# Distributed Adaptive Patching Strategies against Malware Propagation: A Passivity Approach

Phillip Lee, Andrew Clark, Basel Alomair, Linda Bushnell, and Radha Poovendran

*Abstract*— **A computer malware is a malicious code that compromises a node and then attempts to infect the node's neighbors in order to mount further attacks. Strategies for mitigating malware propagation attacks are based on patching each node at a certain rate, which is selected based on a trade-off between removing the viruses and the cost of patching. This selection, however, implicitly assumes that the propagation rate is known, whereas in practice the propagation rate depends on the inherently uncertain goals and capabilities of the attacker. In this paper, we propose and analyze adaptive defense strategies against malware with unknown propagation rates from a control-theoretic perspective. We introduce a distributed defense strategy in which each host increases its patching rate when a malware is detected, and decreases its patching rate when the host is not infected. The proposed patching strategies can drive the probability of infection to an arbitrarily low value at steady-state by varying the patching update parameters. Using a passivity-based approach, we prove that, when each node has the same patching parameters, the adaptive defense strategy ensures that the infection probabilities converge to any desired positive steady-state value. When the parameters are heterogeneous among nodes, we prove local stability of the adaptive patching dynamics, analyze the convergence rate of the infection probability, and formulate an optimization problem for selecting the infection probabilities based on a trade-off between the cost of patching and the cost of infection at steady-state. Our results are illustrated through a numerical study.**

## I. Introduction

Networked systems consist of interconnected hosts that facilitate exchange and processing of information. The growing reliance on networked systems for communication and control [1] makes them inviting targets for cyber attacks. One cyber attack on networked systems, which has been growing in frequency and sophistication is malware propagation. In malware propagation, a malicious code infects one or more hosts via software exploits and uses the infected host's resources to infect its neighboring hosts. Infected hosts may alter or drop exchanged control packets in networked control system (NCS) to severely degrade the performance, or mount large-scale denial of service attacks and spam campaign in communication networks [2].

Different mitigation strategies have been proposed against malware propagation [3]. The standard defense strategy is a patching-based mitigation, in which a host is taken offline for inspection, followed by removal of malware if an infection is detected. The inspected host, however, will be unavailable for use during the cleaning process, leading to performance degradation if the patching rate is too high.

In order to characterize the tradeoff between the performance cost due to patching and the impact of malware propagation, dynamical models have been developed to describe the propagation dynamics of malware as well as the effectiveness of the mitigation strategy [4], [5]. The dynamical models enable an analytical approach for designing efficient mitigation strategies that achieve the optimal tradeoff between patching effort and malware removal.

Analytical design of mitigation strategies, however, assumes various parameters, including scanning rates employed by malware, and the average rate of infecting neighboring nodes, are known *a priori* to the defender. In practice, however, such parameters are unknown to the defender. Mitigation strategies derived in the presence of uncertain propagation dynamics could lead to unnecessarily high patching rates or low patching rates that are insufficient to remove infection at a desired rate. At present, however, design of a mitigation strategy with unknown propagation parameters is still an open and active area of research.

In this paper, we develop adaptive patching strategies when the parameters of the propagation dynamics are unknown to the defender. The proposed patching rules are fully distributed and do not require information exchange between nodes, thus reducing communication overhead and privacy risks associated with sharing traces of infection. We prove that these update rules drive the probability of infection to an arbitrarily low value that can be tuned by varying the patching parameters, and that the asymptotic patching rate is the minimum rate required to achieve the steady-state infection probability. We make the following specific contributions:

- We propose update rules for patching rates based on the outcome of inspections for potential infection. We model the patching update as continuous dynamical system and develop coupled passive systems to represent the interaction between the propagation dynamics and adaptive patching rates.
- We characterize the equilibrium infection probabilities and patching rates, and show that the probability of infection at the equilibrium is determined only by the patching parameters chosen by the defender and does

P. Lee, L. Bushnell, and R. Poovendran are with the Department of Electrical Engineering, University of Washington, Seattle, WA 98195 USA. {leep3, lb2, rp3}@uw.edu

A. Clark is with the Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA 01609 USA. aclark@wpi.edu

B. Alomair is with the National Center for Cybersecurity Technology, King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia. alomair@kacst.edu.sa

This work was supported by ONR grant N00014-14-1-0029, ONR grant N00014-16-1-2710 and NSF grant CNS-1446866

not depend on the propagation rate of the malware. When all nodes have the same patching parameters, we prove the homogeneous patching dynamics guarantee convergence to the equilibrium point via passivity based analysis.

- In the case where nodes have heterogeneous patching parameters, we prove that the equilibrium point is asymptotically stable and characterize the convergence rate to the equilibrium as a function of the patching parameters and propagation rate. We further formulate an optimization problem of selecting patching parameters based on a trade-off between removing viruses and minimizing the cost of patching, and show that this problem is a geometric program.
- We evaluate our framework via a numerical study, which suggests that the infection probabilities converge to the equilibrium under both homogeneous and heterogeneous patching parameters.

The paper is organized as follows. We review the related work in Section II. Section III contains our assumptions of the system and malware. The dynamical models for malware propagation and patching update are also presented. In Section IV, we present our passivity-based analysis for the homogeneous patching update rules. Section V analyzes the adaptive update rule under heterogeneous patching parameters. Section VI includes our numerical results. Section VII concludes the paper.

## II. Related Work

Modeling and mitigating malware propagation have been active areas of research in both control and security communities [6]. Dynamical models of malware propagation have been developed based on epidemic models by Kermack and McKendrick [4]. The propagation models have been extended for different mitigation models including Susceptible-Infected-Susceptible (SIS) and Susceptible-Infected-Recovered (SIR) models as well as propagation of multiple different malwares [7], [8].

Control-theoretic approaches have been used to design efficient mitigation strategies as well as propagation structures of damaging malware [5], [9]. Minimizing the patching efforts while removing all infections against single virus has been studied using optimal control in [5]. Recently, a quarantine-based mitigation strategy has been studied for time-varying graphs in [10] and structures of a graph has been used to characterize the required mitigation efforts as a solution to a resource allocation in [11].

Design of mitigation strategies when the propagation parameters are uncertain have been studied in [5], [12]. Here, the defender is assumed to have *a priori* knowledge regarding the range of possible propagation parameters [12] or the statistical characteristics of parameter estimation error that is modeled as noise [5]. Existing works derive fixed patching strategies to guarantee minimum level of performance under uncertain propagation dynamics. Under our approach, the defense strategy does not depend on any prior knowledge of the propagation parameter, but instead updates the patching rate based on the detected infection during the inspection process.

Passivity-based control design has been used in applications including congestion control [13] and control of cyber-physical systems [14]. One advantage of passivity-based design is that a class of control laws that guarantee stability can be identified using the passive structure. Since any controller that is passive will guarantee stability, a control law can be chosen that is robust to noise or delay [13].

In [15], we studied adaptive patching strategies where each host updates its patching rate based on the outcomes of inspections. This preliminary work proved local convergence under a linearized model around the equilibrium point, but did not contain results for global convergence. In addition, the tradeoff between the patching effort and the probability of infection has not been studied for the adaptive patching strategies.

## III. Model and Preliminaries

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

### A. Adversary and Defense Models

We consider a networked system represented by an undirected graph $G = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of hosts and $\mathcal{E}$ is the set of edges between hosts. We assume that an infected host $i \in \mathcal{V}$ can infect node $j$ only if $j$ is a neighboring node of $i$, i.e., $(i, j) \in \mathcal{E}$. The set of neighboring nodes of node $i$ is denoted as $N_i$, and the number of neighbors of host $i$ is denoted as $d_i = |N_i|$.

We consider patching based mitigation strategy where each host $i$ is taken offline according to a Poisson process with rate $\beta_i$. Once a host is taken offline, it is inspected for infection and patched if it is infected. In this paper, we assume that through inspection, any malicious code can be detected and removed with certainty. The rate $\beta_i$ can be varied over time, based on observed infections at one or more nodes.

We assume Susceptible-Infected-Susceptible (SIS) model [16] where a patched node can be reinfected at a later time. This model is consistent with recent advances in malware including polymorphic worms where a malware mutates its code over time to avoid signature-based detection [17].

### B. Malware Propagation Dynamics

We consider the mean-field approximation to the SIS model, defined as follows [18]. Let $x_i(t)$ denote that probability that node $i$ is infected at time $t$. With the additional approximation that the state of node $i$ is independent of the state of node $j \in N_i$ at time $t$, the mean-field approximation yields the dynamics of $x_i(t)$ as

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

where $\lambda > 0$ is a propagation rate that is determined by the rate at which an infected node attempts to infect its neighbors and the probability that an infection attempt is successful.

We assume that the propagation rate $\lambda$ is unknown to the defender. The first term describes the transition of node $i$ becoming infected and the second term describes the transition of node $i$ becoming susceptible via patching.

### C. Background on Passivity

This section gives background on passivity. All definitions can be found in [19].

*Definition 1:* A dynamical system $\Sigma : \dot{x} = f(x, u), y = h(x, u)$ is *passive* if there exists a positive semidefinite function $V(x)$ (Storage function) such that

$$\dot{V}(t) \leq u(t)^T y(t) \tag{2}$$

for all input $u$ and output $y$ for all time $t$. If in addition, $\dot{V}(t) \leq u(t)^T y(t) - W(x(t))$ for some positive definite function $W$, then the system $\Sigma$ is called *strictly passive*.

*Theorem 1 ([19]):* A negative feedback interconnection between two strictly passive systems is globally asymptotically stable.

For a negative feedback interaction between two strictly passive systems with storage functions $V_1$ and $V_2$, the function $V = V_1 + V_2$ is a Lyapunov function for the combined system.

## IV. 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 (1) and prove the global asymptotic convergence to the equilibrium point under the proposed adaptive patching strategy via passivity analysis.

### A. 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 $\frac{\alpha}{\beta_i(t)}$. Similarly, if the inspection of node $i$ reveals that no malware is present, then the patching rate is decremented by $\frac{\gamma}{\beta_i(t)}$. Since the patching rate for host $i$ will be incremented at the rate $\beta_i(t)x_i(t)$, since the expected rate of increment is $\frac{\alpha}{\beta_i(t)} \cdot \beta_i(t)x_i(t) = \alpha x_i(t)$, and the expected rate of decrement is $\gamma(1 - x_i(t))$ by the same logic, the overall dynamics of patching rate $\beta_i(t)$ is given as

$$\dot{\beta}_i(t) \quad = \quad \{\alpha x_i(t) - \gamma(1 - x_i(t))\}^+_{\beta_i}. \tag{3}$$

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 (1) and (3).

*Theorem 2:* 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 (3) with the propagation dynamics (1). The first equilibrium is $(x_i^*, \beta_i^*)$ 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 $\dot{\bar{\beta}}_i = 0$ 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.

$$\lambda(1 - \bar{x}_i) \sum_{j \in N_i} \bar{x}_j = 0. \tag{4}$$

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 $(x_i^*, \beta_i^*)$, we verify by substituting $x^*$ as $x_i$ for all $i$ and $\beta_i = \beta_i^*$ in the propagation and patching dynamics. We obtain

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

for all $i$.

■

While $(x^*, \beta^*)$ 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 $(x^*, \beta^*)$ when at least one host is initially infected with non-zero probability.

### B. Passivity-Based Analysis of Homogeneous Patching

We prove convergence to $(x^*, \beta^*)$ 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 $(x^*, \beta^*)$, guaranteeing the global asymptotic stability of the overall system as illustrated in Figure 1.

*Lemma 1:* 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

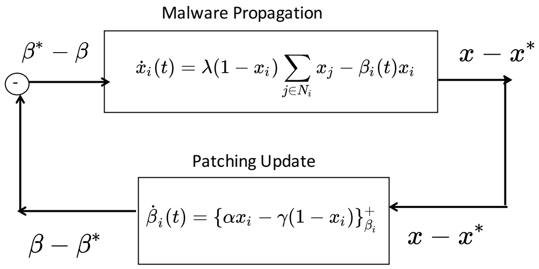

Malware Propagation
$\beta^* - \beta$
-
$\dot{x}_i(t) = \lambda(1-x_i)\sum_{j\in N_i} x_j - \beta_i(t)x_i$
$x - x^*$
Patching Update
$\dot{\beta}_i(t) = \{\alpha x_i - \gamma(1-x_i)\}^+_{\beta_i}$
$x - x^*$
$\beta - \beta^*$

Fig. 1. 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.

$g(x_i, x_j)$ yields

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

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

$$\max_{x_i, x_j \geq 0} g(x_i, x_j) \tag{5}$$

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), 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 3:* 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

$$V_1(\mathbf{x}) = \sum_i \left(x^* \log \frac{x^*}{x_i} + (x_i - x^*)\right) \tag{6}$$

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

$$\nabla^2_{\mathbf{x}} V_1 = diag(\frac{x^*}{x_i^2}) > 0 \tag{7}$$

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 $i$th 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 $\beta_i^*$ term inside the parenthesis, and rearranging the terms, we obtain

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

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

$$\sum_i (x_i - x^*)\left((\frac{1}{x_i} - 1)\sum_{j\in N_i} x_j - (1-x^*)d_i\right) \tag{8}$$

$$= \sum_i (x_i - x^*)\left(\sum_{j\in N_i}(\frac{x_j}{x_i} - x_j - 1 + x^*)\right) \tag{9}$$

$$= \sum_{(i,j)\in\mathcal{E}} [(x_i - x^*)(\frac{x_j}{x_i} - x_j - 1 + x^*) \tag{10}$$

$$+(x_j - x^*)(\frac{x_i}{x_j} - x_i - 1 + x^*)] \tag{11}$$

However, each term of (11) is less than 0 for all $(i,j) \in \mathcal{E}$ due to Lemma 1, implying that $\dot{V}_1 < -\sum_i (x_i - x_i^*)(\beta_i - \beta_i^*)$ and the system is passive. ■

Theorem 3 establishes the passivity of the propagation dynamics. We will now prove the passivity of homogeneous patching dynamics.

*Theorem 4:* 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

$$V_2(\beta) = \frac{1}{2(\alpha+\gamma)}(\beta - \beta^*)^T(\beta - \beta^*) \tag{12}$$

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 3 and 4 show the passivity of both propagation 1 and patching dynamics 3. Using these results, we now show that $x_i(t)$ will converge to $x^*$ for all $i$.

*Theorem 5:* 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 $\beta_i^*$ for all $t$.

*Proof:* Using the storage functions $V_1(\mathbf{x})$ and $V_2(\beta)$ from Theorems 3 and 4 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 1. From Lemma 1, 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 [19], 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 $\mathbf{x}(0) \neq 0$. ■

## V. Heterogeneous Patching Strategy

In Section IV, 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 tradeoff the patching effort and the impact of infection.

### A. 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 $\alpha_i$ and $\gamma_i$ vary for each host. Similarly as in (3), the heterogeneous patching dynamics is given as

$$\dot{\beta}_i(t) = \{\alpha_i x_i(t) - \gamma_i(1 - x_i(t))\}^+_{\beta_i} \tag{13}$$

*Theorem 6:* An equilibrium of heterogeneous patching dynamics together with the propagation dynamics (1) is given as

$$x_i^* = \frac{\gamma_i}{\alpha_i + \gamma_i}, \quad \beta_i^* = \lambda(\frac{1}{x_i^*} - 1)\sum_{j\in N_i} x_j^* \text{ for all } i \tag{14}$$

*Proof:* The patching dynamics is at equilibrium when $x_i^* = \frac{\gamma_i}{\alpha_i+\gamma_i}$. Substituting $x_i^*$ in the (1), 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 $(x_i^*, \beta_i^*)$.

*Theorem 7:* The equilibrium point $(x_i^*, \beta_i^*)$ is asymptotically stable.

*Proof:* Linearizing the propagation dynamics (1) around the equilibrium point $(x_i^*, \beta_i^*)$, we obtain

$$\dot{\bar{\mathbf{x}}} = A\bar{\mathbf{x}} + B\bar{\beta} \tag{15}$$

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 (13) around the equilibrium point, we obtain

$$\dot{\bar{\beta}} = K\bar{\mathbf{x}} \tag{16}$$

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

Since all off-diagonal entries of $A$ are positive, from [20], 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 $i$th 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

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

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

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 $\beta_i^*$ is not a convex function in $\mathbf{x}^*$. However, if we assume that $x_i^* \ll 1$ for all $i$ then the patching rate $\beta_i^*$ 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 $\beta_i^*$. The optimization problem of minimizing a trade-off between the probability of infection and the patching cost at the equilibrium can be formulated as

$$\begin{array}{ll}\text{minimize} & \sum_i c_i x_i^* + \lambda \sum_i \sum_{j \in N_i} x_j^*(x_i^*)^{-1} \\ \text{s.t.} & x_i^* \in (0, 1]\end{array} \qquad (17)$$

where $c_i > 0$ is a positive constant to trade-off the probability of infection at host $i$. The optimization problem (17) is is a geometric program [21], and hence can be solved efficiently using convex optimization algorithms for a large network. Note that the objective function of (17) includes parameter $\lambda$, which is assumed to be unknown. Hence, a nominal value or probability distribution over $\lambda$ can be used in the objective function. While an inaccurate estimate of $\lambda$ will lead to suboptimal values of $x^*$, it will not impact the convergence properties of the adaptive update rule.

### *B. 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 $(x^*, \beta^*)$. 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 $\alpha_i$. 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 7, 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 2:* Let $\Lambda$ denote the set of eigenvalues of $A$. The eigenvalues of the Jacobian $J$ are given as

$$\overline{\Lambda} = \left\{\frac{\eta \pm \sqrt{\eta - 4\gamma}}{2} : \eta \in \Lambda\right\}. \qquad (18)$$

*Proof:* The characteristic polynomial of $J$ is given by

$$\Delta_J(\rho) = \det\left(\begin{array}{cc} A - \rho I & B \\ C & -\rho I\end{array}\right).$$

The matrices $C$ and $-\rho I$ commute, and hence the characteristic polynomial is equivalent to $\Delta_J(\rho) = \det((A - \rho I)(-\rho I) - BC)$ [22]. 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 $\rho$ where $\rho + \frac{\gamma}{\rho} = \eta$ for some eigenvalue $\eta$ of $A$. Solving for $\rho$ gives the desired result. ■

We now derive bounds on the eigenvalues of $A$.

*Lemma 3:* Let $\eta$ 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

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

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

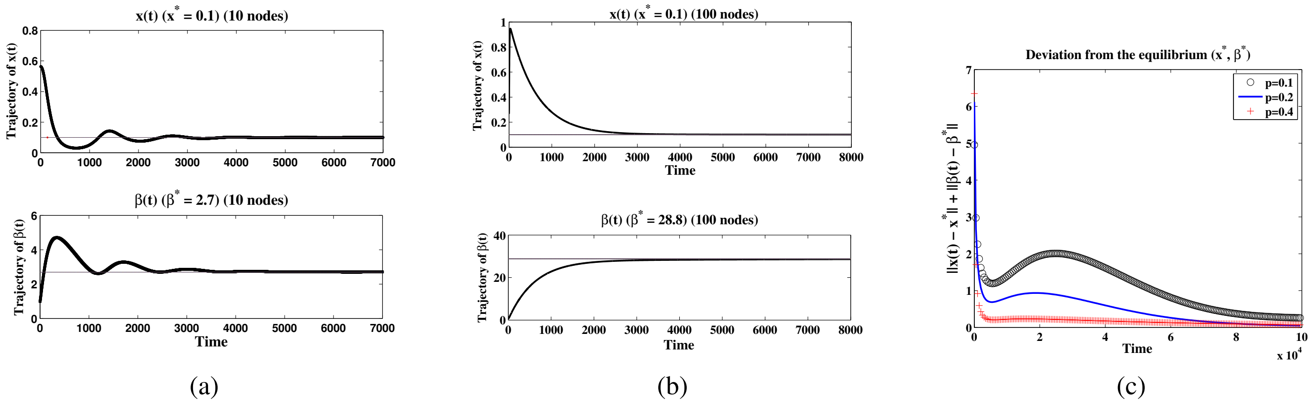
$$\begin{aligned}||D^{-1}ADv||_2 &\leq ||D^{-1}||_2||ADv||_2 \leq \frac{1}{\max_i D_{ii}}||AD||_2||v||_2 \\ &\leq \frac{1}{\max_i x_i^*}\lambda \min_i (x_i^*)^2||v||_2\end{aligned}$$

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 2 and 3 yields the following.

*Theorem 8:* The magnitudes of the real parts of the eigenvalues of $J$ are bounded below by

$$\rho^* = \frac{\eta^* - \sqrt{(\eta^*)^2 - 4\gamma}}{2}, \qquad (19)$$



(a)

(b)

(c)

Fig. 2. Figures illustrating convergence of $x(t)$ and $\beta(t)$ to $x^*, \beta^*$ for adaptive patching strategies. (a) Trajectories of $x(t)$ and $\beta(t)$ for a network with 10 nodes (b) Trajectories of $x(t)$ and $\beta(t)$ for a network with 100 nodes. (c) Convergence of $x(t)$ and $\beta(t)$ for heterogeneous patching strategy. Random networks of 50 nodes were generated for the heterogeneous patching strategies.

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

*Proof:* By Lemma 2, the eigenvalues of $J$ are defined by Eq. (18). The eigenvalue with smallest real part occurs when $|\eta|$ is minimized. Substituting the bound $\eta^*$ from Lemma 3 yields Eq. (19). ■

From Theorem 8, we observe that convergence rate is increasing in $\gamma$ and $\eta^*$. The value of $\eta^*$, in turn, is increasing in $\min_i x_i^*$, increasing in $\lambda$, and decreasing in $\max_i x_i^*$. Hence the convergence rate is maximized when $\gamma$ 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.

## VI. Numerical Study

We evaluated our approach through a Matlab numerical study. We considered randomly generated Erdos-Renyi graphs where an edge exists between two nodes with probability $p$ independent from other edges. In our simulation, edge probability $p$ was chosen as 0.3.

We evaluated both the homogeneous and the heterogenous patching update rules. For the homogeneous case, parameters $\alpha, \gamma$ were chosen as $\alpha = 9$ and $\gamma = 1$. From Theorem 2, $x^* = 0.1$ for all hosts and the steady state patching rate for host $i$ is given as $\beta_i^* = \lambda(1 - x^*)d_i$.

For the homogeneous patching update, we generated two networks of size 10 and 100. Convergence of $x(t)$ and patching rate $\beta(t)$ for the homogeneous patching update is illustrated in Figure 2. A random host was chosen to evaluate $x_i(t)$ and $\beta_i(t)$.

For a network with relatively small number of hosts ($\mathcal{V} = 10$), we observe that the probability of infection and patching rate exhibit oscillatory behavior around the equilibrium point, but asymptotically converge to $x^*, \beta_i^*$ as shown in Figure 2(a). Figure 2(b) shows the convergence of $x_t$ and $\beta_i(t)$ for a larger network of size 100. We observe that as the network size increases, the convergence of state variables become monotonic as compared to the oscillatory behavior exhibited in small-sized networks.

Numerical evaluation of heterogeneous patching update is shown in Figure 2(c). Three networks were generated with 50 nodes by varying the connectivity parameter $p$ as $p = 0.1, 0.2, 0.4$. Initial values of $x_i(t)$ were chosen uniformly random, while the initial $\beta_i(t)$ values were chosen by introducing a small perturbation from $\beta^*$ by adding independent Gaussian random variables of variance 0.1. The metric for deviation from the equilibrium was chosen as $||\mathbf{x}(t) - \mathbf{x}^*||_2 + ||\beta(t) - \beta^*||_2$.

Figure 2 (c) shows that for arbitrary initial values of $x_i(0)$, the deviation converges to 0 for all three cases. This numerical result implies that global convergence of heterogeneous patching dynamics is feasible and maybe proved by constructing an appropriate Lyapunov function. It is observed that the deviation norm is not monotonically decreasing in general. However, as the connectivity parameter increases, the convergence rate increases and the trajectory of deviation becomes more monotonic as $p$ increases. We observe that this trend is analogous to the homogeneous patching case, where the convergence rate is improved as the average degree of the network increases. Investigating this trend analytically will be part of our future work.

## VII. Conclusions

In this paper, we studied distributed adaptive patching strategies against malware propagations attack when the system defender does not have a prior knowledge of the propagation rate of the malware. We proposed two update rules depending on whether the same patching update rule is applied to every host in the network. We modeled the patching update as continuous dynamical systems that are coupled with propagation dynamics and characterized equilibria points for both update rules.

Using passivity-based analysis, we proved that by allowing non-zero, but arbitrarily low probability of infection at the steady state, the homogeneous patching rule guarantees global convergence to the characterized equilibrium if at least one host is infected initially in the network. For the heterogeneous update, we proved the asymptotic convergence to the equilibrium by linearizing the propagation and patching dynamics around the equilibrium. In order to achieve the optimal trade-off between the impact of infection and the patching efforts for each node under the heterogeneous patching dynamics, we formulated a geometric optimization problem that can be solved efficiently for a large network.

For future work, we will consider patching update rules that are robust to errors (false alarms and mis-detections) during inspections by tuning the update parameters. Moreover, if each host has varying defense capabilities, then the propagation rate would depend on which host the malware is targeting. We will incorporate heterogeneous propagation rate as part of future work. Finally, we will investigate the global convergence properties of the heterogeneous patching update rules.

## References

[1] T. C. Yang, “Networked control system: a brief survey,” *IEE Proceedings Control Theory and Applications*, vol. 153, no. 4, p. 403, 2006.

[2] D. Dagon, G. Gu, C. P. Lee, and W. Lee, “A taxonomy of botnet structures,” *Computer Security Applications Conference*, pp. 325–339, 2007.

[3] M. Bailey, J. Oberheide, J. Andersen, Z. M. Mao, F. Jahanian, and J. Nazario, “Automated classification and analysis of internet malware,” in *Recent Advances in Intrusion Detection*. Springer, 2007, pp. 178–197.

[4] 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.

[5] 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.

[6] P. Gutmann, “The commercial malware industry,” *DEFCON conference*, 2007.

[7] 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.

[8] 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.

[9] 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.

[10] P. E. Par, C. L. Beck, and A. Nedi, “Stability analysis and control of virus spread over time-varying networks,” *Conference on Decision and Control (CDC)*, pp. 3554–3559, 2015.

[11] K. Drakopoulos, A. Ozdaglar, and J. N. Tsitsiklis, “A lower bound on the performance of dynamic curing policies for epidemics on graphs,” *arXiv preprint arXiv:1510.06055*, 2015.

[12] 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.

[13] J. T. Wen and M. Arcak, “A unifying passivity framework for network flow control,” *IEEE Transactions on Automatic Control*, vol. 49, no. 2, pp. 162–174, 2004.

[14] J. Sztipanovits, X. Koutsoukos, G. Karsai, N. Kottenstette, P. Antsaklis, V. Gupta, B. Goodwine, J. Baras, and S. Wang, “Toward a science of cyber–physical system integration,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 29–44, 2012.

[15] P. Lee, A. Clark, B. Alomair, L. Bushnell, and R. Poovendran, “Adaptive mitigation of multi-virus propagation: A passivity-based approach,” *arXiv preprint: 1603.04374*, 2016.

[16] R. Pastor-Satorras and A. Vespignani, “Epidemic spreading in scale-free networks,” *Physical review letters*, vol. 86, no. 14, p. 3200, 2001.

[17] Z. Xu, J. Zhang, G. Gu, and Z. Lin, “Autovac: Automatically extracting system resource constraints and generating vaccines for malware immunization,” IEEE, pp. 112–123, 2013.

[18] R. Pastor-Satorras and A. Vespignani, “Epidemic dynamics in finite size scale-free networks,” *Physical Review E*, vol. 65, no. 3, p. 035108, 2002.

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

[20] R. J. Plemmons, “M-matrix characterizations i. Nonsingular M-matrices,” *Linear Algebra and its Applications*, vol. 18, no. 2, pp. 175–188, 1977.

[21] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge university press, 2004.

[22] J. R. Silvester, “Determinants of block matrices,” *The Mathematical Gazette*, vol. 84, no. 501, pp. 460–467, 2000.