Adaptive Mitigation of Multi-Virus Propagation: A Passivity-Based Approach

Phillip Lee, Student Member, IEEE, Andrew Clark, Member, IEEE, Linda Bushnell, Senior Member, IEEE, and Radha Poovendran, Fellow, IEEE

Abstract—Malware propagation poses a growing threat to networked systems such as computer networks and cyber-physical systems. Current approaches to defending against malware propagation are based on patching or filtering susceptible nodes at a fixed rate. When the propagation dynamics are unknown or uncertain, however, the static rate that is chosen may be either insufficient to remove all viruses or too high, incurring additional performance cost. In this paper, we formulate adaptive strategies for mitigating multiple malware epidemics when the propagation rate is unknown, using patching and filtering-based defense mechanisms. In order to identify conditions for ensuring that all viruses are asymptotically removed, we show that the malware propagation, patching, and filtering processes can be modeled as coupled passive dynamical systems. We prove that the patching rate required to remove all viruses is bounded above by the passivity index of the coupled system, and formulate the problem of selecting the minimum-cost mitigation strategy. Our results are evaluated through numerical study.

I. INTRODUCTION

The growing reliance on computer networks for communication creates a corresponding increase in the threat of computer malware. A 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 [2]. Malware has been growing in sophistication, with new attack vectors targeting social networks [3] and mobile devices [4].

A variety of defense mechanisms have been developed for thwarting the spread of malware. The standard approach is to periodically patch nodes 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 nodes [6].

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 [8], [9]. 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 [11].

These uncertainties are especially pronounced when multiple malware strains propagate through a network simultaneously. The interactions between competing 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 [12]. 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 paper, we develop a passivity-based approach to modeling and mitigating multiple malware propagations, using both static and adaptive defenses. Under our approach, when an infection is detected through packet filtering or patching, the patching rate and filtering probabilities are incremented. 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 propagation dynamics. We 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. We formulate the problem of selecting the minimum-cost mitigation strategy to remove multiple viruses.
- 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 performance characteristics as functions of the update parameters.
- We evaluate our approach via numerical study. Our study compares the convergence rates under coexisting and competing malware propagation and verifies convergence of the adaptive patching and filtering dynamics to the desired steady-state.

The paper is organized as follows. Section II discusses the related work. Section III presents the adversary and defense models, and gives background on passivity. Section IV introduces a dynamical model for the multi-virus propagation and mitigation, and presents our passivity-based approach to selecting a fixed patching rate when the propagation rate is known. Section V describes and analyzes our proposed adaptive patching strategies. Section VI discusses adaptive packet filtering strategies. Section VII presents simulation results. Section VIII concludes the paper.

II. RELATED WORK

Malware propagation models have received significant research attention in recent years. Standard approaches for modeling propagation of a single malware are based on ordinary differential equation models from epidemiology, such as the Kermack-McKendrick model [15]. These models have been extensively analyzed theoretically and empirically, including applications to specific outbreaks such as the Code Red and Slammer worms [8]. 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 [16]. Multi-virus propagation has also received recent study [18], [19]. Propagation models have been developed to capture features of specific application domains, including mobile phones [4] and social networks [3]. Control-theoretic techniques for designing optimal malware propagation and attack strategies were presented in [20].

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 [9]. Geometric programming techniques for selecting the least-costly patching and vaccination rates were developed in [23]. Defenses against malware propagation in time-varying networks were considered in [7]. Recently, an optimization approach to defense against epidemics with uncertain propagation parameters was proposed [11]. 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 [2] The preliminary conference version of this work presented a passivity-based approach to modeling and mitigating multiple viruses using patching-based defenses with a fixed rate [24], but did not consider adaptive network defense.

III. MODEL AND PRELIMINARIES

This section presents the model and assumptions of the adversary and network defense. We then give background on passivity.

A. Adversary Model

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 with a fixed probability during each time interval, which we model as a Poisson process with rate $\mu_v$. The receiving host becomes infected 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 node, 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 $v$.

B. Network Defense Model

We consider two types of defense mechanisms, namely, patching and packet filtering. In the patching defense, each node $n_i$ is taken offline with a fixed probability during each time interval, which we model as a Poisson process with rate $\beta_i$, and patched against all known malwares. In the packet filtering defense, each packet that is sent from node $n_i$ to node $n_j$ is randomly forwarded with probability $q$ to an intrusion detection system, which inspects the packet for malware signatures. If such signatures are detected, all malwares are removed from the node that sent the malware packet. The parameters $\beta_i$ and $q$ vary over time, and are assumed to be set by a centralized entity with knowledge of the network topology, which is notified when a malware packet or infected node is detected.

C. Background on Passivity

This section gives background on passivity. All definitions can be found in [25].

**Definition 1:** A system is output feedback passive (OFP) if there exists a positive semidefinite function $W$ and a parameter $\rho$ such that

$$W(t) \leq \rho y(t)^T y(t) + u(t)^T y(t)$$

(1)
for all input $u$ and output $y$ for all time $t$. If $\rho = 0$, then the system is passive.

The parameter $\rho$ is defined as the output feedback passivity index of the system. If there exists a symmetric matrix $Q$ such that $W(t) \leq y(t)^TQy(t) + u(t)^TQ^Ty(t)$ then the output feedback passivity index $\rho$ is given by $\rho = \lambda_{\text{max}}(Q)$, where $\lambda_{\text{max}}$ denotes the largest eigenvalue.

**Definition 2:** Given a dynamical system $x(t) = f(x(t))$ with $x(0) = x_0$, an equilibrium point $\bar{x}$ is exponentially stable if there exist positive constants $c$ and $\alpha$ such that

$$\|x(t)\| \leq c \exp(-\alpha t)\|x_0\|$$

for all initial states $x_0$.

The following theorem gives a condition for exponential stability as well as bounds on the parameters $c$ and $\alpha$.

**Theorem 1:** Let $\dot{x}(t) = f(x(t))$ be a dynamical system with equilibrium point $\bar{x}$. Suppose that there exists a positive semidefinite function $W$ such that $W(x) = 0$ and positive constants $c_1, c_2, c_3$, and $\rho$ such that

$$c_1\|x\|^p \leq W(x) \leq c_2\|x\|^p$$
$$W \leq -c_3\|x - \bar{x}\|^p.$$

Then $\bar{x}$ is exponentially stable with rate of convergence given by

$$\|x(t)\| \leq \left( \frac{c_2}{c_1} \right)^{1/p} \exp\left(-\frac{c_3}{p}c_1 t\right)\|x_0\|.$$

IV. MULTI-VIRUS PROPAGATION DYNAMICS

In this section, a Markov model for the malware propagation and mitigation is formulated. A state-space dynamical model is then 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.

A. Markov Model and Mean-Field Approximation

The time-varying components of the system model defined in Section III consist of the set of viruses infecting each node $n_i$ at time $t$, denoted $S_i(t) \subseteq V$, as well as the patching rate $\beta_i(t)$ of each node $n_i$ 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, $S(t) = (S_1(t), \ldots, S_n(t), \beta_1(t), \ldots, \beta_n(t), q(t))$ comprises the state of the system.

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

Transitions due to the filtering process are described as follows. For any virus $v$ with $v \in S_i(t) \setminus S_j(t)$ with $n_j \in N(n_i)$, node $n_i$ sends malware packets to $n_j$ with rate $\mu^v$, which are inspected with probability $q(t)$. If the packet is inspected, then the node $n_j$ is taken offline and all viruses in $S_j(t)$ are removed, resulting in a transition from $S_i(t)$ to $\emptyset$ with rate $\lambda^v(t) \triangleq q(t)\mu^v$. The last type of transition occurs due to the patching process. This results in a transition from $S_i(t)$ to $\emptyset$ with rate $\beta_i(t)$.

The Markov model defined in this fashion has a number of states that is exponential in the number of nodes and viruses. For tractability of the computation and analysis, we introduce a mean-field approximation analogous to [15], [18]. [26]. The mean-field model is described by the states $x^S_i(t) : i \in N, S \subseteq V$, defined as the probability that node $i$ 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

$$\bigcup_{v \in S} \{(S \setminus \{v\}) \cup R : R \subseteq C_v\}.$$

Hence the net transitions into state $S_i$ are described by

$$\dot{x}^S_i(t) = \sum_{v \in S} \sum_{R \subseteq C_v} \sum_{j \in N(i)} \left[ \lambda^{S \setminus \{v\} \cup R, v} \right] x^S_i(t) \sum_{R \subseteq C_v} \sum_{j \in N(i)} \left[ -\beta_i(t) x^S_i(t) \right]$$

In the above, Eq. (2) describes transitions to $S$ due to infection, while Eq. (3) describes transitions from $S$ due to infection with viruses not in $S$. Eqs. (4) and (5) describe the impact of filtering and patching, respectively. As an approximation, we make an independence assumption that

$$\Pr(S_i(t) = S, S_j(t) = T) = x^S_i \lambda^{S \setminus \{v\} \cup R, v} x^S_j \text{T}$$

for all $i, j, S, T$. With this assumption, the dynamics of $x^S_i(t)$ are rewritten as

$$\dot{x}^S_i(t) = \sum_{v \in S} \sum_{R \subseteq C_v} \sum_{j \in N(i)} \lambda^{S \setminus \{v\} \cup R, v} x^S_i(t) \sum_{R \subseteq C_v} \sum_{j \in N(i)} (-\beta_i(t) x^S_i(t))$$

Note that, while the independence assumption is common in models of malware propagation, it is known to overestimate the propagation of a single virus [26] and underestimate the...
propagation of multiple viruses \cite{27}. In Section VII, we empirically analyze the accuracy of our approximate dynamical model.

Letting \( \pi_i^v(t) \) denote the probability that node \( n_i \) is infected with virus \( v \) at time \( t \), so that \( \pi_i^v(t) = \sum_{S} x_i^S(t) \), we have that

\[
\dot{x}_i^S(t) = \sum_{S:v \notin J \in N(i)} \lambda_{S,v} x_j^S(t) x_i^S(t) - \sum_{S:v \in J \in N(i)} \sum_{j \in J} \lambda_{S,v} x_j^S(t) x_i^S(t) - \beta_i^v(t) \pi_i^v(t).
\]

The following theorem uses the results of Lemma 1 to establish output feedback passivity of the propagation dynamics, using the storage function

\[
W_i(x) = \frac{1}{2} \sum_{S \neq \emptyset} (x_i^S)^2.
\]

**Lemma 2**: In the SIS case,

\[
W_i \leq x_i^0 Q_i x_i + \sum_{n_j \in N(n_i)} x_j^0 Q x_j + u_i^T x_i,
\]

where \( Q_i \) is a diagonal matrix with

\[
Q_i(S, S) = \frac{|N(n_i)|}{6} \sum_{v \in S} \sum_{R \subseteq S} 2|V \cap C_v| - 1 \lambda_{S,v} x_i\bigg|_{R,v}^v.
\]

**Proof**: By Lemma 1, \( W_i(x) \) is equal to

\[
\dot{W}_i = \sum_{S \in R} \sum_{v \in S} \sum_{R \subseteq C_v} \left[ \gamma_{S \setminus \{v\} \cup R \to S}(t) - \left(x_i^S \big|_{R,v}^v \right)^2 + x_i^S \big|_{R,v}^v \right]
\]

where the inequality follows from the identity \((2x_i^S \big|_{R,v}^v)^2) \geq 0 \). Since

\[
\gamma_{S \setminus \{v\} \cup R \to S}(t) = \sum_{n_j \in N(n_i)} \lambda_{S \setminus \{v\} \cup R,v} x_j^S,
\]

we have

\[
\dot{W}_i \leq \frac{1}{4} \sum_{S \in R} \sum_{v \in S} \sum_{R \subseteq C_v} \sum_{n_j \in N(n_i)} \lambda_{S \setminus \{v\} \cup R,v} x_j^S \bigg((x_i^S)^2 + x_i^S \bigg)^2
\]

by the inequality \( abc \leq \frac{1}{3} (a^2 + b^2 + c^2) \). Grouping like terms yields

\[
\dot{W}_i \leq \frac{1}{12} \sum_{n_j \in N(n_i)} \sum_{v \in V} \left[ \left( \sum_{S \neq \emptyset} \lambda_{S,v} \right) \left( \sum_{T \neq T} x_i^T \right)^2 \right] + \frac{|N(n_i)|}{6} \sum_{S \in R} \sum_{v \in S} \sum_{R \subseteq C_v} \lambda_{S \setminus \{v\} \cup R,v} (x_i^S)^2.
\]

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,

\[
Q_i(S, S) = \frac{|N(n_i)|}{6} \sum_{v \in S} 2|V| - 1 \lambda_{S\{v\}, v}.
\]
while in the competing case

$$Q_i(S, S) = \frac{|N(n_i)|}{6} \left[ \sum_{u \neq v} \lambda^{u,v} + \lambda^0_{i,v} \right].$$

In general, the passivity index in the competing case will be less than the passivity index in the coexisting case.

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 2:** The mean-field approximation of the multi-virus propagation dynamics is output feedback passive from input ($u_{i,v}$) to output (x_i: i ∈ N), with passivity index $\rho$ bounded by

$$\rho \leq \max_i \{Q_i + d_i Q\},$$

where $\lambda_{\text{max}}(\cdot)$ denotes the largest eigenvalue of a matrix.

**Proof:** Select the storage function $W(x) = \sum_{i \in N} W_i(x)$.

By Lemma 2

$$W(x) = \sum_i W_i \leq \sum_i x_i^T Q_i x_i + \sum_{i \in N} x_i^T Q_i x_i + u^T x = \sum_i x_i^T Q_i x_i + d_i x_i^T Q_i x_i + u^T x = \sum_{i \in N} x_i^T (Q_i + d_i Q) x_i + u^T x,$$

implying that the system is OFP with passivity index $\max_i \{\lambda_{\text{max}}(Q_i + d_i Q)\}$.

**C. Design of Static Mitigation Strategies**

If the compromise rates $\lambda^{S,v}$ are known for all S and v, then the results of Lemma 2 and Theorem 2 can be used to select the patching rates {β_i} while minimizing a desired cost function. The following proposition provides a sufficient condition for removal of all viruses at a desired rate $\epsilon$.

**Proposition 1:** Let $B \beta_i = \hat{\beta}_i d_i(1-x_i)$, 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

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

If $B - \overline{Q} \geq \epsilon I$, then “≥” denotes inequality in the semidefinite cone, then all viruses will be removed in steady-state and $||x(t)||_2 \leq \sqrt{n\epsilon e^{-\epsilon t}}$ for all $t \geq 0$.

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

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

Hence

$$||x(t)||_2 \leq e^{-\epsilon t} ||x||_2 \leq e^{-\epsilon t} \left( \sum_{i \in N} \left( \sum_{s \in V} x_i^S \right)^2 \right)^{1/2} \leq \sqrt{n\epsilon e^{-\epsilon t}},$$

since $\sum_s x_i^S \leq 1$.

Proposition 1 implies that an optimal patching strategy can be selecting using semidefinite programming, with the problem formulation

$$\text{minimize} \quad \sum_{i \in N} c_i(\hat{\beta}_i)$$

$$\text{s.t.} \quad B \hat{\beta} \geq \overline{Q} + \epsilon I,$$

$$\hat{\beta}_i \geq 0 \forall i$$

When the infection parameters $\lambda^{S,v}$ are known, the optimization problem (11) 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 (11), 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.

**V. PATCHING-BASED ADAPTIVE MITIGATION**

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

**A. 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 use the state dynamics of $\pi_i = \sum_s x_i^S$, defined by

$$\dot{x}_i = (1 - x_i) \sum_{n_i \in N(n_i)} \sum_{v \in V} \lambda^{0,v} \pi_j^v - \beta_i \pi_i.$$

Define $\hat{\lambda}^v = \sum_{S \subseteq S} \lambda^{S,v}$.

**Proposition 2:** The dynamics of $\pi_i$ are passive from input $(d_i \hat{\lambda} - \beta_i)$ to output $(\pi_i)^2$.

**Proof:** Define the storage function $\tilde{V}(x) = \sum_{i \in N} (\pi_i^v)^2$.

Differentiating with respect to time gives

$$\dot{\tilde{V}}(x) = \sum_{i \in N} (1 - x_i) \sum_{n_i \in N(n_i)} \sum_{v \in V} \lambda^{0,v} \pi_j^v - \beta_i (\pi_i)^2 \leq \sum_{i \in N} (1 - x_i) \sum_{n_i \in N(n_i)} \hat{\lambda} x_j - \sum_{i \in N} \beta_i (\pi_i)^2 \leq \sum_{i \in N} \sum_{j \in N(n)} \lambda x_i x_j - \sum_{i \in N} \beta_i (\pi_i)^2 \leq \sum_{i \in N} (\pi_i^v)^2 (x_j)^2 - \sum_{i \in N} \beta_i (\pi_i)^2 \leq \sum_{i \in N} (d_i \hat{\lambda} - \beta_i) (\pi_i)^2.$$ 

The existence of the storage function $\tilde{V}$ satisfying the final inequality implies passivity of $\pi_i$.

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 $\hat{\beta}_i(t)$ that is passive
from input \((\mathcal{T}_i)^2\) to output \((d_i\dot{\lambda} - \beta_i)\). One such adaptive rule is given by
\[
\hat{\beta}_i(t) = \alpha \mathcal{T}_i,
\]
for some \(\alpha > 0\), which can be implemented by incrementing \(\beta_i\) by \(\frac{\alpha}{\beta_i(t)}\) when an infection of node \(n_i\) is detected. This rule requires that \(\beta_i(0) > 0\).

**Theorem 3:** Under the patching update rule \(\hat{\beta}(t) = \alpha \mathcal{T}_i(t)\), \(\lim_{t \to \infty} \mathcal{T}_i(t) = 0\) for all \(i \in N\), implying that all malwares are removed asymptotically from the network.

**Proof:** The proof is via the LaSalle Invariance Principle. Define the energy storage function \(V(x, \beta)\) by
\[
V(x, \beta) = \sum_{i \in N} \sum_{v \in V} (\mathcal{I}^v_i)^2 + \sum_{i \in N} \sum_{v \in V} \mathcal{G}^v_i(\beta_i),
\]
where
\[
\mathcal{G}^v_i(\beta_i) = \begin{cases} \frac{1}{\beta_i} (d_i \hat{\lambda}^v - \beta_i)^2, & \beta_i \leq d_i \hat{\lambda}^v \\ 0, & \text{else} \end{cases}
\]
By inspection, \(V\) is continuously differentiable. We now show that \(\dot{V}(x, \beta) \leq 0\). By Proposition \(2\)
\[
\dot{V}(x, \beta) \leq \sum_{i \in N} \sum_{v \in V} (d_i \hat{\lambda}^v - \beta_i)(\mathcal{I}^v_i)^2 - \sum_{i \in N} \sum_{v \in V} \mathcal{G}^v_i(\beta_i)
\]
\[
= \sum_{i \in N} \sum_{v \in V} \left[ (d_i \hat{\lambda}^v - \beta_i)(\mathcal{I}^v_i)^2 - \mathcal{G}^v_i(\beta_i) \right].
\]
We will show that each term of the inner summation is bounded above by zero. If \(\beta_i \leq d_i \hat{\lambda}^v\), then, the corresponding term is given by
\[(d_i \hat{\lambda}^v - \beta_i)((\mathcal{I}^v_i)^2 - \mathcal{I}^v_i) \leq 0,
\]
since \((\mathcal{I}^v_i)^2 \leq \mathcal{I}^v_i\). On the other hand, if \(\beta_i > d_i \hat{\lambda}^v\), then the corresponding term is simply \((d_i \hat{\lambda}^v - \beta_i)((\mathcal{I}^v_i)^2 - \mathcal{I}^v_i) \leq 0\).

By the LaSalle Invariance Principle, all trajectories of \((x, \beta)\) converge to \(\{(x, \beta) : V(x, \beta) = 0\}\). We show that this set is equal to \(\{(x, \beta) : x = 0\}\). First, note that \(\dot{V}(0, \beta) = 0\) for all \(\beta\). On the other hand, \(\dot{V}(x, \beta)\) is given by
\[
\dot{V}(x, \beta) = \sum_{i \in N} \sum_{v \in V} \left[ \mathcal{I}^v_i \left( \sum_{S : v \in S} \lambda(S, v)^S \mathcal{I}^v_j \right) \sum_{n_j \in \mathcal{N}(n_i)} \mathcal{I}^v_j - \beta_i(\mathcal{I}^v_i)^2 - \mathcal{G}^v_i(\beta_i) \right],
\]
which is identically zero if and only if \(\mathcal{I}^v_i = 0\) for all \(i \in N\) and \(v \in V\).

**B. Analysis of Adaptive Patching Rate**

We now analyze the time required for the adaptive patching rate to converge to \(\hat{\beta}(t) = d_i \hat{\lambda}^v\). As an approximation, we assume that the malware propagation \(\mathcal{T}_i(t)\) instantaneously converges to a fixed point, denoted \(s^l_i(\beta)\), and that \(\mathcal{T}_i\) instantaneously converges to fixed point \(s_i\). We then have \(\hat{\beta}_i(t) = \alpha \sum_{v \in V} s^l_i(\beta)\). In order to bound the convergence rate, we derive a lower bound for \(s^l_i\) as follows. We have that
\[
(1 - s_i) \sum_{n_j \in \mathcal{N}(n_i)} \lambda(S, v)^S s_j^l - \beta_i s_i,
\]
and hence the union bound \(\sum v s^l_v \geq s_j\) implies that
\[
(1 - s_i) \sum_{n_j \in \mathcal{N}(n_i)} \lambda_{\min} s_j \leq \beta_i s_i.
\]
Summing over \(i\) and rearranging terms yields
\[
\sum_{i \in N} \lambda_{\min} d_i s_i \leq 2 \sum_{i \in N} \lambda_{\min} s_i s_j + \sum_{i \in N} \beta_i s_i
\]
\[
\leq \sum_{i \in N} d_i \lambda_{\min} s_i^2 + \sum_{i \in N} \beta_i s_i.
\]
We then arrive at the lower bound
\[
\sum_{i \in N} s_i (\lambda_{\min} d_i - \beta_i - d_i \lambda_{\min} s_i) \leq 0.
\]
Based on this inequality, we take the approximation \(s_i \geq \frac{d_i \lambda_{\min} - \beta_i}{d_i \lambda_{\min} - \beta_i}\), leading to the dynamics
\[
\dot{\beta}_i(t) = \alpha \sum_{v \in V} s_i^l \geq \alpha \sum_{v \in V} \frac{d_i \lambda_{\min} - \beta_i}{d_i \lambda_{\min} - \beta_i} (d_i \lambda_{\min} - \beta_i).
\]
The resulting lower bound on \(\beta_i(t)\) is then given by
\[
\beta_i(t) \geq \frac{\alpha m d_i}{x} + \left( \beta_i(0) - \frac{\alpha m d_i}{x} \right) \exp \left( -\frac{x}{d_i} t \right),
\]
where \(x = \sum_{v \in V} s_{\infty}^l\).

Next, we consider the final value of \(\beta_i\) that is reached after the infection rates converge to zero. The approach is to upper bound \(\mathcal{T}_i(t)\), leading to an upper bound on \(\dot{\beta}_i(t)\) and hence on \(\beta_i(t)\). Since \(\beta_i\) is nondecreasing over time, we have
\[
\dot{\mathcal{T}}_i(t) \leq \sum_{j \in N(i)} \lambda_{\max} (1 - \mathcal{T}_i) \mathcal{T}_j - \beta_i \mathcal{T}_i
\]
\[
\leq \lambda_{\max} \sum_{j \in N(i)} \mathcal{T}_j - \beta_i(0) \mathcal{T}_i
\]
which can be expressed in matrix form as \(\dot{x}(t) = (\lambda_{\max} A - B_0) x(t)\) 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
\[
\dot{x}(t) \leq e^{(\lambda_{\max} A - B_0) t} x(t) \leq e^{(\lambda_{\max} A - B_0) t} 1.
\]
Applying this bound gives
\[
\sum_{i \in N} \beta_i(t) \leq \sum_{i \in N} \alpha e^{(\lambda_{\max} A - B_0) t} 1
\]
\[
= \alpha 1^T e^{(\lambda_{\max} A - B_0) t} 1 \leq \frac{\alpha}{\mu_{\lambda}(A - B_0)} e^{(\lambda_{\max} A - B_0) t},
\]
where \(\mu_{\lambda}(A - B_0)\) denotes the maximum eigenvalue of the matrix \((\lambda_{\max} A - B_0)\). Integrating yields
\[
\sum_{i \in N} \beta_i(t) \leq \beta_i(0) + \frac{mn^2 \alpha}{\mu_{\lambda}(A - B_0)} (1 - (1 - \mu_{\lambda}(A - B_0) | t)),
\]
giving a final value \(\beta^*_i \leq \beta_i(0) + \frac{mn^2 \alpha}{\mu_{\lambda}(A - B_0)}\).

This bound depends on the value of \(\beta_i(0)\), and is valid whenever \(\beta_i(0) > \lambda_{\max} d_i\). We therefore have
\[
\sum_{i \in N} \beta_i(t) \leq \min_{\epsilon_1, \ldots, \epsilon_n} \left\{ \frac{n^2 \alpha}{\mu_{\lambda}(A - B_0)} + \sum_{i \in N} (\lambda d_i + \epsilon_i) \right\}.
\]
We apply the Gershgorin Circle Theorem to obtain a lower bound
\[ |\mu_1(\lambda A - B_0)| \geq \min \{ \epsilon_i : i = 1, \ldots, n \}, \]
so that
\[ \sum_{i \in N} \beta_i^* \leq \epsilon \left( \frac{n^2 \alpha}{\epsilon} + \lambda|E| + n\epsilon \right) = \lambda|E| + 2n\sqrt{n\alpha}. \]
This gives an average \( \beta_i^* \) value of approximately \( \lambda d_{avg} + 2\sqrt{n\alpha} \).

C. Non-Monotone Patching Strategy

The adaptive patching strategy [12] results in a patching rate that is monotone nondecreasing in time, and hence may overshoot the malware propagation rate. We now present a patching strategy that can drive the probability of infection to an arbitrarily small final value without exceeding the propagation rate \( \lambda \), in the single-virus case. The patching dynamics are defined by
\[ \hat{x}_i(t) = \frac{\alpha x_i(t) - \gamma(1 - x_i(t))}{\beta_i(t)} + \beta_i(t), \]
This patching strategy can be implemented by incrementing \( \beta_i(t) \) when an infection is detected at node \( n_i \), and decrementing \( \beta_i(t) \) when inspection of node \( n_i \) reveals that no virus is present.

Taken together with the single-virus propagation dynamics
\[ \dot{x}_i(t) = \lambda(1 - x_i(t)) \sum_{n_j \in N(n_i)} x_j(t), \]
we have that the steady-state values for the infection probability and patching rate are given by \( x_i^* = \frac{\gamma}{\alpha + \gamma} \) and \( \beta_i^* = \frac{\gamma}{\alpha + \gamma} d_i \lambda \), respectively. Hence, the probability of infection can be set arbitrarily low, and the patching rate can be set arbitrarily close to the propagation rate, by decreasing \( \frac{\gamma}{\alpha + \gamma} \).

The local stability of these patching dynamics is governed by the following theorem.

Theorem 4: The fixed point \((x, \beta)\) with \( x_i^* = \frac{\gamma}{\alpha + \gamma} \) and \( \beta_i^* = \frac{\gamma}{\alpha + \gamma} d_i \lambda \) for all \( i \in N \) is asymptotically stable.

Proof: Linearizing the system around this fixed point, we obtain the Jacobian matrix
\[ A = \begin{pmatrix} \bar{A} & -\frac{\gamma}{\alpha + \gamma} I \\ (\alpha + \gamma)I & 0 \end{pmatrix} \]
where \( I \) denotes the \( n \times n \) identity matrix and \( \bar{A} \) is defined by
\[ \bar{A}_{ij} = \begin{cases} -d_i \lambda, & i = j \\ \frac{\lambda \alpha}{\alpha + \gamma}, & n_j \in N(n_i) \\ 0, & \text{else} \end{cases} \]
We will now show that the matrix \( A \) is Hurwitz. By Lyapunov's Theorem, a necessary and sufficient condition is to construct a symmetric positive definite matrix \( P \) such that \( A^T P + PA = -\epsilon I \) for some \( \epsilon > 0 \).

First, note that \( \bar{A} \) is symmetric and is negative definite by the Gershgorin Circle Theorem. We select a matrix \( P \) as
\[ P = \left( \frac{\gamma}{\alpha + \gamma} I \right)^{-1} \left( \frac{(\alpha + \gamma)\epsilon}{\gamma} I \right) \left( \frac{(\alpha + \gamma)\epsilon}{2\gamma} I \right)^{-1} \]
with \( \tau = -\frac{1}{2} \left( \epsilon + \frac{(\alpha + \gamma)^2}{\gamma} \right) \). It can be shown that \( A^T P + PA = -\epsilon I \). Furthermore, \( P \) is symmetric since the matrices \( \bar{A} \) and \( \bar{A}^{-1} \) are symmetric. It remains to show that \( P \) is positive definite. We apply the Schur complement theorem, which states that \( P \) is symmetric if and only if
\[ \frac{\gamma}{(\alpha + \gamma)^2} \tau \bar{A}^{-1} - \left( \frac{\epsilon + (\alpha + \gamma)\epsilon}{2\gamma} \right)^2 \left( \frac{1}{\tau} \right) \bar{A} > 0 \]
where “\( > \)” denotes inequality in the positive definite cone. Eq. [14] holds since \( \bar{A} \) is negative definite and \( \tau < 0 \). After simplifying, Eq. [15] holds since \( \gamma > 0 \) and \( \bar{A} \) is negative definite. We have that there exists a positive definite matrix \( P \) such that the Jacobian matrix \( A \) satisfies \( A^T P + PA = -\epsilon I \), implying that the linearized system matrix \( A \) is Hurwitz and the fixed point is asymptotically stable.

VI. ADAPTIVE PACKET FILTERING-BASED MITIGATION

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

A. 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 nodes \( n_i \) and \( n_j \). These passivity properties are analyzed in the following proposition. As a preliminary, define \( X^v = q\mu^v \).

Proposition 3: The multi-virus propagation dynamics are passive from input \( ((\lambda v - \bar{X}^v) : v \in V) \) to output \( (y^v(t) : (i, j) \in E, v \in V) \), where
\[ y^v(t) = \sum_{(i, j) \in E} \mu^v(\pi^v_{ij}(1 - \pi^v_{ij}) + \pi^v_{ij}(1 - \pi^v_{ij})) \]
and \( \mu^v \) is the rate at which malware \( v \) sends packets to neighboring nodes.

Proof: Define a storage function by
\[ V(x) = \frac{1}{2} \sum_{i=1}^{n} \sum_{v \in V} (\pi^v_{ii})^2. \]
We then have
\[
\dot{V}(x) \leq \sum_{v \in V} \sum_{i=1}^{n} \left[ v_i \left( \sum_{j \in N(i)} \lambda^v_{max} (1 - x^v_j) x^v_j \right) - \sum_{v \in S} \sum_{j \in N(i)} u_j (1) \mu^v x^S_i (1 - x^v_j) \right]
\]
where \( \lambda^v_{max} = \max \{ \lambda^v_{S,v} : v \notin S \} \). Furthermore, we have that
\[
\sum_{v \in S} \mu^v x^S_i (1 - x^v_j) \geq \mu^v x^S_i (1 - x^v_j)
\]
for any \( v \in S \), and hence
\[
\dot{V}(x) \leq \sum_{v \in V} \sum_{i \in V} (\lambda^v_{max} (1 - x^v_j) + x^v_j (1 - x^v_j)) - \sum_{v \in V} \sum_{i \in V} \gamma u^v (1) (1 - x^v_j) + (x^v_j)^2 (1 - x^v_j).
\]
Now, since \( 2x^v_j \leq (x^v_j)^2 + (x^v_j)^2 \), we have
\[
\dot{V}(x) \leq \sum_{v \in V} \sum_{i \in V} (x^v_j)^2 (1 - x^v_j)
\]
This completes the proof of passivity.

Proposition 3 implies that the propagation dynamics are passive from input \((\lambda - \lambda)\) to output \(y\). We consider the filtering probability update rule
\[
\dot{q}(t) = \gamma \left\{ \sum_{v \in V} \sum_{i} \mu^v (1 - x^v_j) + x^v_j (1 - x^v_j) \right\}
\]
This update rule can be implemented by incrementing \(q(t)\) by \(\frac{\gamma}{\beta} \) whenever a malware packet is detected, since \(\gamma(t)\) and \(\gamma\) are known parameters at each time.

**Theorem 5:** The update rule (10) guarantees convergence of \(x^v\) to 0 for all \(i \in N\) and \(v \in V\).

**Proof:** Define a storage function \(V(x, q)\) by
\[
V(x, q) = \left\{ \begin{array}{ll}
\frac{1}{2} \sum_{i \in N} \sum_{v \in V} (x^v_j)^2 + \frac{1}{2} (q - p_{max})^2, & q < p_{max} \\
\frac{1}{2} \sum_{i \in N} \sum_{v \in V} (x^v_j)^2, & q \geq p_{max}
\end{array} \right.
\]
Then \(V(x, q)\) is bounded by
\[
\dot{V}(x, q) \leq \sum_{v \in V} \sum_{i \in V} (p^v - q)((1 - x^v_j) (x^v_j)^2 + (1 - x^v_j) (x^v_j)^2) + \sum_{v \in V} \sum_{i \in V} \mu^v (q - p^v)((1 - x^v_j) x^v_j + (1 - x^v_j) x^v_j) - \sum_{i \in N} \sum_{v \in V} \beta_i (x^v_j)^2 \leq - \sum_{i \in N} \sum_{v \in V} \beta_i (x^v_j)^2 < 0
\]
when \( q < p_{max} \) and \( \dot{V}(x, q) < 0 \) when \( q \geq p_{max} \) as well. Hence, the function \(V\) is strictly decreasing and converges to the set \(\{V = 0\}\), which occurs exactly when \(x^v_i = 0\) for all \(i \in N\) and \(v \in V\).

**B. 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.

We first analyze the time required for \(q(t)\) to approach \((p_{max}^v - \beta_i)\). Let \(\{r^v_i(q) : i \in N, v \in V\}\) denote a fixed point of \(x^v\) 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 \(x^v\) converge instantaneously to \(r^v_i\) for all \(i\) and \(v\).

Under this approximation, the dynamics of \(q(t)\) are
\[
\dot{q}(t) = \sum_{i \in V} \sum_{v \in V} \mu^v ((1 - r^v_i(q)) r^v_i(q) + (1 - r^v_i(q)) r^v_i(q)) \quad q < 1
\]
A lower bound on the convergence time is described as follows.

**Proposition 4:** The filtering probability \(q(t)\) satisfies
\[
\dot{q}(t) \leq \gamma \beta_{max} \left( \frac{n - d_{min} (n - d_{min}) \lambda_{max} - \beta_{min}}{\mu_{min} (p_{min} - q)} \right)
\]
when \(q(t) \leq p_{min}\).

The proof is omitted due to space constraints. The upper bound on \(q(t)\) can be used to analyze the time required for the filtering probability to converge to \(p_{min}\).

**Lemma 3:** If \(p_{min} \ll 1\), then the time required for the filtering probability \(q(t)\) to equal \(p_{min}\) is bounded below by
\[
\frac{p_{min}^3 \mu_{min}}{3 \gamma \beta_{max} ((n - d_{min}) \lambda_{max} - \beta_{min})}
\]
The proof is omitted due to space constraints.

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 \(\beta\). At the equilibrium \(r_i\), we have
\[
\beta \sum_i r_i = (p - q) \mu \sum_i \{r_i (1 - r_j) + r_j (1 - r_i)\}
\]
By symmetry, there exists \(r\) such that \(r_i = r\) for all \(i \in N\). Hence the approximation (17) is equivalent to \(\dot{q}(t) = \frac{\beta \gamma n \beta}{p - q}\). By symmetry, we have
\[
r = (p - q) (n - 1) \mu - \beta
\]
which implies that
\[
\dot{q}(t) \geq \frac{n \beta}{p} \left( \frac{(n - 1) p - \beta}{(n - 1) \mu - q} \right)
\]
The bound agrees exactly with (18).
C. 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 \( p_{max} \), 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 \( \gamma \) and \( \beta \).

Proposition 5: The final value of \( q(t) \) satisfies

\[
q^* \leq \min \left\{ p_{max} + m \gamma \sum_{i \in N} \frac{d_i}{\beta_i^2}, 1 \right\}.
\]

The proof is omitted due to space constraints.

VII. SIMULATION STUDY

In this section, we conduct a numerical study via Matlab. We conduct three numerical studies. First, we simulate the effectiveness of the static patching strategies when the infection rates \( \lambda \) values are known. Second, we simulate the adaptive patching strategy where the patching rate for node \( i \) is incrementally increased when the infection of node \( i \) is detected. Finally, we conduct a numerical study for the adaptive patching strategy proposed in Section V-C.

We consider a randomly generated network with 200 nodes and an average node degree of 12, where the maximum degree was 20. We assume there are two viruses \( v_1, v_2 \) propagating through the network, and the infection rates are given as \( \lambda^{I,v_1} = \lambda_1 = 1 \) and \( \lambda^{I,v_2} = \lambda_2 = 2 \) for all sets \( I \subset \{v_1, v_2\} \) in the coexisting case, and the same infection rates are given as \( \lambda^{I,v_1} = \lambda^{I,v_2} = 1 \), \( \lambda^{v_1,v_2} = 2 \) in the competing case. We assume that initially, each node is not infected with any virus with probability of 0.25, and the remaining probability is distributed uniformly at random to other states \( \sum_i x_i = 0.75 \). We also assume that each node is susceptible to all viruses.

We first evaluate the impact of mitigation strategies for different patching rates for the static patching strategy. Figure 2 shows that when the patching rate satisfies the sufficient conditions derived in Section IV-C, where the patching rate is higher than the passivity index of the propagation dynamics, the static patching strategy removes all malwares asymptotically from the network for both competing and coexisting cases.

Convergence of patching rates for the non-decreasing adaptive patching strategy for different \( \alpha \) values are shown in Figure 3 for both competing and coexisting cases. The network configuration is same as the static patching rate case, and the initial \( \beta \) values were set to 10 for all nodes.

Figure 4 verifies that the average patching value will converge to a finite final patching rate. It is illustrated that the larger values of the update parameter \( \alpha \) ensures faster convergence to the final state where no node is infected with any malware. However, the large update parameter values \( \alpha \) also result in higher final average patching rate at the equilibrium, resulting in unnecessarily high patching rates at the equilibrium.

The adaptive update rule (13) was evaluated as follows. We considered propagation of a single virus in an Erdos-Renyi random graph with \( n = 100 \) and \( p = 0.05 \). The propagation rate \( \lambda = 1 \), while \( \alpha = 1 \) and \( \gamma = 0.1 \). For each node, the 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 4(a). Each of the three trajectories converges to the fixed point \( \frac{1}{\alpha + 1} \) from the initial state. We observed this behavior in all independent trials that were run, leading us to conjecture that convergence to the desired steady-state occurs from any initial state and hence is not a purely local phenomenon. We plan to investigate this conjecture in future work. The value of the adaptive patching rates \( \beta \) is shown in Figure 4(b). As in the case of the infection probabilities \( x_i(t) \), we observed that the patching rates converged to steady-state values \( d_i \frac{1-\alpha}{\alpha+1} \lambda \) for all \( i \). On the other hand, the patching rates appeared to converge at a slower rate than the infection probabilities.

We compared the infection probability dynamics under different values of \( \alpha \) and \( \gamma \) in Figure 4(c). The figure shows the mean-square deviation of the infection probabilities from their steady-state values, defined as

\[
\sum_{i \in N} \left( x_i - \frac{\gamma}{\alpha + \gamma} \right)^2.
\]

Convergence to the steady-state occurred from random initial states for all values of the parameters. Larger values of \( \alpha \) led to faster convergence to the steady-state, even when the value...
of \( \gamma \) was increased by a promotional amount. Furthermore, we observed that the mean-square deviation was not strictly decreasing over time, although asymptotic convergence occurred in all cases.

**VIII. CONCLUSIONS**

In this paper, we investigated static and adaptive mitigation strategies against propagation of multiple competing and co-existing malware. 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.

When the propagation rates are not known a priori, we proposed adaptive mitigation strategies that vary the rate of patching a node, or the probability of filtering a packet, in response to the observed malware infections. We proposed 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 proposed an adaptive packet filtering strategy for removing all viruses.

The adaptive update strategies proposed in this paper involve each node updating its own patching rate based on its observed infection probability. In future work, we plan to investigate more adaptive strategies in which each node also leverages infection information from other nodes, including its neighbors, in order to more quickly converge to the optimal patching rate. We will also investigate generalizations to other propagation models, such as Susceptible-Infected-Recovered (SIR).

**REFERENCES**

[1] P. Wang, L. Wu, B. Aslam, and C. C. Zou, “A systematic study on peer-to-peer botnets,” *Proceedings of 18th IEEE International Conference on Computer Communications and Networks*, pp. 1–8, 2009.

[2] G. Gu, P. A. Porras, V. Yegneswaran, M. W. Fong, and W. Lee, “Bothunter: Detecting malware infection through ids-driven dialog correlation.” *Usenix Security*, vol. 7, pp. 1–16, 2007.

[3] G. Yan, G. Chen, S. Eidenbenz, and N. Li, “Malware propagation in online social networks: nature, dynamics, and defense implications,” *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pp. 196–206, 2011.

[4] Y. Zhou and X. Jiang, “Dissecting android malware: Characterization and evolution,” *IEEE Symposium on Security and Privacy*, pp. 95–109, 2012.

[5] F. B. Muhaya, M. K. Khan, and Y. Xiang, “Polymorphic malware detection using hierarchical hidden markov model,” *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, pp. 151–155, 2011.

[6] C. C. Zou, W. Gong, and D. Towsley, “Worm propagation modeling and analysis under dynamic quarantine defense,” *Proceedings of the 2003 ACM workshop on Rapid malcode*, pp. 51–60, 2003.

[7] N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Pearson Education, 2007.

[8] C. C. Zou, W. Gong, and D. Towsley, “Code red worm propagation modeling and analysis,” *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 138–147, 2002.

[9] M. Bloem, T. Alpcan, and T. Başar, “Optimal and robust epidemic response for multiple networks,” *Control Engineering Practice*, vol. 17, no. 5, pp. 525–533, 2009.

[10] C. Nowzari, V. M. Preciado, and G. J. Pappas, “Analysis and control of epidemics: A survey of spreading processes on complex networks,” *arXiv preprint arXiv:1505.00768*, 2015.

[11] S. Han, V. M. Preciado, C. Nowzari, and G. J. Pappas, “Data-driven allocation of vaccines for controlling epidemic outbreaks,” *arXiv preprint arXiv:1412.2144*, 2014.

[12] M. Bailey, E. Cooke, F. Jahanian, and D. Watson, “The blaster worm: Then and now,” *IEEE Security & Privacy*, vol. 3, no. 4, pp. 26–31, 2005.

[13] F. Castaneda, E. C. Sezer, and J. Xu, “Worm vs. worm: preliminary study of an active counter-attack mechanism,” *Proceedings of the 2004 ACM workshop on Rapid malcode*, pp. 83–93, 2004.

[14] S. Wen, W. Zhou, J. Zhang, Y. Xiang, W. Zhou, W. Jia, and C. C. Zou, “Modeling and analysis on the propagation dynamics of modern email malware,” *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 4, pp. 361–374, 2014.

[15] J. O. Kephart and S. R. White, “Directed-graph epidemiological models of computer viruses,” *IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 343–359, 1991.

[16] Y. Wang, D. Chakrabarti, C. Wang, and C. Faloutsos, “Epidemic spreading in real networks: An eigenvalue viewpoint,” pp. 25–34, 2003.

[17] A. Ganesh, L. Massoulié, and D. Towsley, “The effect of network topology on the spread of epidemics,” pp. 1455–1466, 2005.

[18] S. Xu, W. Lu, and Z. Zhan, “A stochastic model of multivirus dynamics,” *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 30–45, 2012.

[19] N. Watkins, C. Nowzari, V. Preciado, and G. Pappas, “Optimal resource allocation for competing epidemics over arbitrary networks,” *Proceedings of the American Control Conference*, pp. 1381–1386, 2015.

[20] M. H. R. Khouzani, S. Sarkar, and E. Altman, “Maximum damage
malware attack in mobile wireless networks,” *IEEE/ACM Transactions on Networking*, vol. 20, no. 5, pp. 1347–1360, 2012.

[21] W. Lu, S. Xu, and X. Yi, “Optimizing active cyber defense,” *Decision and Game Theory for Security*, pp. 206–225, 2013.

[22] M. Khouzani, S. Sarkar, and E. Altman, “Saddle-point strategies in malware attack,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 31–43, 2012.

[23] V. M. Preciado, M. Zargham, C. Enyioha, A. Jadbabaie, and G. Pappas, “Optimal vaccine allocation to control epidemic outbreaks in arbitrary networks,” 52nd *IEEE Conference on Decision and Control (CDC)*, pp. 7486–7491, 2013.

[24] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, “Passivity framework for composition and mitigation of multi-virus propagation in networked systems,” *American Control Conference (ACC)*, pp. 2453–2460, 2015.

[25] H. K. Khalil, *Nonlinear Systems*. Prentice Hall Upper Saddle River, 2002.

[26] P. Van Mieghem, J. Omic, and R. Kooij, “Virus spread in networks,” *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 1–14, 2009.

[27] N. J. Watkins, C. Nowzari, V. M. Preciado, and G. J. Pappas, “Deterministic bounding systems for stochastic compartmental spreading processes,” *arXiv preprint arXiv:1507.05208*, 2015.

[28] K. J. Aström and B. Wittenmark, *Adaptive Control*. Addison-Wesley, 1995.