resulting utility from the Stackelberg equilibrium is given by

$$E(t) = \sum_j [z_j(t)^*(c_j x_j(t) + (1 - x_j(t))r_j) - z_j^*(x_j^* c_j + (1 - x_j^*)r_j)].$$

The following theorem provides an upper bound on $E(t)$ as a function of the convergence rate.

Theorem 6.2. *The expression $E(t)$ satisfies*

$$E(t) \leq 2\max_j \{|c_j||x_j(t) - x_j^*| + |r_j||x_j(t) - x_j^*|\} + \max_j |c_j - r_j| \sum_j |x_j(t) - x_j^*|. \quad (6.18)$$

Proof. Letting $\alpha_j(x_j(t)) = c_j x_j(t) + r_j(1 - x_j(t))$,

$$\begin{aligned} E(t) &= \sum_j [\alpha_j(x_j(t))(z_j(t)^* - z_j^* + z_j^*) - z_j^*\alpha_j(x_j^*)] \\ &= \sum_j [\alpha_j(x_j(t))(z_j(t)^* - z_j^*) + z_j^*(\alpha_j(x_j(t)) - \alpha_j(x_j^*))]. \quad (6.19) \end{aligned}$$

Considering the two terms of the inner summation in (6.19) separately, we first have that $\sum_j \alpha_j(x_j(t))(z_j(t)^* - z_j^*)$ is equal to $\alpha_j(x_j(t)) - \alpha_i(x_i(t))$, where j is the target attacked by the adversary in the best-response to distribution $\mathbf{x}(t)$ and i is the target attacked by the adversary in the best-response to $\mathbf{x}^*$. We then have

$$\begin{aligned} \alpha_j(x_j(t)) - \alpha_i(x_i(t)) &= c_j x_j(t) + r_j(1 - x_j(t)) - c_i x_i(t) - r_i(1 - x_i(t)) \\ &= c_j\hat{x}_j(t) - r_j\hat{x}_j(t) - c_i\hat{x}_i(t) + r_i\hat{x}_i(t) \\ &\quad + c_j x_j^* + r_j(1 - x_j^*) - c_i x_i^* - r_i(1 - x_i^*) \\ &\leq c_j\hat{x}_j(t) - r_j\hat{x}_j(t) - c_i\hat{x}_i(t) + r_i\hat{x}_i(t) \quad (6.20) \\ &\leq |c_j||x_j - x_j^*| + |r_j||x_j - x_j^*| \quad (6.21) \\ &\quad + |c_i||x_i - x_i^*| + |r_i||x_i - x_i^*| \end{aligned}$$

where (6.20) follows from the fact that i is a best-response to $\mathbf{x}^*$ and (6.21) follows from the triangle inequality. Taking an upper bound over i and j yields the first term of (6.18).

Now, consider the second term of $E(t)$. We have

$$\alpha_j(x_j(t)) - \alpha_j(x_j^*) = c_j x_j(t) + (1 - x_j(t))r_j - c_j x_j^* - r_j(1 - x_j^*) = (c_j - r_j)(x_j(t) - x_j^*).$$

Hence

$$\begin{aligned} \sum_j z_j^*(\alpha_j(x_j(t)) - \alpha(x_j^*)) &= \sum_j z_j^*(c_j - r_j)(x_j(t) - x_j^*) \\ &\leq \max_i |c_i - r_i| \sum_j |x_j(t) - x_j^*|, \end{aligned}$$

the second term of (6.18). □

Theorem 6.1 implies that the deviation between the optimal adversary utility at time t and the Stackelberg equilibrium is determined by the convergence rate. The convergence rate can be bounded via a Lyapunov-type argument. As a preliminary, we have the following standard result.

Proposition 6.3. *[40] Let $V(x)$ be a continuously differentiable function such that*

$$c_1||x||^a \leq V(x) \leq c_2||x||^a \tag{6.22}$$

$$\dot{V}(x) \leq -c_3||x||^a \tag{6.23}$$

over a domain $D \subset \mathbb{R}^n$. Suppose $\dot{x} = f(x)$ satisfies $f(0) = 0$. Then

$$||x(t)|| \leq \left(\frac{c_2}{c_1}\right)^{1/a} \exp\left(-\frac{c_3}{c_2 a}\right)||x(0)||.$$

A bound on the convergence rate can then be derived via the passivity analysis of Section 6.3.

Proposition 6.4. *Define $K_p = P^T(\frac{K+K^T}{2})P$, where $P = (I - \frac{1}{n}\mathbf{1}\mathbf{1}^T)$, and suppose that $K_p \leq 0$. Denote the eigenvalues of K_p as $0 \geq -\lambda_1 \geq \cdots \geq -\lambda_{n-1}$ and associated eigenvector of λ_i as q_i. Then, the deviation $||\mathbf{x}(t) - \mathbf{x}^*||_2$ satisfies*

$$||\mathbf{x}(t) - \mathbf{x}^*||_2 \leq \exp(-\lambda_1). \tag{6.24}$$

Proof. Let $V(\hat{\mathbf{x}}) = \frac{1}{2}\hat{\mathbf{x}}^T\hat{\mathbf{x}}$. In the notation of Proposition 6.3, we have $a = 2$ and $c_1 = c_2 = \frac{1}{2}$. We will bound $\dot{V}(\hat{\mathbf{x}})$ as a function of $||\hat{\mathbf{x}}||^2$. Any $\hat{\mathbf{x}}$ such that $\mathbf{1}^T\hat{\mathbf{x}} = 0$ satisfies $\hat{\mathbf{x}} = P\hat{\mathbf{x}}$. Then, from the passivity analysis in Proposition 6.1, we have

$$\dot{V}(\hat{\mathbf{x}}) \leq \hat{\mathbf{x}}^T K \hat{\mathbf{x}} = \hat{\mathbf{x}}^T P^T \frac{K + K^T}{2} P\hat{\mathbf{x}} = \hat{\mathbf{x}}^T K_p \hat{\mathbf{x}}$$

which can be upper bounded as

$$\begin{aligned}
\hat{\mathbf{x}}^T K_p \hat{\mathbf{x}} &\overset{(a)}{=} \sum_{i=1}^{n-1} -\lambda_i (\mathbf{q}_i^T \hat{\mathbf{x}})^2 \leq -\lambda_1 \sum_{i=1}^{n-1} \hat{\mathbf{x}}^T \mathbf{q}_i \mathbf{q}_i^T \hat{\mathbf{x}} \\
&\overset{(b)}{=} -\lambda_1 \sum_{i=1}^{n-1} \hat{\mathbf{x}}^T (I - \frac{1}{n}\mathbf{1}\mathbf{1}^T)\hat{\mathbf{x}} = -\lambda_1 \hat{\mathbf{x}}^T P \hat{\mathbf{x}} \\
&\overset{(c)}{=} -\lambda_1 \hat{\mathbf{x}}^T P^T P \hat{\mathbf{x}} = -\lambda_1 ||\hat{\mathbf{x}}||^2
\end{aligned}$$

where (a) is from eigen decomposition, (b) is from the orthogonality of eigenvectors for symmetric matrices, and (c) is from the idempotent property of the projection matrix. Substituting $-\lambda_1$ as c_3 from Proposition 6.3, we obtain the desired bound. □

The proof of Proposition 6.4 implies that $\dot{V}(\hat{\mathbf{x}}) \leq -\lambda_1 \hat{\mathbf{x}}^T \hat{\mathbf{x}}$, implying that λ_1 is a *passivity index* [40] for the system (Σ_1). Proposition 6.4 shows that maximizing over the convergence rate is equivalent to maximizing $|\lambda_1|$, which will be considered in the following section.

6.4.2 Optimizing the Convergence Rate

The problem of maximizing the convergence rate subject to the mobility constraint can be formulated as

$$
\begin{aligned}
&\text{maximize} \quad s \\
&Q, K, s \\
&\text{s.t.} \qquad\quad K = D^*(Q - Q^T) + Q^T \\
&\qquad\qquad\quad K\mathbf{x}^* = D^*Q\mathbf{1} \\
&\qquad\qquad\quad Q_{ij} \geq 0 \ \forall i \neq j, \ Q_{ii} = 0 \ \forall i \\
&\qquad\qquad\quad \textstyle\sum_{i=1}^{n} \sum_{j=1}^{n} d_{ij} Q_{ij} \leq d \\
&\qquad\qquad\quad \max_j \{\min\{Q_{ji}, Q_{ij}\}\} > 0 \ \forall i \\
&\qquad\qquad\quad P\left(\tfrac{K+K^T}{2}\right) P + sP \leq 0, s \geq 0
\end{aligned}
\tag{6.25}
$$

The first four constraints are from (6.17). The last constraint ensures the negative semi-definiteness of the matrix $P(K + K^T)P$ and maximization of $|\lambda_1|$, as shown in the following proposition.

Proposition 6.5. *Denote the eigenvalues of $P(K + K^T)P$ as $0, \lambda_1, \ldots, \lambda_{n-1}$ ordered such that $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{n-1}$, and let q_i denote the eigenvector associated with eigenvalue λ_i. If $P(K + K^T)P + sP \leq 0$, then $\lambda_1 \leq -s$.*

Proof. Let $K_P = P(K + K^T)P$. Then the matrix $K_P + sP$ can be rewritten as

$$K_P + sP = PK_PP + sPIP = P(K_P + sI)P \tag{6.26}$$

by the idempotent property of P. If $P(K_P + sI)P \leq 0$, then $\mathbf{x}^T P(K_P + sI)P\mathbf{x} \leq 0$ for all $\mathbf{x}$. Letting $\hat{\mathbf{x}} = P\mathbf{x}$, we have

$$\hat{\mathbf{x}}^T(K_P + sI)\hat{\mathbf{x}} \leq 0$$

for all $\hat{\mathbf{x}}$ that satisfies $\mathbf{1}^T\hat{\mathbf{x}} = 0$. In particular, choose $\hat{\mathbf{x}} = q_1$, which satisfies the condition $\mathbf{1}^T q_1$ from the orthogonality of eigenvectors of a symmetric matrix. Then $q_1^T(K_P + I)q_1 = \lambda_1 + s \leq 0$, and hence $\lambda_1 \leq -s$. □

By Proposition 6.5, the constraints $P(K + K^T)P + sP$ and $s \geq 0$ ensure the negative semidefiniteness of $P(K + K^T)P$ and maximizing s will result in $s^* = |\lambda_1|$. The formulated

optimization problem is a semidefinite program and can be solved efficiently in polynomial time as in the case of (6.17).

An alternative optimization is minimizing the patrol cost for a given convergence rate λ. This optimization problem can be formulated as

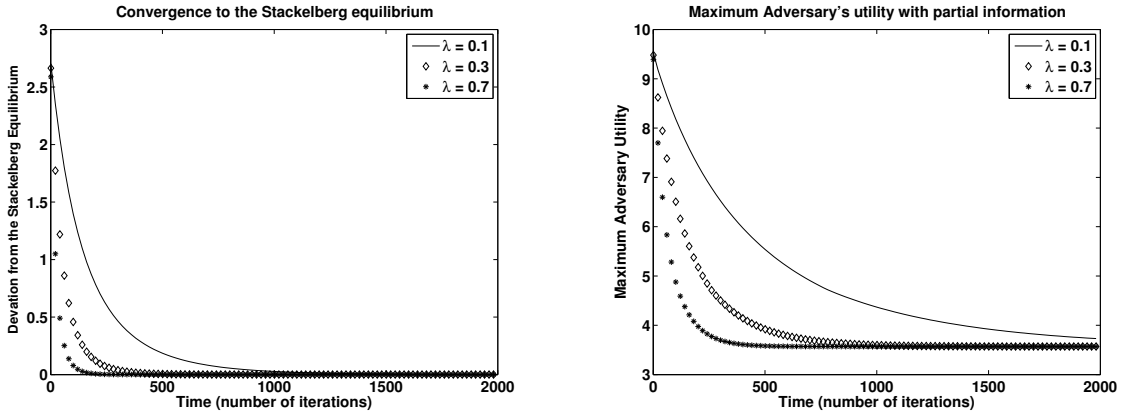
$$\begin{array}{ll} \text{minimize} & \sum_{i=1}^{n}\sum_{j=1}^{n} d_{ij}Q_{ij}x_i^*(1-x_j^*) \\ Q, K & \\ \text{s.t.} & K = D^*(Q-Q^T)+Q^T \\ & P\left(\frac{K+K^T}{2}\right)P + \lambda P \leq 0 \\ & K\mathbf{x}^* = D^*Q\mathbf{1} \\ & Q_{ij} \geq 0 \ \forall i \neq j, \ Q_{ii} = 0 \ \forall i \end{array} \tag{6.27}$$

which is also convex. This optimization problem is always feasible by the same argument given in Theorem 6.1, since given a $\lambda > 0$, one can set $\zeta = \lambda$ in the proof of Theorem 6.1 and construct a matrix Q that satisfies the constraint of (6.27). This optimization problem returns the least costly patrolling policy given a security constraint of achieving a desired convergence rate to the Stackelberg equilibrium.

6.5 Numerical Study

In this section, we conduct a numerical study via Matlab on a patrolling application. The formulated optimization problems were solved using cvx. We consider a network with 30 targets deployed uniformly at random in a square of size 10. The mobility cost d_{ij} was set as the Euclidean distance between target i and j. The number of defenders was set to 5. The diagonal reward and cost matrices R and C were randomly generated where the reward and cost values r_i and c_i were chosen uniformly in the interval $(0, 10)$.

We first obtained a Stackelberg equilibrium $\mathbf{x}^*$ by solving the convex optimization problem (6.5), and solved for Q for a set of convergence rates λ by solving the optimization problem (6.27) where the movement cost is minimized for a given convergence rate. The adversary's utility at the Stackelberg equilibrium was 3.56.



(a) (b)

Figure 6.2: (a) Figure illustrating the convergence of $\mathbf{x}(t)$ to $\mathbf{x}^*$. Metric for deviation from the Stackelberg equilibrium was $||\mathbf{x}(t) - \mathbf{x}^*||$ with Q matrices obtained with varying λ by solving optimization problem (6.27). (b) Maximum adversary's utility with information of the initial locations of defenders. The maximum utility of the adversary decays exponentially, with the maximum utility being the reward value of the target that is not covered by a defender initially.

Convergence of $\mathbf{x}(t)$ to the Stackelberg equilibrium $\mathbf{x}^*$ under the continuous dynamics (6.6) is shown in Figure 6.2(a). The initial positions were chosen at random among 30 targets. We observe that $\mathbf{x}(t)$ converges to $\mathbf{x}^*$ exponentially with differing convergence rates as shown in Proposition 6.4. Figure 6.2(b) shows the maximum utility of the adversary over time when the adversary observes the positions of defenders at time $t = 0$. The maximum utility of the adversary at time $t = 0$ is shown to be 9.5 which is the maximum reward value of targets that are not guarded by defender at time $t = 0$. Maximum adversary's utility converges to the defender's utility at Stackelberg equilibrium. The maximum utility of the adversary also decays exponentially with higher convergence rate of (6.6) offering faster decay of the adversary's utility as observed in Theorem 6.2.

Our proposed approach is compared with the integer programming-based technique, denoted Raptor, for centralized computation of patrol routes developed in [76] as shown in Figure 6.3. Each data point represents an average over 15 independent and random trials

with different cost and reward matrices, as well as target locations. The number of defenders was set to 3. For our approach, the minimum patrolling cost was obtained from the optimization problem (6.27), while the movement cost of Raptor is the minimum cost to transition between two sets of patroller locations sampled randomly with distribution $\mathbf{x}^*$. Our approach is able to achieve comparable mobility cost to Raptor with a convergence rate of $\lambda = 10^{-3}$. We observe that under our approach, as the number of targets increases, the minimum movement cost increases, with the rate of increase proportional to the convergence rate while Raptor's minimum patrolling cost stays relatively constant as the number of targets increase.

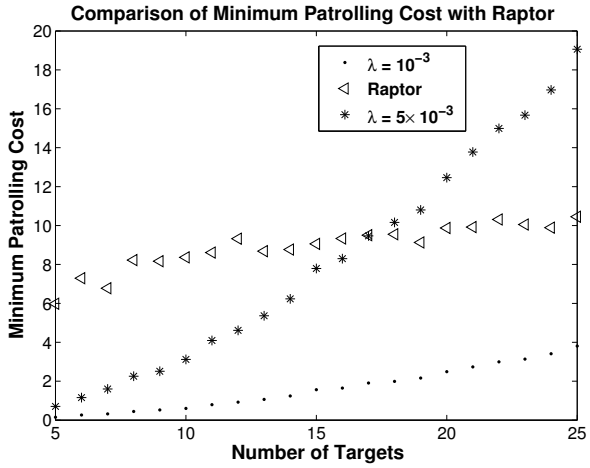


Figure 6.3: Minimum patrolling cost with different convergence rate λ and Raptor [76]. The number of defenders was set to 3. It is shown that our approach is able to achieve comparable mobility cost to Raptor with a convergence rate of $\lambda = 10^{-3}$. Under our approach, the minimum movement cost grows in a linear manner as the number of targets grows, and the slope of the line is proportional to the convergence rate λ. Raptor's minimum patrolling cost remains relatively constant as the number of targets grows.

6.6 Conclusions and Future Work

Stackelberg security games are a modeling framework for scenarios in which a defender chooses a randomized security policy, and an adversary observes the distribution of the

randomized policy and selects an attack accordingly. In this chapter, we developed a strategy for a team of defenders to implement a stochastic Stackelberg equilibrium security policy. Under our proposed strategy, each defender selects a target according to a precomputed probability distribution at each time step and moves to that target if the target is currently unoccupied. We formulated sufficient conditions, via a passivity-based approach, for a chosen probability distribution to guarantee convergence to the desired Stackelberg equilibrium.

We analyzed the behavior of an intelligent adversary who observes the previous positions of the set of defenders and selects an attack strategy based on these positions and the knowledge of the defender strategies. We proved that the additional impact of the attack provided by knowledge of the defender positions can be bounded as a function of the convergence rate of the defenders to the Stackelberg equilibrum. Under the passivity framework, this convergence rate is interpreted as a passivity index. We formulated the problem of selecting the minimum-cost (in terms of defender movement) strategy to achieve a desired convergence rate, as well as the problem of selecting the fastest-converging defender strategy under mobility constraint, as semidefinite programs, enabling efficient computation of the optimal patrols for each defender. Numerical results verified that both the deviation from the Stackelberg equilibrium and the adversary's utility decayed exponentially over time. The numerical study also suggested that the minimum patrolling cost increased linearly in the number of targets for a fixed number of defenders.

The approach presented in this chapter assumes a set of identical defenders that are capable of moving between any two targets within a desired time. A direction of future research is to generalize the approach to heterogeneous defenders who require multiple time steps to move between distant targets, reflecting a deployment over a wide geographical area. We will also extend the proposed approach to arbitrary topologies with mobility constraint of defenders and numerically evaluate the approach with real-world data including the transit network used in [76]. In addition, we will investigate incorporating Bayesian framework where both the defender and the adversary have prior distribution of each other's utility function and develop approximation algorithms to solve the Bayesian Stackelberg game.

Chapter 7

RESOURCE TAKEOVER GAME MODEL FOR ADVANCED PERSISTENT THREATS

7.1 Introduction

In a malware propagation attack, a malware process takes partial or complete control over a system, modifies the system's intended functionality, and attempts to infect other devices [28]. The potential impact of malware is especially severe in cyber-physical systems, which depend on real-time exchange of control information between cyber and physical components. As seen in the case of Stuxnet [46], malwares can cause significant physical damage by compromising the integrity and availability of this information exchange.

An increase in malware sophistication has been observed in recent years, adding to the security threats to cyber-physical systems [28, 85]. Two salient features have been observed in advanced malwares. The first feature is the malware's ability to mutate its code over time, known as polymorphic worms, enabling a malware to avoid signature-based intrusion detection while keeping its functionality intact [85]. The second feature is the competition among different malwares for control of targeted devices, in which a newly-installed malware detects and removes other malwares from the system [28]. The *persistent and adaptive nature* of malware creates a continuous, strategic interaction between the system owner and multiple competing malwares, which must be modeled and understood in order to develop effective mitigation strategies.

The FlipIt game was recently proposed in the security community to model defense against such advanced persistent threats [74]. In FlipIt, two players (attacker and defender) continuously compete for control of a host. The fraction of the time that each player controls the device, together with the resources expended to take over the device at different time

instances, quantify the effectiveness of the defense strategy and provide insight into the optimal system defense.

FlipIt provides a first step in modeling the interaction between the system owner and a persistent malware. Currently, however, there is no framework in which the system owner defends against an arbitrary number of malwares competing over a single resource. Furthermore, while existing literatures have analyzed the equilibrium behavior of the attacker and defender, there has been no study of the dynamic behavior of the players, who will update their strategies based on observation of the other player's strategies. In particular, identifying efficient and realistic strategies that can be implemented by the defender and multiple malwares, and guarantee convergence to the Nash equilibrium, is an open problem for FlipIt.

In this chapter, we develop a control-theoretic approach to modeling the strategies of adaptive, competing malware in FlipIt, as well as designing an optimal mitigation strategy. We consider the class of adversaries and defenders who adopt exponential takeover strategies, in which the host is compromised (by the adversary) or restored (by the defender) according to a Poisson process. The strategy is characterized by the takeover rate, and was identified as one of the key strategies in FlipIt [74] due to its ease of implementation and unpredictability to other players. Our approach is to model the takeover rate of the defender and each malware as a dynamical system, where the takeover rate of each player is a state variable that changes over time based on that player's current utility.

- We generalize the FlipIt game to include one defender and an arbitrary number of competing malwares, each of which employs an exponential strategy with a time-varying takeover rate. We then prove the existence and uniqueness of the Nash equilibrium, and present a closed form characterization of the equilibrium.

- We formulate a dynamical model for the takeover rate of each malware, in which the malware owner observes the sum of the takeover rates and updates its own takeover rate according to gradient ascent. We prove that the proposed dynamics guarantee convergence to the Nash equilibrium via passivity based analysis.

- We investigate the optimal mitigation strategy of the system. We model the mitigation as a Stackelberg game, and prove that the optimal mitigation strategy can be obtained as the solution to a convex optimization problem.

- We evaluate the convergence of malware strategies to the Nash equilibrium via a numerical study. We verify that the proposed dynamics ensure convergence to the Nash equilibrium, and characterize the utility of the system owner under different mitigation parameters.

The chapter is organized as follows. Section 7.2 contains our assumptions of the system and malwares, as well as background on FlipIt. Section 7.3 presents a host takeover game formulation for multiple malwares and characterizes the unique Nash equilibrium. We describe the dynamics of each player's strategy and prove convergence to the equilibrium in Section 7.4. In Section 7.5, we propose a polynomial time algorithm for computing the optimal mitigation strategy. Section 7.6 includes our numerical results. Section 7.7 concludes the chapter.

7.2 Model and Preliminaries

In this section, we present the adversary and system models, and give a formal definition of FlipIt [74].

7.2.1 Adversary Model

We consider multiple persistent malwares that compete to take control of a host. Once a malware infects the host, it removes any existing malware and installs an anti-virus software to detect attempted infections from other malwares. Each malware's signature is learned over time by both the owner of the host and other malwares. In order to avoid detection, each malware's author will change the malware's binaries to change its signature. The effort required for the author to change the binaries creates a cost associated with infecting the host for each malware.

7.2.2 System model

A system owner regularly inspects and cleans the targeted host from any potential infection from malwares. The owner inspects signatures of malwares that infected the host and patches exploited software vulnerabilities. In addition, the owner updates its anti-virus software to prevent any future infection from known malwares. We assume that during the cleaning process, the host will be taken offline, and will be unavailable for use. This creates a cost associated with cleaning the host.

7.2.3 FlipIt

FlipIt is a two-player game where attacker and defender are competing over a shared resource. Each player can make a *move* at any time. Once a player makes a move, the player owns the resource until the opponent makes a move. Each time player i makes a move, player i pays an associated cost $c_i > 0$. The number of moves made by player i up to time t is denoted as $n_i(t)$.

The utility of each player is defined as the average fraction of time the player owns the resource minus the average cost of takeover. Formally, the utility of player i is given as

$$U_i = \liminf_{t\to\infty} \frac{1}{t}\left(\int_0^t C_i(\tau)d\tau - c_i n_i(t)\right) \tag{7.1}$$

where $C_i(t) = 1$ if player i owns the resource at time t, and $C_i(t) = 0$ otherwise.

7.3 Game Formulation and Nash Equilibrium

In this section, we formally define the resource takeover game between multiple malwares, and prove the existence and uniqueness of the Nash equilibrium of the proposed game.

7.3.1 Game Formulation

We consider an $(n + 1)$-player resource takeover game between the system owner and n competing malwares. The system owner is indexed as player 0, while the n malwares are

indexed from 1 to n. Malware i has a cost per takeover denoted as c_i. Without loss of generality, we index the malwares based on the rank order of their respective costs c_i, such that $c_1 \leq c_2 \leq ... \leq c_n$. We denote $\{T_i(m)\}$ as the sequence of times that player i has taken over the resource.

In this chapter, we assume that all $n+1$ players employ exponential strategies. A takeover strategy is defined as exponential if the time differences between two consecutive takeovers, i.e., $\{T_i(m) - T_i(m-1)\}$ are independent, exponential random variables. The exponential strategy was proposed in [74] due to its unpredictability compared to deterministic periodic strategies.

We consider the case when the system owner sets its takeover rate x_0 and malwares play a noncooperative game to choose the takeover rates given a fixed x_0. We denote the rate of takeover for malware i as x_i. We say that a malware *drops out* of the game if its takeover rate $x_i = 0$ and say that a malware *participates* in the game if $x_i > 0$.

Theorem 7.1. *The utility of malware i when each malware employs an exponential strategy with rate x_i, and the owner employs an exponential strategy with rate x_0, is given as*

$$U_i(\mathbf{x}) = \frac{x_i}{\sum_{j=0}^{n} x_j} - c_i x_i. \tag{7.2}$$

The proof when two players can be found in [74]. The proof with multiple players follows from the fact that the minimum of independent exponential random variables with corresponding rates $x_1, \ldots, x_n$ is another exponential random variable with rate being $\sum_{i=1}^{n} x_i$. We can then group the set of adversaries into one adversary to characterize the utility function by using the same techniques in [74].

7.3.2 Characterization of the Nash Equilibrium

We define $\mathbf{x}_{-i} := \{x_j : j \neq i\}$. The Nash equilibrium (N.E.) is defined as $\bar{\mathbf{x}} = (\bar{x}_1, \ldots, \bar{x}_n) \in \mathbb{R}_+^n$ such that

$$U_i(\bar{x}_i, \bar{\mathbf{x}}_{-i}) \geq U_i(x_i, \bar{\mathbf{x}}_{-i}) \text{ for } i = 1, ..., n$$

for all $x_i \neq \bar{x}_i$, where $\bar{\mathbf{x}}_{-i} = \{\bar{x}_j : j \neq i\}$. The characterization of the Nash equilibrium is given in the following Theorem. To simplify notations, we denote $S_c(r) := \sum_{i=1}^{r} c_i$, and $f(x_0, r) := \sqrt{(r-1)^2 + 4x_0 S_c(r)}$ for $r \geq 1$ for the rest of the chapter.

Theorem 7.2. *For a given x_0, there exists a unique Nash equilibrium amongst n malwares. If c_1 satisfies the inequality $c_1 \geq \frac{1}{x_0}$, then $\bar{x}_i = 0$ for all malwares. If $c_1 < \frac{1}{x_0}$, then the unique Nash equilibrium is characterized as follows:*

If there exists a malware whose cost c_{m+1} satisfies

$$c_{m+1} \geq \frac{2S_c(m)}{m - 1 + f(x_0, m)} \tag{7.3}$$

then $\bar{x}_j = 0$ for all $j \geq m+1$. For malwares $i = 1, ..., m$, the N.E. is given as

$$\bar{x}_i = \frac{-x_0 c_i}{S_c(m)} + \frac{m - 1 + f(x_0, m)}{2(S_c(m))^2} \left(S_c(m) - (m-1)c_i\right). \tag{7.4}$$

Proof. In order to characterize the Nash equilibrium, we first compute the best response of malware i given the sum of the other players' takeover rates. It can be verified that $\frac{\partial^2 U_i}{\partial x_i^2} \leq 0$ for a given $\sum_{j \neq i} x_j$. Therefore, U_i is a concave function in x_i given $\sum_{j \neq i} x_j$, and the best response of malware i, denoted as BR_i, is given as the solution of $\frac{\partial U_i}{\partial x_i} = 0$ when $BR_i(\sum_{j \neq i} x_j) > 0$ and 0 otherwise. The best response of malware i can be explicitly written as

$$BR_i(\sum_{j \neq i} x_j) = \begin{cases} \sqrt{\frac{\sum_{j \neq i} x_j}{c_i}} - \sum_{j \neq i} x_j, & c_i < \frac{1}{\sum_{j \neq i} x_j} \\ 0, & \text{else} \end{cases} \tag{7.5}$$

To show that $\bar{x}_i$'s constitute a NE, it suffices to show that $BR_i(\sum_{j \neq i} \bar{x}_j) = \bar{x}_i$. Replacing for $\bar{x}_i$ from Theorem 7.2, we obtain

$$\bar{u}(x_0) := x_0 + \sum_{i=1}^{m} \bar{x}_i = \frac{m - 1 + f(x_0, m)}{2S_c(m)}. \tag{7.6}$$

Therefore, $BR_j(\bar{u}(x_0)) = 0$ for all malware j such that $c_j \geq \frac{1}{\bar{u}(x_0)}$. For the malwares indexed $i = 1, \ldots, m$, we need to show that

$$BR_i(x_0 + \sum_{j \neq i} \bar{x}_j) = \sqrt{\frac{\bar{u}(x_0) - \bar{x}_i}{c_i}} - (\bar{u}(x_0) - \bar{x}_i) = \bar{x}_i \tag{7.7}$$

which is equivalent to $\bar{x}_i = \bar{u}(x_0) - \bar{u}(x_0)^2 c_i$. Note that $\bar{u}^2(x_0)$ can be expressed as

$$\begin{aligned}\bar{u}^2(x_0) &= \frac{(m-1)^2 + (m-1)f(x_0,m) + 2x_0 S_c(m)}{2S_c(m)^2} \\ &= \bar{u}(x_0)\frac{m-1}{S_c(m)} + \frac{x_0}{S_c(m)}.\end{aligned}$$

Therefore,

$$\bar{u}(x_0) - \bar{u}(x_0)^2 c_i = -\frac{x_0 c_i}{S_c(m)} + \bar{u}(x_0)\frac{S_c(m) - (m-1)c_i}{S_c(m)}$$

which shows that $\bar{u}(x_0) - \bar{u}(x_0)^2 c_i = \bar{x}_i$ as given in (7.4) for all $i = 1, \ldots, m$.

Since any N.E. $\bar{\mathbf{x}}$ has to satisfy $\bar{u}(x_0) - \bar{u}(x_0)^2 c_i = \bar{x}_i$ for $i = 1, \ldots, m$, summing over $\bar{u}(x_0) - \bar{u}(x_0)^2 c_i = \bar{x}_i$ from $i = 1$ to m results in

$$S_c(m)\bar{u}(x_0)^2 - (m-1)\bar{u}(x_0) - x_0 = 0$$

which is a quadratic equation in $\bar{u}(x_0)$. This quadratic equation admits one positive, and one negative solution with the positive solution being equation (7.6). Substituting $\bar{u}(x_0)$ from equation (7.6) to $\bar{x}_i = \bar{u}(x_0) - \bar{u}(x_0)^2 c_i$ for $i = 1, \ldots m$, we obtain $\bar{x}_i$ as equation (7.4). This establishes the uniqueness of the Nash equilibrium.

□

Theorem 7.2 establishes existence and uniqueness of the Nash equilibrium, but does not guarantee that the equilibrium is reached by the malwares. In the next section, we prove convergence to the Nash equilibrium arising from simple distributed strategies of the players.

7.4 Convergence to the Nash Equilibrium

In this section, we propose a dynamical model of the malware strategy, in which each adversary greedily updates its takeover rate at each time step. We prove that, under these greedy dynamics, the takeover rates converge to the unique N.E. identified in Section 7.3.

The proof that all malwares converge to the N.E. of Theorem 7.2 is divided into three parts. In the first part (Section 7.4.2), we prove that all malwares with $\bar{x}_i = 0$ will eventually drop out under the proposed dynamics. In the second part (Section 7.4.3), we establish that

there exists a finite time T_{part} such that $x_i(t) > 0$ for all malwares i with $\bar{x}_i > 0$ and all $t > T_{part}$. In the third part (Section 7.4.4), we prove convergence to the unique N.E. using passivity analysis, under the assumption that all malwares $1, \ldots, m$ participate and malwares $(m+1), \ldots, n$ have dropped out (i.e., $t > \max\{T_{drop}, T_{part}\}$).

7.4.1 Greedy Dynamics of Malwares

We assume that each malware can observe the sum of takeover rates $u(t) := \sum_{i=0}^{n} x_i(t)$ at time t. Each malware i can compute the total takeover rate $u(t)$ by observing the fraction of time that i controls the host.

We consider an adversary who, at each time t, updates its takeover rate $x_i(t)$ to move in the gradient direction, corresponding to an adaptive and greedy (myopic) adversary. This behavior results in dynamics

$$\dot{x}_i(t) = \left(-x_i(t) + u(t) - u^2(t)c_i\right)^+_{x_i} \tag{7.8}$$

where $(\cdot)^+_{x_i}$ is the positive projection defined as

$$(h(x_i, u))^+_{x_i} = \begin{cases} 0, & x_i = 0 \text{ and } h(x_i, u) < 0 \\ h(x_i, u), & \text{else} \end{cases}$$

We say that the positive projection is active in the case $x_i = 0$ and $h(x_i, u) < 0$, and inactive otherwise. The dynamics (7.8) capture the behavior of an adversary who attempts to maximize his utility at each time step, and can be computed by an adversary using only knowledge of the total takeover rate $u(t)$. We now show the proposed dynamics guarantee convergence to the Nash equilibrium in Theorem 7.2.

7.4.2 Malware Dropout

In this subsection, we show that all malwares $i \geq m+1$ will eventually drop out of the game, i.e., there exists time T_{drop} such that the positive projections will remain active for malwares $i \geq m+1$ at any time $t > T_{drop}$. We begin by proving the following lemmas.

Lemma 7.1. *Suppose there exists a malware $m+1$ with cost c_{m+1} satsifying the inequality (7.3). Then, for all malwares indexed $j \geq m+1$, the following inequalities hold:*

$$c_j \geq \frac{2S_c(j)}{j + f(x_0, j-1)} \tag{7.9}$$

$$c_j \geq \frac{-(j-2) + f(x_0, j-1)}{2x_0} \tag{7.10}$$

$$= \frac{2S_c(j-1)}{j-2+f(x_0, j-1)} \tag{7.11}$$

Proof: We start with the case $j = m+1$. Since $m+1$ drops out at N.E, c_{m+1} satisfies the inequality $c_{m+1} \geq \frac{2S_c(m)}{m-1+f(x_0,m)}$ from inequality (7.3). Therefore, (7.11) is true for $j = m+1$. This inequality can be rearranged to

$$c_{m+1}(m - 1 + f(x_0, m)) \geq 2S_c(m) \tag{7.12}$$

By adding $2c_{m+1}$ to both sides of the inequality, we obtain

$$c_{m+1} \geq \frac{2S_c(m+1)}{m+1+f(x_0, m)} \tag{7.13}$$

This proves inequality (7.9) for $j = m+1$.

We state the following identity which shows that inequalities (7.10) and (7.11) are equivalent.

$$\frac{-(j-2) + f(x_0, j-1)}{2x_0} = \frac{2S_c(j-1)}{j-2+f(x_0, j-1)} \tag{7.14}$$

which is true for all $j \geq 2$ since

$$-\left((j-2)^2 - f(x_0, j-1)^2\right) = 4x_0 S_c(j-1)$$

Therefore, inequalities (7.9) – (7.11) hold for $j = m+1$. We will now show that (7.11) is true for $j = m+2$ by first proving the following inequality.

$$m + 1 + f(x_0, m) \leq m + f(x_0, m+1) \tag{7.15}$$

By squaring both sides of the above inequality and rearranging the terms, we obtain the following inequality,

$$c_{m+1} \geq \frac{-(m-1) + f(x_0, m)}{2x_0} \tag{7.16}$$

which is true from inequality (7.10). Therefore, from (7.15), (7.13), and the $c_{m+2} \geq c_{m+1}$ by definition, we obtain

$$c_{m+2} \geq c_{m+1} \geq \frac{2S_c(m+1)}{m+1+f(x_0,m)} \geq \frac{2S_c(m+1)}{m+f(x_0,m+1)}$$

Starting with (7.11) for $j = m+2$, the same argument can be made to prove (7.9)–(7.10) for $j = m+2$, and to show (7.11) for $j = m+3$. This process is repeated inductively to prove set of lower bounds for all $j \geq m+1$. ■

We now develop an inductive proof that malwares $\{m+1, \ldots, n\}$ eventually drop out. We first show that, for any $j \geq (m+1)$, if malwares $\{(j+1), \ldots, n\}$ drop out, then malware j will eventually drop out as well.

Lemma 7.2. *Consider the set* $U_j = \{\frac{1}{c_{j+1}} \leq u(t) \leq \frac{1}{c_j}\}$ *where* $m+1 \leq j \leq n-1$. *Suppose that* $x_i(t) = 0$ *for* $i \geq j+1$, *and* $\bar{u}(x_0) \neq \frac{1}{c_j}$. *Then,* $\dot{u}(t) > 0$ *for all* $u(t) \in U_j$, *and there exists a finite time* $T_{escape}(j)$ *such that* $u(t) > \frac{1}{c_j}$ *for all* $t \geq T_{escape}(j)$. *If* $x_i(t) = 0$ *for* $i \geq j+1$, *and* $\frac{1}{c_j} = \bar{u}(x_0)$, *then* $u(t)$ *converges to* $\bar{u}(x_0)$ *if* $u(t_0) \in U_j$ *for some* t_0.

Proof. If $u(t) \in U_j$, then positive projections are inactive for all malwares $1, \ldots, j$ since $u - u^2 c_i \geq 0$ for all $i \leq j$. Moreover, $u - u^2 c_i \leq 0$ for all $i = (j+1), \ldots, n$. If $x_i(t) = 0$ for $i \geq j+1$, then the positive projections are active for $i \geq j+1$, and $\dot{u}(t)$ can be computed as

$$\dot{u}(t) = (j-1)u - u^2 S_c(j) + x_0 \tag{7.17}$$

We will now show that $\dot{u}(t) \geq 0$ for $\{\frac{1}{c_{j+1}} \leq u(t) \leq \frac{1}{c_j}\}$ if $x_i(t) = 0$ for $i \geq j+1$. We have

$$\begin{aligned} \dot{u}(t) &= u\,(j-1-uS_c(j)) + x_0 \\ &\geq \frac{j-2-f(x_0,j-1)}{2c_j} + x_0 \geq -x_0 + x_0 = 0 \end{aligned}$$

The first inequality follows from the assumption that $u(t) \geq \frac{1}{c_j}$, the lower bound (7.9), and the fact that $j-2-f(x_0,j-1) < 0$ for all $x_0 > 0$. The last inequality is from (7.10) and the negativity of $j-2-f(x_0,j-1)$.

The set of inequalities hold with equality if and only if $u(t) = \frac{1}{c_j}$, and c_j satisfies the inequalities (7.9)-(7.11) with equality. From the proof of Lemma 7.1, this is true if and only if $c_j = c_{m+1} = \frac{1}{\bar{u}(x_0)}$. Therefore, if $\frac{1}{c_j} \neq \bar{u}(x_0)$, then $\dot{u}(t) > 0$ for $u(t) \in U_j$.

Since $u(t)$ is monotonically increasing in U_j, there exists a finite time $T_{escape}(j)$ such that $u(t)$ will exit U_j to the set U_{j-1}, and $u(t)$ will not enter U_j for all $t \geq T_{escape}(j)$ since $\dot{u}(t) > 0$ at the boundary point $u(t) = \frac{1}{c_j}$.

If $\frac{1}{c_j} = x_0$, then $\dot{u}(t) > 0$ in U_j and $\dot{u}(t) = 0$ at $u(t) = \frac{1}{c_j}$. Hence $u(t) \to \bar{u}(x_0)$ if $u(t) \in U_j$ initially. □

Given Lemmas 7.1 and 7.2, we now prove the following theorem, which states that malwares $i \geq m + 1$ will eventually drop out of the game.

Theorem 7.3. *If $\bar{u}(x_0) \neq \frac{1}{c_{m+1}}$, then there exists a finite time T_{drop} such that $u(t) > \frac{1}{c_{m+1}}$ and $x_i(t) = 0$ for $i \geq m + 1$ and $t \geq T_{drop}$. If $\bar{u}(x_0) = \frac{1}{c_{m+1}}$, and $u(t) \leq \frac{1}{c_{m+1}}$, then $u(t)$ converges to $\bar{u}(x_0)$.*

Proof. First assume that $\bar{u}(x_0) \neq \frac{1}{c_{m+1}}$. We start by considering the case $0 \leq u(t) \leq \frac{1}{c_n}$, and use induction to prove that all malwares $i \geq m + 1$ will drop out of the game. For $0 \leq u(t) \leq \frac{1}{c_n}$, the positive projection is inactive for all malwares. Therefore, $\dot{u}(t)$ is written as

$$\dot{u}(t) = (n-1)u - u^2 S_c(n) + x_0 \tag{7.18}$$

By the same argument as we made for the set $U_j = \{\frac{1}{c_{j+1}} \leq u(t) \leq \frac{1}{c_j}\}$ in Lemma 7.2, $\dot{u}(t) > 0$, for $\{0 < u(t) \leq \frac{1}{c_n}\}$, and there exists $T_{escape}(n)$ such that $u(t) > \frac{1}{c_n}$ for all $t \geq T_{escape}(n)$.

Moreover, in the interval $u(t) \geq \frac{1}{c_n}$, $x_n(t)$ is monotonically decreasing since

$$\dot{x}_n(t) = \left(-x_n(t) + u(t) - u^2(t)c_n\right)^+_{x_n} < 0 \text{ for } x_n(t) > 0$$

Therefore, there exists a finite time $T_{drop}(n)$ such that $x_n(t) = 0$ for all $t \geq T_{drop}(n)$, and the positive projection will remain active for malware n.

Given that malware n's positive projection is active, from Lemma 7.2, we conclude that there exists a finite time $T_{escape}(n-1)$ such that $u(t) > \frac{1}{c_{n-1}}$ for all $t > T_{escape}(n-1)$. Since $x_{n-1}(t)$ is monotonically decreasing when $u(t) > \frac{1}{c_{n-1}}$, there exists a time $T_{drop}(n-1)$ such that malware $(n-1)$ will be active for $t \geq T_{drop}(n-1)$.

Inductively, given $x_i(t) = 0$ for $i \geq j+1$, we conclude that $u(t)$ will escape the set $\{\frac{1}{c_{j+1}} < u(t) \leq \frac{1}{c_j}\}$ and will remain in $\{u(t) > \frac{1}{c_j}\}$. This proves that there exists time T_{drop} such that for all $t > T_{drop}$, $u(t) > \frac{1}{c_{m+1}}$ and $x_i(t) = 0$ for $i \geq m+1$.

On the other hand, suppose that $\bar{u}(x_0) = \frac{1}{c_{m+1}}$, and $u(t) \leq \frac{1}{c_{m+1}}$ initially. Then, for all U_j such that $c_j \neq c_{m+1}$ and $j > m+1$, $u(t)$ will eventually escape U_j in a finite time and enter $U_{c_{m+1}}$. From Lemma 7.2, $u(t)$ will converge to $\frac{1}{c_{m+1}}$, which completes the proof. □

7.4.3 Participation of Malwares

In this subsection, we prove that all malwares with positive takeover rates $\bar{x}_i > 0$ at N.E. will eventually participate in the game. In other words, we will show that all positive projections will eventually become inactive and remain inactive for malwares $i \leq m$.

The following inequality holds for malwares $i = 1, \ldots, m$, and can be derived by the same approach as Lemma 7.1.

$$c_j < \frac{2S_c(j)}{j + f(x_0, j-1)} \tag{7.19}$$

$$c_j < \frac{2S_c(j-1)}{j - 2 + f(x_0, j-1)} \tag{7.20}$$

$$= \frac{-(j-2) + f(x_0, j-1)}{2x_0} \tag{7.21}$$

Furthermore, $c_1 < \frac{1}{x_0}$.

The following theorem shows that malware $i \leq m$ will eventually participate in the game.

Theorem 7.4. *There exists some finite time T_{part} such that, for all $t > T_{part}$, $u(t) < \frac{1}{c_m}$ and positive projections are inactive for malwares $i \leq m$.*

Proof. Consider the set $U_1 = \{u(t) : \frac{1}{c_1} \leq u(t) < \infty\}$. In U_1, $\dot{u}(t) = 0$ if and only if $x_1, \ldots, x_n = 0$ and $u(t) = x_0$ since $u - u^2 c_i \leq 0$ for all $i \geq 1$. However, this case is not

possible since $x_0 < \frac{1}{c_1}$ which violates the definition of U_1. Therefore, $\dot{u}(t) < 0$ in U_1 and hence there exists a finite time $T_{escape}(1)$ such that $u(t) < \frac{1}{c_1}$ for all $t \geq T_{escape}(1)$.

Now, consider the set $U_j = \{u(t) : \frac{1}{c_j} \leq u(t) < \frac{1}{c_{j-1}}\}$ for $2 \leq j \leq m$. In U_j, positive projections are inactive for malwares $i \leq j-1$. Denote $I(t) = \{i : i \geq j, \dot{x}_i \neq 0\}$. Then $\sum_{i=1}^{j-1} \dot{x}_i(t)$ can be bounded above by

$$\begin{aligned}
&\sum_{i=1}^{j-1} \dot{x}_i(t) = -\sum_{i=1}^{j-1} x_i + u(t)(j-1) - u^2(t)S_c(j) \\
= \;& u(t)\left(j - 2 - u(t)S_c(j-1)\right) + x_0 + \sum_{k \in I(t)} x_k(t) \\
< \;& \frac{1}{c_j}\left(\frac{j-2-f(x_0, j-1)}{2}\right) + x_0 + \sum_{k \in I(t))} x_k(t) \\
\leq \;& -x_0 + x_0 + \sum_{k \in I(t)} x_k(t) = \sum_{k \in I(t)} x_k(t)
\end{aligned}$$

where the first inequality follows from the assumptions that $u(t) > \frac{1}{c_j}$ and (7.20), and the last inequality is from (7.21). However, in U_j, $\dot{x}_i \leq -x_i$ for all $i \in I(t)$ since $u - u^2 c_i \leq 0$ for all $i \geq j$. Therefore, $\dot{u}(t) < 0$, and hence there exists a finite time $T_{escape}(j)$ such that $u(t) < \frac{1}{c_j}$ for all $t \geq T_{escape}(j)$. Let $T_{part} = \max_j\{T_{escape}(j)\}$, then $u(t) < \frac{1}{c_m}$ after for all $t \geq T_{part}$. Moreover since $u - u^2 c_i > 0$ for all $i \leq m$, positive projection will be inactive for all $t \geq T_{part}$. □

The following Corollary states that all malwares $i \geq m+1$ will eventually drop out of the game and the game will be played only by the malwares $i \leq m$.

Corollary 7.1. *There exists a finite time T such that for all $t > T$, $x_i = 0$ and $\dot{x}_i = 0$ for malwares $i \geq m+1$, and positive projections are inactive for malwares $i \leq m$. Moreover, $u(t) \in \left[\frac{1}{c_{m+1}}, \frac{1}{c_m}\right]$ for $t \geq T$.*

Proof. Let $T = \max\{T_{drop}, T_{part}\}$, where T_{drop} and T_{part} were defined in Theorems 7.3 and 7.4 respectively. It is straightforward to conclude that claims of this Corollary is true for $t > T$ from the definitions of T_{drop} and T_{part}. □

Corollary 7.1 implies that all malwares with $\bar{x}_i = 0$ (e.g., $i > m$) will eventually drop out and all malwares with $\bar{x}_i > 0$ (e.g., $i \leq m$) will eventually participate. In what follows, we show that the dynamics of the participating malware takeover rates eventually converge to the N.E.

7.4.4 Passivity Approach for Convergence to the N.E.

In this section, we use a passivity analysis to prove that the proposed dynamics (7.8) guarantees convergence to the N.E. when only the malwares $i \leq m$ participate in the game.

Define $v_i(t) = u(t) - u^2(t)c_i$ and $\bar{v}_i = \bar{u}(t) - \bar{u}(t)^2 c_i$. Since positive projections are inactive in the interval $\left[\frac{1}{c_{m+1}}, \frac{1}{c_m}\right]$ for all $i \leq m$, $\dot{x}_i$ is given as

$$\dot{x}_i(t) = -x_i(t) + u(t) - u^2(t)c_i = -x_i(t) + v_i(t) \tag{7.22}$$

The main intuition of the proof is the following. If $u(t) \to \bar{u}(x_0)$, then $v_i(t) \to \bar{v}_i = \bar{x}_i$ for all i. Then the dynamics of x_i will guarantee that $x_i \to \bar{u} - \bar{u}^2 c_i$, which is the Nash equilibrium of malware i as shown in Section 7.3.

We will first show that $u(t)$ converges to $\bar{u}(x_0)$ using a Lyapunov method.

Lemma 7.3. *Under the dynamics (7.8), $u(t)$ asymptotically converges to $\bar{u}(x_0)$.*

Proof. Consider the Lyapunov function

$$V_1(u) = \gamma \int_{\bar{u}}^{u} (\sigma^2 - \bar{u}^2) d\sigma$$

where $\gamma > 0$. Then, $V_1(\bar{u}) = 0$, $\frac{dV_1}{du} = 0$ if $u = \bar{u}$, and $\frac{d^2V_1}{du^2} = 2u \geq 0$ for $u \geq 0$. Therefore, in the region $u \geq 0$, V_1 is a convex function which achieves its global minimum zero at $u = \bar{u}$.

Differentiating $V_1(u)$ with respect to time, we obtain

$$\begin{aligned} & \dot{V}_1(u) = \gamma(u^2 - \bar{u}^2)\dot{u} \\ = \; & \gamma(u^2 - \bar{u}^2)\left((m-1)(u-\bar{u}) - S_c(m)(u^2 - \bar{u}^2)\right) \\ = \; & \gamma(u+\bar{u})(u-\bar{u})^2 \frac{m-1-f(x_0,m)}{2} \\ & -\gamma S_c(m) u (u+\bar{u})(u-\bar{u})^2 \\ = \; & \gamma(u+\bar{u})(u-\bar{u})^2 \left(\frac{m-1-f(x_0,m)}{2} - S_c(m)u\right) \end{aligned}$$

which is bounded above by zero since $m - 1 < f(x_0, m)$ for all $x_0 > 0$. Therefore $\dot{V}_1(u) = 0$ if and only if $u = \bar{u}$ and $\dot{V}_1(u) < 0$ otherwise. □

We will now prove the main result of the section which shows that the greedy dynamics (7.8) guarantees convergence to the N.E. We use a passivity-based analysis [40] and interpret the overall dynamics as a negative feedback interconnection of two systems (Figure 7.1). The top block is the greedy dynamics block where each malware updates its takeover rate, and the bottom block is the computation of the gradient ascent direction of the utilities.

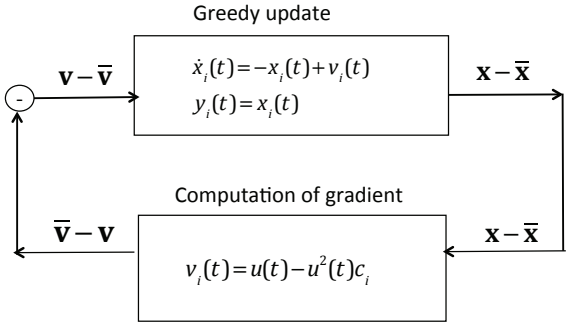


Figure 7.1: Figure illustrating passivity approach for proving convergence to the N.E. The update dynamics of malwares is decomposed into two blocks, where the top block takes in the ascent direction v_i, and updates its takeover rate, and the bottom block computes the gradient from the updated x_i. Shortage of passivity of the bottom block is dissipated by the excess of passivity of the top block.

Theorem 7.5. *The greedy dynamics (7.22) is output strictly passive from input* $(\mathbf{v} - \bar{\mathbf{v}})$ *to output* $\mathbf{x} - \bar{\mathbf{x}}$.

Proof. Consider the storage function V_{top} given as

$$V_{top} = \frac{1}{2}\sum_{i=1}^{m}(x_i - \bar{x}_i)^2 + \gamma \int_{\bar{u}}^{u}(\sigma^2 - \bar{u}^2)d\sigma$$

Differentiating V_{top} with respect to time, we obtain

$$\begin{aligned}\dot{V}_{top} &= \sum_i (x_i - \bar{x}_i)\dot{x}_i + (u^2 - \bar{u}^2)\dot{u} \\ &= \sum_i (v_i - \bar{v}_i)(x_i - \bar{x}_i) - \sum_i (x_i - \bar{x}_i)^2 + \gamma(u^2 - \bar{u}^2)\dot{u}\end{aligned}$$

Moreover, from Lemma 7.3, we know that $\dot{V}_1(u) \leq 0$ except at $u = \bar{u}$. Therefore,

$$\dot{V}_{top} \leq (\mathbf{v} - \bar{\mathbf{v}})^T(\mathbf{x} - \bar{\mathbf{x}}) - P_{top}(\mathbf{x} - \bar{\mathbf{x}}) \tag{7.23}$$

where $P_{top}(\cdot) : R^m \to R_+$ is a positive definite function defined as

$$P_{top}(\mathbf{x} - \bar{\mathbf{x}}) = (\mathbf{x} - \bar{\mathbf{x}})^T(\mathbf{x} - \bar{\mathbf{x}}) - \dot{V}_1(u) \geq 0 \tag{7.24}$$

with $P_{top}(\mathbf{x} - \bar{\mathbf{x}}) = 0$ if and only if $\mathbf{x} = \bar{\mathbf{x}}$. □

Theorem 7.6. *Computation of* $v_i(\cdot)$ *is input-feedforward passive from input* $\mathbf{x} - \bar{\mathbf{x}}$ *to output* $\bar{\mathbf{v}} - \mathbf{v}$*, i.e., there exists a function* $P_{bot}(\mathbf{x} - \bar{\mathbf{x}})$ *such that*

$$(\mathbf{x} - \bar{\mathbf{x}})^T(\bar{\mathbf{v}} - \mathbf{v}) \geq P_{bot}(\mathbf{x} - \bar{\mathbf{x}}) \tag{7.25}$$

Proof. Define $P_{bot}(\mathbf{x} - \bar{\mathbf{x}})$ as

$$P_{bot}(\mathbf{x} - \bar{\mathbf{x}}) = -(u - \bar{u})^2 + \sum_i c_i(x_i - \bar{x}_i)(u^2 - \bar{u}^2)$$

since $u - \bar{u} = \mathbf{1}^T(\mathbf{x} - \bar{\mathbf{x}})$, P_{bot} is a function of $\mathbf{x} - \bar{\mathbf{x}}$. Expanding $(\mathbf{x} - \bar{\mathbf{x}})^T(\bar{\mathbf{v}} - \mathbf{v})$, we obtain

$$\begin{aligned}&\sum_i (x_i - \bar{x}_i)(\bar{v}_i - v_i) = (x_i - \bar{x}_i)(\bar{u} - u + (u^2 - \bar{u}^2)c_i) \\ &= -(u - \bar{u})^2 + \sum_i c_i(x_i - \bar{x}_i)(u^2 - \bar{u}^2)\end{aligned}$$

Therefore

$$\sum_i (x_i - \bar{x}_i)(\bar{v}_i - v_i) \geq -(u - \bar{u})^2 + \sum_i c_i (x_i - \bar{x}_i)(u^2 - \bar{u}^2)$$

thus satisfying the condition (7.25) with equality. □

The following theorem proves convergence to the N.E. The intuition is that any shortage of passivity from the computation of v_i is dissipated by the excess of passivity in the greedy dynamics.

Theorem 7.7. *Consider the negative feedback interconnection of of the two dynamical systems corresponding to greedy update and computation of the gradient direction (Figure 7.1). The equilibrium of the closed loop system $\mathbf{x} = \bar{\mathbf{x}}$ is globally asymptotically stable.*

Proof. Let γ be chosen such that

$$\gamma \geq \frac{K}{S_c(m)} \cdot \frac{m - 1 + f(x_0, m)}{-m + 1 + f(x_0, m)} \tag{7.26}$$

where K is given as

$$K = \frac{1}{4m} \left(m \sum_i c_i^2 - S_c(m)^2 \right)$$

Using V_{top} as a candidate Lyapunov function, we obtain

$$\begin{aligned} \dot{V}_{top} &\leq -P_{bot}(\mathbf{x} - \bar{\mathbf{x}}) - P_{top}(\mathbf{x} - \bar{\mathbf{x}}) \\ &= (u - \bar{u})^2 - \sum_i c_i (x_i - \bar{x}_i)(u^2 - \bar{u}^2) - \sum_i (x_i - \bar{x}_i)^2 \\ &+ \gamma (u + \bar{u})(u - \bar{u})^2 \left(\frac{m - 1 - f(x_0, m)}{2} - S_c(m) u \right) \end{aligned}$$

In order to obtain an upper bound on the above expression, we will first upper bound the term $(u-\bar{u})^2 - (u^2 - \bar{u}^2) \sum_i c_i (x_i - \bar{x}_i) - \sum_i (x_i - \bar{x}_i)^2$. To do so, we solve a convex optimization problem

$$\begin{aligned} \min_{\mathbf{z}} \quad & \textstyle\sum_i z_i^2 + (u^2 - \bar{u}^2) \sum_i c_i(z_i) \\ \text{s.t.} \quad & \textstyle\sum_i z_i = u - \bar{u} \end{aligned} \tag{7.27}$$

which is a quadratic program with equality constraint. Solving the optimization problem, and substituting $z_i^* = x_i - \bar{x}_i$, we obtain

$$\begin{aligned}
&(u-\bar{u})^2 - (u^2-\bar{u}^2)\sum_i c_i(x_i-\bar{x}_i) - \sum_i (x_i-\bar{x}_i)^2 \\
&\leq \frac{1}{4m}(m\sum_i c_i^2 - S_c^2)(u^2-\bar{u}^2)^2 \\
&\quad + \frac{1}{m}(u-\bar{u})^2(m-1-S_c(m)(u+\bar{u})) \leq K(u^2-\bar{u}^2)^2
\end{aligned}$$

where the last inequality is due to the fact that

$$m-1-S_c(m)\bar{u} = \frac{1}{2}\left(m-1-f(x_0,m)\right) \leq 0$$

Therefore,

$$\begin{aligned}
&\dot{V}_{top} \leq -P_{bot}(\mathbf{x}-\bar{\mathbf{x}}) - P_{top}(\mathbf{x}-\bar{\mathbf{x}}) \\
&\leq K(u^2-\bar{u}^2)^2 \\
&\quad + \gamma(u+\bar{u})(u-\bar{u})^2\left(\frac{m-1-f(x_0,m)}{2} - S_c(m)u\right) \\
&= (u-\bar{u})^2(u+\bar{u})\left((K-\gamma S_c)u + K\bar{u} + \gamma\frac{m-1-f}{2}\right) \\
&\leq (u-\bar{u})^2(u+\bar{u})\left((K-\gamma S_c)u\right) \leq 0
\end{aligned}$$

where the last two inequalities are from (7.26). □

The results of this section imply that, for a given mitigation strategy modeled as the takeover rate x_0, the takeover rates of the malwares will converge to the Nash equilibrium. In the following section, we investigate selection of the optimal mitigation strategy.

7.5 Optimal Mitigation Strategy

In this section, we derive an optimal mitigation strategy against competing malwares as the solution to a Stackelberg game. In the Stackelberg formulation, the system owner selects the takeover rate, x_0, and establishes this rate as a fixed policy. The malwares then select their takeover rates as the Nash equilibrium given the policy x_0, based on the dynamics of Section

7.4. Since the sum of the takeover rates $\sum_{i=0}^{n} x_i$ will converge to $\bar{u}(x_0)$, a system owner will select x_0 to maximize the utility function

$$U_0(x_0) = \frac{x_0}{\bar{u}(x_0)} - c_0 x_0. \tag{7.28}$$

The following theorem shows that an efficient optimization algorithm can be constructed to maximize $U_0(x_0)$.

Theorem 7.8. *Given the number of participating malwares at the N.E. m, $U_0(x_0)$ is a concave function in x_0.*

Proof. It suffices to show the concavity of $\frac{x_0}{\bar{u}(x_0)}$ since $c_0 x_0$ is a linear function in x_0. From equation (7.6), we have

$$\frac{x_0}{\bar{u}(x_0)} = \frac{2S_c(m)x_0}{m - 1 + f(x_0, m)}$$

by rewriting

$$\frac{2S_c(m)}{m - 1 + f(x_0, m)} = \frac{-(m-1) + f(x_0, m)}{2x_0}$$

we obtain

$$\frac{x_0}{\bar{u}(x_0)} = \frac{1}{2}\left(-(m-1) + f(x_0, m)\right)$$

which is concave in x_0 since $f(x_0, m)$ is a composition of a concave function (square root) with an affine function of x_0. □

Based on the theorem, the following optimization algorithm can be constructed by the system owner. The owner can divide the possible values of x_0 into a set of $n+1$ intervals $\{I_m(x_0)\}_{m=0}^{n}$ where

$$I_m(x_0) = \{x_0 : m \text{ malwares participate at N.E.}\}$$

These intervals will be disjoint since m is a monotone decreasing function in x_0. By Theorem 7.8, the owner can obtain $x_0^{(m)} \triangleq \arg\max\{U_0(x_0) : x_0 \in I_m\}$ for $m = 1, \ldots, n$ by solving a convex optimization problem, and then select the optimal takeover rate as $x_0^* = \arg\max\{U_0(x_0^{(m)}) : m = 1, \ldots, n\}$.

We observe that, in order to solve the convex optimization problem for each interval I_m, the system owner needs to know the parameters m and $S_c(m)$. To estimate these parameters, the owner can choose an x_0 and observe the fraction of time $\frac{x_0}{\bar{u}(x_0)}$. Based on this information, the owner can construct an equation

$$\frac{x_0}{\bar{u}(x_0)} = S_c(m)\bar{u}(x_0) - (m-1)$$

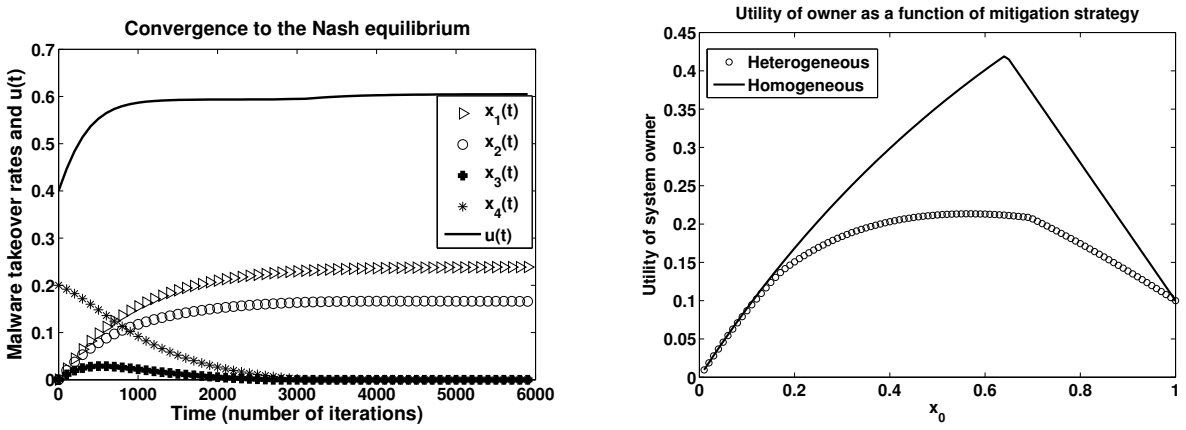
which is a linear equation in m and $S_c(m)$ given x_0 and $\bar{u}(x_0)$. Therefore, the owner can estimate the parameters by choosing two different x_0 values and constructing two linear independent equations based on the responses of the adversary.

7.6 Numerical Study

We evaluated our approach using Matlab simulation. We conducted two numerical simulations. The first simulation verifies the convergence to the Nash equilibrium given the system owner's takeover rate x_0 and analyzes the malware dynamics prior to convergence. In the second simulation, we numerically evaluate the utility of the system owner in two cases. In the first case, multiple competing malwares have heterogeneous costs. In the second case, the competing malwares have equal costs of takeover and hence are homogeneous. The sum of the costs was equal in both cases.

Figure 7.2(a) shows the convergence to the N.E. of malwares given a fixed x_0. At the equilibrium, malwares 1, 2 and the system owner own the resource 0.4, 0.27 and 0.33 fraction of time respectively. Initial takeover rates of malwares were set as [0,0,0,0.2] with corresponding costs [1,1.2,1.7,1.72]. The system owner's takeover rate was fixed at $x_0 = 0.2$. Under these parameters, Theorem 7.2 implies that malwares 3 and 4 will drop out, and malwares 1 and 2 will converge to N.E with positive takeover rates. The numerical value of $\bar{\mathbf{x}}$ is consistent with values computed from Theorem 7.2.

We observe from Figure 7.2(a) that the proposed dynamics (7.8) ensures that malwares 1 and 2 participate in the game even when initial takeover rates were initialized to zero. Malware 3 initially increases its takeover rate, but eventually drops out as malwares 1 and



(a) (b)

Figure 7.2: (a) Figure illustrating the convergence to the Nash equilibrium. Initial takeover rates of malwares were given as [0,0,0, 0.2] with corresponding costs [1,1.2, 1.7, 1.72]. System owner's takeover rate was fixed at $x_0 = 0.2$. (b) Figure illustrating the utility of the system owner when competing against heterogeneous malwares and equally powerful malwares. The cost of system owner was set to $c_0 = 0.9$. In the heterogeneous case, six malwares have corresponding costs [1,1.2,1.7,1.72, 1.8, 1.9]. In the homogeneous case, all malwares had equal cost $c = 1.553$ so that sum of the costs is equal in both cases.

2 begin to converge to the N.E. It is also shown numerically that the dropouts are not necessarily sequential, i.e., malwares with higher costs do not drop out of the game first. Malware 4, given high initial takeover rate and highest cost c_4, does not drop out until after malware 3 drops out.

Figure 7.2(b) compares the utility of the system owner for heterogeneous and homogeneous malwares. In both cases, the simulations numerically verify that the owner's utility is a concave function in x_0, and the utility function becomes $1 - c_0 x_0$ after all malwares drop out of the takeover game. The maximum achieved utility is higher when competing against equally powerful malwares where all malwares either participate or dropout at the N.E. Letting $\hat{x}_0$ denote the minimum x_0 to make all malwares drop out in the homogeneous case, we observe that the malware with the lowest cost in the heterogeneous case will maintain a positive takeover rate when $x_0 = \hat{x}_0$. Hence, we observe that the utility of the system owner

is mainly determined by the capabilities of the most powerful malware.

7.7 Conclusions and Future Work

In this chapter, we modeled the interaction between competing, adaptive malwares and a system owner by formulating a generalized version of the FlipIt game. We derived a closed form for the unique Nash equilibrium of the formulated game when the system owner and malwares employ exponential strategies for taking over the host with time-varying rates.

We modeled the adaptive nature of malwares as gradient ascent dynamics where each malware updates its takeover rate in order to maximize its utility. The proposed dynamics only requires the knowledge of either the fraction of time one owns the resource. Using a passivity-based approach, we proved that the greedy dynamics guarantee convergence to the Nash equilibrium. We derived an optimal mitigation strategy as a solution to a Stackelberg game, in which the system owner first commits its takeover rate x_0.

While our approach assumed that each malware can accurately observe the total takeover rate by observing the fraction of time one controls the host, in practice the observation capabilities may vary for different malwares, and may lead to incorrect estimation. Incorporating noisy observation and characterizing the deviation from the identified Nash equilibrium will be part of future work. In addition, for the case when the system owner's takeover rate $x_0 = 0$, the host takeover game between malwares reduces to a linear resource allocation game where regret minimization dynamics have been shown to guarantee convergence [25]. We will investigate whether learning dynamics can be applied to our Stackelberg-Nash game set-up.

BIBLIOGRAPHY

[1] Cyber-physical systems vision statement. Retrieved from http://www.nitrd.gov/nitrdgroups/index.php?title=Cyber_Physical_Systems_(CPS_SSG).

[2] Immediate opportunties for strengthening the nation's cybersecurity. Retrieved from http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf.

[3] Noa Agmon, Sarit Kraus, Gal Kaminka, et al. Multi-robot perimeter patrol in adversarial settings. *International Conference on Robotics and Automation*, pages 2339–2345, 2008.

[4] Tansu Alpcan and Tamer Başar. *Network security: A decision and game-theoretic approach*. Cambridge University Press, 2010.

[5] Eitan Altman and Laura Wynter. Equilibrium, games, and pricing in transportation and telecommunication networks. *Networks and Spatial Economics*, 4(1):7–21, 2004.

[6] Karl J Åström and Björn Wittenmark. *Adaptive Control*. Addison-Wesley, 1995.

[7] Michael Bailey, Evan Cooke, Farnam Jahanian, and David Watson. The blaster worm: Then and now. *IEEE Security & Privacy*, 3(4):26–31, 2005.

[8] John S Baras, Svetlana Radosavac, George Theodorakopoulos, Dan Sterne, Peter Budulas, and Richard Gopaul. Intrusion detection system resiliency to byzantine attacks: The case study of wormholes in OLSR. *IEEE Military Communications Conference (MILCOM)*, pages 1–7, 2007.

[9] Emrah Bayraktaroglu, Christopher King, Xin Liu, Guevara Noubir, Rajmohan Rajaraman, and Bishal Thapa. Performance of IEEE 802.11 under jamming. *Mobile Networks and Applications*, 18(5):678–696, 2013.

[10] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. *Proceedings of the 1st ACM conference on Computer and communications security*, pages 62–73, 1993.

[11] Sourabh Bhattacharya and Tamer Başar. Game-theoretic analysis of an aerial jamming attack on a UAV communication network. *American Control Conference (ACC)*, pages 818–823, 2010.

[12] Michael Bloem, Tansu Alpcan, and Tamer Basar. An optimal control approach to malware filtering. *Proceedings of the 46th IEEE Conference on Decision and Control*, pages 6059–6064, 2007.

[13] Michael Bloem, Tansu Alpcan, and Tamer Başar. Optimal and robust epidemic response for multiple networks. *Control Engineering Practice*, 17(5):525–533, 2009.

[14] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[15] Gerald Brown, Matthew Carlyle, Javier Salmerón, and Kevin Wood. Defending critical infrastructure. *Interfaces*, 36(6):530–544, 2006.

[16] Alvaro A Cárdenas, Saurabh Amin, and Shankar Sastry. Research challenges for the security of control systems. *HotSec*, 2008.

[17] Alvaro A Cardenas, Saurabh Amin, and Shankar Sastry. Secure control: Towards survivable cyber-physical systems. *The 28th International Conference on Distributed Computing Systems Workshops*, pages 495–500, 2008.

[18] Lin Chen and Jean Leneutre. A game theoretical framework on intrusion detection in heterogeneous networks. *IEEE Transactions on Information Forensics and Security*, 4(2):165–178, 2009.

[19] Mung Chiang, Steven H Low, A Robert Calderbank, and John C Doyle. Layering as optimization decomposition: A mathematical theory of network architectures. *Proceedings of the IEEE*, 95(1):255–312, 2007.

[20] Eric Chien, Liam O.Murchu, and Nicolas Falliere. W32. Duqu: the precursor to the next Stuxnet. *Proc. of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2012.

[21] Andrew Clark, Kun Sun, and Radha Poovendran. Effectiveness of IP address randomization in decoy-based moving target defense. *Conference on Decision and Control (CDC)*, pages 678–685, 2013.

[22] Andrew Clark, Quanyan Zhu, Radha Poovendran, and Tamer Başar. Deceptive routing in relay networks. *Decision and Game Theory for Security*, pages 171–185, 2012.

[23] Danny Dolev and Andrew. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[24] Kimon Drakopoulos, Asuman Ozdaglar, and John N Tsitsiklis. An efficient curing policy for epidemics on graphs. *IEEE Transactions on Network Science and Engineering*, 1(2):67–75, 2014.

[25] Eyal Even-Dar, Yishay Mansour, and Uri Nadav. On the convergence of regret minimization dynamics in concave games. *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 523–532, 2009.

[26] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. Stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5, 2011.

[27] Guofei Gu, Phillip A Porras, Vinod Yegneswaran, Martin W Fong, and Wenke Lee. Bothunter: Detecting malware infection through ids-driven dialog correlation. *Usenix Security*, 7:1–16, 2007.

[28] Peter Gutmann. The commercial malware industry. *DEFCON conference*, 2007.

[29] M. H. R. Khouzani, Saswati Sarkar, and Eitan Altman. Maximum damage malware attack in mobile wireless networks. *IEEE/ACM Transactions on Networking*, 20(5):1347–1360, 2012.

[30] MD Hadley, JB McBride, TW Edgar, LR ONeil, and JD Johnson. Securing wide area measurement systems. *US Department of Energy*, 2007.

[31] Shuo Han, Victor M Preciado, Cameron Nowzari, and George J Pappas. Data-driven allocation of vaccines for controlling epidemic outbreaks. *arXiv preprint arXiv:1412.2144*, 2014.

[32] Roger A Horn and Charles R Johnson. *Matrix Analysis*. Cambridge University Press, 2012.

[33] Y-C Hu, Adrian Perrig, and David B Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, pages 1976–1986, 2003.

[34] Farnam Jahanian and Aloysius Ka-Lau Mok. Safety analysis of timing properties in real-time systems. *IEEE Transactions on Software Engineering*, (9):890–904, 1986.

[35] Albert Xin Jiang, Thanh H Nguyen, Milind Tambe, and Ariel D Procaccia. Monotonic maximin: A robust stackelberg solution against boundedly rational followers. *Decision and Game Theory for Security*, pages 119–139, 2013.

[36] Kyoung-Don Kang and Sang Hyuk Son. Real-time data services for cyber physical systems. *IEEE Distributed Computing Systems Workshops*, pages 483–488, 2008.

[37] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, 1(2):293–315, 2003.

[38] Frank Kelly and Thomas Voice. Stability of end-to-end algorithms for joint routing and rate control. *ACM SIGCOMM Computer Communication Review*, 35(2):5–12, 2005.

[39] Jeffrey O Kephart and Steve R White. Directed-graph epidemiological models of computer viruses. *IEEE Computer Society Symposium on Research in Security and Privacy*, pages 343–359, 1991.

[40] Hassan K Khalil. *Nonlinear Systems*. Prentice Hall Upper Saddle River, 2002.

[41] Hassan K Khalil and JW Grizzle. *Nonlinear systems*, volume 3. Prentice hall New Jersey, 1996.

[42] Christopher Kiekintveld, Janusz Marecki, and Milind Tambe. Approximation methods for infinite bayesian stackelberg games: Modeling distributional payoff uncertainty. *The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 3*, pages 1005–1012, 2011.

[43] Peter Kruus, Dan Sterne, Richard Gopaul, Michael Heyman, Brian Rivera, Peter Budulas, Brian Luu, Tommy Johnson, Natalie Ivanic, and Geoff Lawler. In-band wormholes and countermeasures in OLSR networks. *Securecomm and Workshops, 2006*, pages 1–11, 2006.

[44] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[45] Cédric Langbort and Valery Ugrinovskii. One-shot control over an avc-like adversarial channel. pages 3528–3533, 2012.

[46] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *Security & Privacy, IEEE*, 9(3):49–51, 2011.

[47] Aron Laszka, Gabor Horvath, Mark Felegyhazi, and Levente Buttyán. Flipthem: Modeling targeted attacks with flipit for multiple resources. *International Conference on Decision and Game Theory for Security*, pages 175–194, 2014.

[48] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. *Second ACM Conference on Wireless Network Security*, pages 169–180, 2009.

[49] Phillip Lee, Andrew Clark, Linda Bushnell, and Radha Poovendran. A passivity framework for modeling and mitigating wormhole attacks on networked control systems. *arXiv preprint*, 2013.

[50] Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):13, 2011.

[51] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi. Analysis of wormhole intrusion attacks in MANETs. *IEEE Military Communications Conference (MILCOM)*, pages 1–7, 2008.

[52] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Başar, and Jean-Pierre Hubaux. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3):25–39, 2013.

[53] Richard D McKelvey and Thomas R Palfrey. Quantal response equilibria for normal form games. *Games and economic behavior*, 10(1):6–38, 1995.

[54] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012.

[55] EC-H Ngai, Jiangchuan Liu, and Michael R Lyu. On the intruder detection for sinkhole attack in wireless sensor networks. *IEEE International Conference on Communications*, 8:3383–3389, 2006.

[56] Masaki Ogura and Victor M Preciado. Stability of spreading processes over time-varying large-scale networks. *arXiv preprint arXiv:1507.07017*, 2015.

[57] Miroslav Pajic, Shreyas Sundaram, George J Pappas, and Rahul Mangharam. The wireless control network: A new approach for control over networks. *IEEE Transactions on Automatic Control*, 56(10):2305–2318, 2011.

[58] Praveen Paruchuri, Jonathan P Pearce, Janusz Marecki, Milind Tambe, Fernando Ordonez, and Sarit Kraus. Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games. *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems*, 2:895–902, 2008.

[59] Fabio Pasqualetti, F Dorfler, and Francesco Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729, 2013.

[60] James Pita, Manish Jain, Janusz Marecki, Fernando Ordóñez, Christopher Portway, Milind Tambe, Craig Western, Praveen Paruchuri, and Sarit Kraus. Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International Airport. *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track*, pages 125–132, 2008.

[61] Robert J Plemmons. M-matrix characterizations i. Nonsingular M-matrices. *Linear Algebra and its Applications*, 18(2):175–188, 1977.

[62] Richard Poisel. *Modern Communications Jamming: Principles and Techniques*. Artech House, 2011.

[63] Radha Poovendran and Loukas Lazos. A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wireless Networks*, 13(1):27–59, 2007.

[64] Victor M Preciado, Michael Zargham, Chinwendu Enyioha, Ali Jadbabaie, and George Pappas. Optimal vaccine allocation to control epidemic outbreaks in arbitrary networks. *52nd IEEE Conference on Decision and Control (CDC)*, pages 7486–7491, 2013.

[65] David Reitter, Jens Grossklags, and Alan Nochenson. Risk-seeking in a continuous game of timing. *Proceedings of the 13th International Conference on Cognitive Modeling (ICCM)*, pages 397–403, 2013.

[66] Sheldon M Ross. *Introduction to Probability Models*. Academic Press, 2009.

[67] Fred B Schneider. Blueprint for a science of cybersecurity. *The Next Wave*, 19(2):47–58, 2012.

[68] Eric Shieh, Bo An, Rong Yang, Milind Tambe, Craig Baldwin, Joseph DiRenzo, Ben Maule, and Garrett Meyer. Protect: A deployed game theoretic system to protect the ports of the United States. *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems*, 1:13–20, 2012.

[69] Bruno Sinopoli, Luca Schenato, Massimo Franceschetti, Kameshwar Poolla, Michael Jordan, Shankar S Sastry, et al. Kalman filtering with intermittent observations. *Automatic Control, IEEE Transactions on*, 49(9):1453–1464, 2004.

[70] Ronggong Song, Peter C Mason, and Ming Li. Enhancement of frequency-based wormhole attack detection. *IEEE Military Communications Conference (MILCOM)*, pages 1139–1145, 2011.

[71] Ahren Studer and Adrian Perrig. The Coremelt Attack. In *Computer Security - Esorics*, pages 37–52. Springer, 2009.

[72] Janos Sztipanovits, Xenofon Koutsoukos, Gabor Karsai, Nicholas Kottenstette, Panos Antsaklis, Vijay Gupta, Bill Goodwine, John Baras, and Shige Wang. Toward a science of cyber–physical system integration. *Proceedings of the IEEE*, 100(1):29–44, 2012.

[73] Patrick Tague, David Slater, Radha Poovendran, and Guevara Noubir. Linear programming models for jamming attacks on network traffic flows. In *IEEE International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, pages 207–216, 2008.

[74] Marten Van Dijk, Ari Juels, Alina Oprea, and Ronald L Rivest. Flipit: The game of stealthy takeover. *Journal of Cryptology*, 26(4):655–713, 2013.

[75] Piet Van Mieghem, Jasmina Omic, and Robert Kooij. Virus spread in networks. *IEEE/ACM Transactions on Networking*, 17(1):1–14, 2009.

[76] Pradeep Varakantham, Hoong Chuin Lau, and Zhi Yuan. Scalable randomized patrolling for securing rapid transit networks. *Proceedings of the Twenty-Fifth Innovative Applications of Artificial Intelligence Conference.*

[77] Yevgeniy Vorobeychik, Bo An, Milind Tambe, and Satinder Singh. Computing solutions in infinite-horizon discounted adversarial patrolling games. *International Conference on Automated Planning and Scheduling*, 2014.

[78] Yang Wang, Deepayan Chakrabarti, Chenxi Wang, and Christos Faloutsos. Epidemic spreading in real networks: An eigenvalue viewpoint. pages 25–34, 2003.

[79] Yue Wang, Vijay Gupta, and Panos J Antsaklis. On passivity of networked nonlinear systems with packet drops. *ISIS Technical Report*, 2012.

[80] Nicholas Watkins, Cameron Nowzari, Victor Preciado, and George Pappas. Optimal resource allocation for competing epidemics over arbitrary networks. *Proceedings of the American Control Conference*, pages 1381–1386, 2015.

[81] Nicholas J Watkins, Cameron Nowzari, Victor M Preciado, and George J Pappas. Deterministic bounding systems for stochastic compartmental spreading processes. *arXiv preprint arXiv:1507.05208*, 2015.

[82] John T Wen and Murat Arcak. A unifying passivity framework for network flow control. *IEEE Transactions on Automatic Control*, 49(2):162–174, 2004.

[83] Shouhuai Xu, Wenlian Lu, and Zhenxin Zhan. A stochastic model of multivirus dynamics. *IEEE Transactions on Dependable and Secure Computing*, 9(1):30–45, 2012.

[84] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. *International Symposium on Mobile ad hoc Networking and Computing*, pages 46–57, 2005.

[85] Zhaoyan Xu, Jialong Zhang, Guofei Gu, and Zhiqiang Lin. AUTOVAC: Automatically extracting system resource constraints and generating vaccines for malware immunization, 2013.

[86] Guanhua Yan, Guanling Chen, Stephan Eidenbenz, and Nan Li. Malware propagation in online social networks: nature, dynamics, and defense implications. *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pages 196–206, 2011.

[87] Rong Yang, Fernando Ordonez, and Milind Tambe. Computing optimal strategy against quantal response in security games. *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 2*, pages 847–854, 2012.

[88] Yajin Zhou and Xuxian Jiang. Dissecting android malware: Characterization and evolution. *IEEE Symposium on Security and Privacy*, pages 95–109, 2012.

[89] Saman Zonouz, Himanshu Khurana, William H Sanders, and Timothy M Yardley. Rre: A game-theoretic intrusion response and recovery engine. *IEEE Transactions on Parallel and Distributed Systems*, 25(2):395–406, 2014.

[90] Cliff Changchun Zou, Weibo Gong, and Don Towsley. Code red worm propagation modeling and analysis. *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 138–147, 2002.

[91] Cliff Changchun Zou, Weibo Gong, and Don Towsley. Worm propagation modeling and analysis under dynamic quarantine defense. *Proceedings of the 2003 ACM workshop on Rapid malcode*, pages 51–60, 2003.

Appendix A

LIST OF PUBLICATIONS

1. P. Lee, A. Clark, L. Bushnell, and R. Poovendran, *A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems.* IEEE Transactions on Automatic Control (TAC), Special Issue on Control of Cyber-Physical Systems, Vol.59, No.12, pp. 3224-3237, 2014.

2. P. Lee, A. Clark, L. Bushnell, and R. Poovendran. *Modeling and Designing Network Defense against Control Channel Jamming Attacks: A Passivity-Based Approach.* IEEE Conference on Information Science and Systems (CISS), Workshop on Control of Cyber-Physical Systems, April 2013. **Invited Paper.**

3. P. Lee, O. Saleh, B. Alomair, L. Bushnell, and R. Poovendran. *Graph-Based Verification and Misbehavior Detection in Multi-Agent Network.* in the 3rd ACM Conference on High Confidence Networked Systems (HiCONS), Berlin, Germany, April 2014

4. P. Lee, A. Clark, B. Alomair, L. Bushnell and R. Poovendran. *Jamming-Based Adversarial Control of Network Flow Allocation: A Passivity Approach.* in American Control Conference (ACC), Chicago, July 2015.

5. P. Lee, A. Clark, L. Bushnell and R. Poovendran. *Passivity Framework for Composition and Mitigation of Multi-Virus Propagation in Networked Systems.* in American Control Conference (ACC), Chicago, July 2015.

6. P. Lee, A. Clark, B. Alomair, L. Bushnell, and R. Poovendran. *Passivity-Based Distributed Strategies for Stochastic Stackelberg Security Games.* in IEEE Conference on

Game and Decision Theory for Security (GameSec), London, UK, Nov 2015.

7. P. Lee, A. Clark, B. Alomair, L. Bushnell, and R. Poovendran. *A Host Takeover Game Model for Competing Malware.* in IEEE Conference on Decision and Control (CDC), Osaka, Japan, Dec 2015.

8. Z. Liu, A. Clark, P. Lee, L. Bushnell, D. Kirschen, and R. Poovendran *Towards Scalable Voltage Control in Smart Grid.* in International Conference on Cyber-Physical Systems (ICCPS), IEEE/ACM CPS Week, Vienna, Austria, 2016.

9. P. Lee, A. Clark, B. Alomair, L. Bushnell, and R. Poovendran. *Distributed Adaptive Patching Strategies against Malware Propagation: A Passivity Approach* in IEEE Conference on Decision and Control (CDC), Las Vegas, Dec 2016.

10. Z. Liu, A. Clark, P. Lee, L. Bushnell, D. Kirschen, and R. Poovendran *MinGen: Minimal Generator Set Selection for Small Signal Stability in Power Systems: A Submodular Framework* in IEEE Conference on Decision and Control (CDC), Las Vegas, Dec 2016.

11. P. Lee, A. Clark, B. Alomair, L. Bushnell, and R. Poovendran. *Adaptive Mitigation of Multi-Virus Propagation: A Passivity-Based Approach* under revision IEEE Transactions on Control of Network Systems (TCNS).

VITA

Phillip Lee received the B.S. (magna cum laude) degree in Electrical engineering and the M.S. degree in Electrical and Computer Engineering from the University of Washington-Seattle and University of California-San Diego in 2006 and 2009, respectively. He is a recipient of the Powell Fellowship Award in 2006. His research interests include control-theoretic modeling of cyber threats, modeling and design of cyber-physical systems and smart-grid security.