Visibility-Aware Optimal Contagion of Malware Epidemics

Soheil Eshghi, Saswati Sarkar, and Santosh S. Venkatesh

***Abstract*—Recent innovations in the design of computer viruses have led to new trade-offs for the attacker. Multiple variants of a malware may spread at different rates and have different levels of visibility to the network. In this work we examine the optimal strategies for the attacker so as to trade off the extent of spread of the malware against the need for stealth. We show that in the mean-field deterministic regime, this spread-stealth trade-off is optimized by computationally simple single-threshold policies. Specifically, we show that only one variant of the malware is spread by the attacker at each time, as there exists a time up to which the attacker prioritizes maximizing the spread of the malware, and after which she prioritizes stealth.**

***Index Terms*—Computer virus, inter-node, malware.**

I. Introduction

Malware (i.e., viruses, worms, trojans, etc.) has been a prominent feature of computer networks since the 1980's [1], and has evolved with the growing capabilities of computing technology. More recently, the focus has shifted to more "surgical" strikes where visibility is highly undesirable, as awareness can lead the intended target to cease communication (e.g., by quarantining the targets) [2]–[6]. Thus there is a new **critical** trade-off for the attacker—to ensure maximum damage while minimizing visibility to the defender.

Malware spreads from one computing device to another when there is a communication opportunity between the devices. In networks, both wired and wireless, inter-node communication can be visible to the network administrator, and can serve as a way of detecting the presence of malware before its function is fully understood. However, the attacker also has a conflicting onus to ensure the rapid propagation of her program, as the exploit(s) that the malware targets will be noticed and patched in due course. Thus, an attacker will seek to minimize her communication footprint while still trying to ensure the timely spread of the malware.

In particular, we consider the case where two variants of a single emerging malware spread in a network that is unaware of their existence. One spreads aggressively in every contact, and is thus visible to the network due to its communications, while the other, passive, variant does not spread subsequent to infecting a node. We assume that the network cannot determine the infection state of any particular node and does not have patches to remedy the attack, but can detect an attack by looking at the unusual communication patterns resulting from malware spread at a network scale. The natural question that arises is to characterize the structure of the optimal malware variant mix that the attacker will spread at each instant depending on their goal structures and the communication mechanisms that they may have at their disposal. This is an imperative first step to devising remedies for such attacks.

Manuscript received March 31, 2016; revised October 29, 2016; accepted November 8, 2016. Date of publication November 23, 2016; date of current version September 25, 2017. Recommended by Associate Editor D. Hristu-Varsakelis.

S. Eshghi is with the Electrical Engineering Department, Yale University, New Haven, CT (e-mail: soheil.eshghi@yale.edu).

S. Sarkar and S. S. Venkatesh are with the Electrical and Systems Engineering Department, University of Pennsylvania, Philadelphia, PA (e-mail: swati@seas.upenn.edu; venkates@seas.upenn.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2016.2632426

A. Problem Description

We consider a network under attack by these two variants of a malware. Depending on their infection status, nodes can be divided into 4 groups: Germinators (G), Susceptibles (S), Zombies (Z), and Passives (P):

1) *Germinators* (G), the only nodes under the attacker's direct control, are a *fixed* (potentially very small) fraction of nodes. Germinators are the only nodes that can *choose* how to interact with susceptibles and zombies depending on the goal of the attacker: at each encounter with a susceptible, they decide whether to turn it into a zombie or a passive, or to leave it as a susceptible. They damage the network by executing malicious code but are visible to the network due to their communications.

2) *Susceptibles* (S) are nodes that have not received any variant of the malware. Upon receipt of the malware from germinators, they can turn into zombies (Z) or passives (P). Upon receipt of the malware from zombies, they will turn into zombies (Z).

3) *Zombies* (Z) have received the aggressive malware variant and upon meeting a susceptible, will turn into a zombie. They damage the network by executing malicious code, and are visible to the network due to their communications. In the augmentation in § III-B, the additional mechanism of *halting* can turn zombies into passives.

4) *Passives* (P) have received the passive variant of the malware, and will *not* propagate it any further, making them *invisible* to the network. They damage the network by executing malicious code.

We assume that all nodes mix *homogeneously* (i.e., contacts between nodes are independent and exponentially distributed) with rates that only depends on the infection states of the two nodes. This abstraction simplifies the interaction model for analysis in the population limit.

In these models, the attacker *controls* the mixture of zombie and passive malware variants through the germinators under its direct control. Whenever a germinator meets a susceptible, based on the control chosen by the attacker, it spreads either the zombie or passive variant of the malware to the susceptible, or leaves it as it is. In the dynamics in § IV-B, the germinator has an additional controlled mechanism of action, whereby upon meeting a node with the zombie variant of the malware, it can replace the variant with the passive one (a "halting" mechanism). These controls are assumed to be *piecewise continuous*, but they can take any value between zero and one, which determines the percentage of relevant interactions for which the specified action happens.

Later, we also investigate the effect of defense strategies on the optimal spread of malware variants (§ III-C). In these defense strategies, the defender limits the effective contacts of nodes using a pre-determined function of malware visibility (which changes over time) as a means

to limit the spread of malware. We consider two classes of network defense functions: affine and sigmoid. These defense strategies, however, come at the cost of stopping legitimate communication within the network. This is akin to choosing the communication ranges of nodes as a decreasing function of the visibility of the malware, which is a form of *quarantine*.

We allow the attacker to choose the malware spreading controls so as to maximize a measure of overall damage (described in § III-E). We first consider a damage function that depends on a) malware efficacy, which is a function of the aggregate number of zombies and passives, and b) malware visibility, which is a function of the number of zombies (for the models in § III-A and § III-B). Then, we consider a damage function where malware efficacy is the attacker's only direct concern, and is thus the damage function to be maximized, for the case where visibility is built into the network dynamics through a network defense policy which is a function of the fraction of zombies (as in the model in § III-C).

B. Results

We then derive necessary structures for optimal solutions for each of the cases, using Pontryagin's Maximum Principle and custom arguments constructed for each case (in § IV). We show that the attacker's optimal strategy in all of these models is for the germinators to spread only one variant of the epidemic at each time: the germinators will create zombies up to a certain threshold time, and then only create passives (including by halting zombies) from then on. That is, the optimal controls are *bang-bang* (i.e., only taking their minimal and maximum values) with only one jump.

It is interesting to note that in each of the variations we consider, our analysis reveals that all the controls in each model have the same threshold, a fact that is not at all clear *a priori*. Thus the entire control space can be described by one time threshold. This structure is invaluable for deriving the optimal controls computationally (by solving the scalar optimization problem with the state ODEs mapping the variable to the damage objective). Furthermore, the controls are deterministic and easy to implement as the germinators need to be programmed with just one time instant for all of their controls.

II. Literature Review

The *key* distinction between the control of biological epidemics [7]–[11] and that of malware ones is that in malware epidemics the *attacker* can also decide to *use her resources optimally* and to *adapt* to foresee the response of the defender. Within the majority of malware epidemic models, e.g., [12]–[18], the spread of *only one* malware has been examined, while we focus on the case where two variants are spreading in conjunction with each other. Furthermore, in these papers it is assumed that the attacker's sole aim is to maximize the spread of the malware, which is no longer the case for the emerging class of surgical malware such as Regin [2] and Stuxnet [3] or malware designed for continuous stealthy operation like Bitcoin mining botnets [19].

Among the work on the control of a single-type/variant of malware (and the closely related literature on the spread of a message in Delay Tolerant Networks [20], [21] and the spread of a rumor [22]), the closest work to this topic (in terms of approach and spreading models) was in two papers [18], [23]. In both papers, however, the authors assume that the malware can control the transmission range of infected nodes and *patching* is the major defense of the network and starts as soon as the epidemic spreads. Furthermore, the adaptive defense model and the results on the simultaneity of 3 optimal control switching times for the halting model are without precedent in the literature.

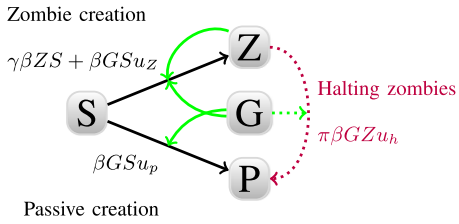

Fig. 1. The blocks represent the 4 states of nodes with regard to the malware. The solid black lines show the dynamics in § III-A with the transition rates super-imposed. The green arrows point from each source of malware to the resulting transition. The dotted red lines show the additional halting action in § III-B. The model in § III-C has the same dynamics as the solid black lines, but with β being a function of Z (i.e., $\beta(Z)$).

III. System Model and Objective Formulation

In this section we model the spread of malware in a homogeneous network with random contacts. This can be the case where malware spreads among mobile devices with proximity-based communication, or where random contacts in an address-book are utilized. The virus propagates in the network between times 0 and T. We represent the fraction of *susceptible*, *germinator*, *zombie*, and *passive* nodes at time t with $S(t)$, $G(t)$, $Z(t)$, and $P(t)$ respectively, and assume that they are differentiable functions of time. We assume that for any pair of states, the statistics of meeting times between all pairs of nodes of those two states are identical and exponentially distributed, where the mean is equal to the *homogeneous mixing rate* of those two states. It has been shown [24], [25, p.1] that the resulting evolution of such a set of state fractions (where state transitions occur according to a Poisson contact process) will converge pathwise to the solution of a set of ordinary differential equations derived from the dynamics in the population limit (i.e., in the mean-field) on any limited time period (in particular, including the transient phase).

We describe the state dynamics of such systems as an epidemic for the cases where: 1) germinator agents can only interact with susceptible agents (§ III-A), 2) germinator agents can also interact with zombies as well (§ III-B), and 3) effective network contact rates are a function of the infection spread, mirroring the response of a network defender (§ III-C) (Fig. 1). We state and prove a key observation about all these dynamics (§ III-D). We next formulate the aggregate damage of attack efficacy and the ensuing visibility (§ III-E). Finally, we lay out the optimization problem in § III-F.

A. SGZP Model With No Halting

The attacker can spread the malware in two ways: 1- upon encountering a susceptible, she can, through the control variable $u_Z(t)$, turn that susceptible node into a zombie, i.e., one that will henceforth propagate that infection to susceptibles it meets. 2- upon encountering a susceptible, she can, through the control variable $u_P(t)$, turn that susceptible into a *Passive*, P. These control variables—$(u_Z, u_P) \in \mathcal{U}$, where $\mathcal{U}$ is the set of piecewise continuous controls—can be thought of as the probabilities that an interaction of a germinator and a susceptible at time t will lead to the susceptible becoming a zombie and a passive respectively. To maintain such a probabilistic intuition, we constrain their sum to be less than one.

$$\dot{S} = -\beta GS(u_P + u_Z) - \gamma\beta ZS \tag{1a}$$

$$\dot{Z} = \beta GSu_Z + \gamma\beta ZS \tag{1b}$$

$$\dot{P} = \beta GSu_P \tag{1c}$$

$$u_P + u_Z \leq 1 \tag{2a}$$

$$0 \leq u_P \leq 1 \; 0 \leq u_Z \leq 1 \tag{2b}$$

Here, β is the mixing rate between S and G (which the attacker can calculate using time averages of contact times), and $\gamma\beta$ is the mixing rate between Z and S (with $\gamma > 0$). Thus, γ is the relative secondary rate of spread of the malware. We consider all values of the parameter γ, with an associated trade-off: if γ is high, the zombies spread fast and increase visibility, while if γ is low, the malware does not spread to cause significant damage.

B. SGZP Model With Halting

This model is akin to the previous one, with one more mechanism added: germinator nodes (G) can force a zombie (Z) to become passive (P) through a process we will call "halting". This happens through another control variable u_h, which, in keeping with the intuition, can be thought of as the probability of halting encountered zombies at each instant. Again, we take $(u_Z, u_P, u_h) \in \mathcal{U}'$, where $\mathcal{U}'$ is the set of piecewise continuous controls. The system dynamics become:

$$\dot{S} = -\beta GS(u_P + u_Z) - \gamma\beta ZS \tag{3a}$$

$$\dot{Z} = \beta GSu_Z + \gamma\beta ZS - \pi\beta GZu_h \tag{3b}$$

$$\dot{P} = \beta GSu_P + \pi\beta GZu_h, \tag{3c}$$

with $0 < \pi \leq 1$ signifying the extent to which the zombies can be stopped when encountered by the original germinators. The constraints now become:

$$u_P + u_Z \leq 1 \tag{4a}$$

$$0 \leq u_P \leq 1, \; 0 \leq u_Z \leq 1, \; 0 \leq u_h \leq 1. \tag{4b}$$

C. SGZP Model With No Halting and Adaptive Defense

Instead of allowing a constant rate of interactions β, the network defender can choose the effective mixing rate β to be a function of the fraction of zombies as her defense policy ($\beta(Z)$). In these policies, the network defender regulates the rate of contact between nodes based on the illicit communication detected, a function of the number of zombie nodes. The network can implement a quarantine defense policy, captured by $\beta(Z)$, which will be a function of likelihood the malware is detected, and which will decrease the spread of the malware.

We consider the system dynamics described in the no-halting model, and adapt them accordingly:

$$\dot{S} = -\beta(Z)GS(u_P + u_Z) - \gamma\beta(Z)ZS \tag{5a}$$

$$\dot{Z} = \beta(Z)GSu_Z + \gamma\beta(Z)ZS \tag{5b}$$

$$\dot{P} = \beta(Z)GSu_P \tag{5c}$$

The controls available are also the same as those in (2). In particular, they are still assumed to be piecewise continuity.

We consider two classes of $\beta(Z)$ functions: 1) Affine functions (*gradual throttling*): $\beta(Z) = -aZ + \beta_{max}$ for $0 \leq a \leq \beta_{max}$. If $a = 0$, this simplifies to the constant β case. 2) Exponential sigmoids (*threshold throttling*): $\beta(Z) = \beta_0/(1 + e^{\alpha(Z - Z_{th})})$, with $0 < Z_{th} < 1$ being a fixed threshold and $\alpha > 0$ denoting the sharpness of the cut-off. As α increases, $\beta(Z)$ can become arbitrarily close to $\beta(Z) = \beta_0 \mathbf{1}_{Z \leq Z_{th}}$, an all-or-nothing policy. The network never shuts down due to infection ($\beta(Z) > 0$ for all Z) and more visibility leads to more restrictions from the network $\frac{d\beta(Z)}{dZ} \leq 0$ for all Z. In mobile epidemics, this is equivalent to nodes decreasing their communication range upon the detection of an infection, e.g. as in [26].

D. Key Observations

Theorem 1: For a system with the mechanics described in either § III-A, § III-B, or § III-C, with initial conditions $S(0) = S_0 > 0$, $G(0) = G_0 > 0$, $Z(0) = Z_0 \geq 0$, and $P(0) = P_0 \geq 0$, and $S_0 + G_0 + Z_0 + P_0 = 1$, and with piecewise continuous controls u_P, u_Z (and in (3), u_h), the dynamical systems (1), (3), and (5) have unique state solutions $(S(t), G(t), Z(t), P(t))$, with $S(t) > 0$, $Z(t) \geq 0$, $P(t) \geq 0$, and $(S + G + Z + P)(t) = 1$ for all $t \in [0, T]$.

This follows from standard results in the theory of ordinary differential equations [27, Theorem A.8, p. 419] and derivative bounding arguments (see [28]).

E. Utility Function

As we discussed, the attacker tries to maximize attack efficacy while minimizing visibility. We capture efficacy as a function $f(\cdot)$ of the aggregate number of zombies (Z) and passives (P) at each time instant. Meanwhile, visibility is only a function of zombies that re-spread the malware, as that is the only time the malware is detectable. We can capture instantaneous visibility as a function $g(\cdot)$ of the number of zombies at that instant. While the attacker cannot in general measure the malware's visibility, she can choose $g(\cdot)$ based on how detrimental detection would be for her purposes. This leads to the following aggregate damage function that the attacker seeks to maximize:

$$J = \int_0^T (f(Z(t) + P(t)) - g(Z(t)))\, dt. \tag{6}$$

We have some natural assumptions on $f(.)$ and $g(.)$: $f(0) = g(0) = 0$, with $\frac{dg(Z)}{dZ} > 0$ and $\frac{\partial f(Z+P)}{\partial Z} = \frac{\partial f(Z+P)}{\partial P} > 0$.

We assume that $f(x)$ is **concave**, which means that incremental damage does not increase as the number of infected agents increases [i.e., the pay-off per infected agent decreases].

In § IV-A: We assume $g(x)$ is **convex**. This means that an increment in the zombies is costlier (results in more visibility) when the infection is already more visible.

In § IV-B: We simplify g to be **linear**, $g(x) = k_g x$, $k_g > 0$.

In § IV-C: We set $g(x) \equiv 0$, as the effects of visibility have been built into the network dynamics through $\beta(Z)$.

F. Problem Statement

In § IV-A and § IV-C, the attacker seeks to choose controls $(u_Z, u_P) \in \mathcal{U}$ satisfying (2) so as to maximize J (6), while in § IV-B, she seeks to maximize J (6) through a choice of $(u_Z, u_P, u_h) \in \mathcal{U}'$ that satisfies (4).

IV. Structural Results

Using Pontryagin's Maximum Principle and custom arguments specific to each case, we obtain the *one-jump bang-bang* structure of the optimal controls for the various cases in § III-A, § III-B, and § III-C. We provide the proof for § IV-A in the main text (§ IV-D) and the one for § IV-C in §Appendix A. The proof for § IV-B is similar to § IV-D (see [28]).

A. Results for the No Halting Model

Theorem 2: Any optimal control in $\mathcal{U}$ will satisfy

$$u_P(t) = \begin{cases} 0 & t \in [0, t^*) \\ 1 & t \in (t^*, T) \end{cases} \qquad u_Z(t) = \begin{cases} 1 & t \in [0, t^*) \\ 0 & t \in (t^*, T) \end{cases}$$

for some $t^* \in [0, T)$.

This result means that for any optimal control, there exists a time threshold t^* such that prior to t^*, the germinators convert all the susceptibles they encounter to zombies, and subsequent to it they convert the susceptibles to passives.

B. Results for the Halting Model

Theorem 3: Any optimal control in $\mathcal{U}'$ will satisfy

$$u_P(t) = u_h(t) = \begin{cases} 0\, t \in [0, t^*) \\ 1\, t \in (t^*, T) \end{cases} \qquad u_Z(t) = \begin{cases} 1\, t \in [0, t^*) \\ 0\, t \in (t^*, T) \end{cases}$$

for some $t^* \in [0, T)$, except in the case where $Z(t) = 0$ for all $t \in [0, T]$, in which case u_h can be arbitrary with the other two structures holding.

This means that there exists a time threshold t^* such that prior to t^*, the germinators again convert all the susceptibles they encounter to zombies while not halting any zombies they meet, and subsequent to it they convert both the susceptibles and zombies they encounter to passives. Here, the added halting control can be used to slow the spread of zombies.

The proof of this result (see [28]) follows the same steps as the proof methodology in § IV-D, with an additional analytical argument for u_h changing at t^*.

C. Results for the Adaptive Defense Model

Theorem 2 holds (with the difference that $t^* \in [0, T]$) for constant, affine, and sigmoid $\beta(Z)$. This is remarkable given that here, β changes as a function of Z. This result is proved in §Appendix A.

D. Proof of Theorem 2 for the No Halting Model

Proof: This proof utilizes the necessary conditions for an optimal control derived from Pontryagin's maximum principle. In particular, we explicitly characterize the optimal controls as functions of the optimal states and *co-states* (akin to Lagrange multipliers). Subsequently, we start at terminal time, where the co-states are known, and follow their evolution backward in time till we arrive at the initial time, thereby implicitly characterizing the necessary structure of the optimal controls.

Define continuous co-states $(\lambda_S, \lambda_P, \lambda_Z, \lambda_0)$ such that at points of continuity of the controls:

$$\begin{aligned} \dot{\lambda}_S &= \beta[(\lambda_S - \lambda_P)Gu_P + (\lambda_S - \lambda_Z)Gu_Z + (\lambda_S - \lambda_Z)\gamma Z] \\ \dot{\lambda}_Z &= -f'(Z+P) + g'(Z) + (\lambda_S - \lambda_Z)\gamma\beta S \\ \dot{\lambda}_P &= -f'(Z+P), \end{aligned} \tag{7}$$

with final co-state constraints:

$$\lambda_S(T) = \lambda_Z(T) = \lambda_P(T) = 0. \tag{8}$$

Towards characterizing properties of optimal solutions, we define the *Hamiltonian* as:

$$\begin{aligned} \mathcal{H}(t) := \lambda_0(f(Z+P) - g(Z)) + (\lambda_P - \lambda_S)\beta GSu_P \\ + (\lambda_Z - \lambda_S)\beta GSu_Z + (\lambda_Z - \lambda_S)\gamma\beta ZS. \end{aligned} \tag{9}$$

Pontryagin's Maximum Principle [27, p.182] states any optimal control vector u^* must satisfy these necessary conditions:

$$(\lambda_S(t), \lambda_P(t), \lambda_Z(t), \lambda_0) \neq \vec{0}\ \ \forall_{t\in[0,T]},\ \ \lambda_0 \in \{0, 1\}, \tag{10}$$

$$\begin{aligned} &\forall_{u\in\mathcal{U}, t\in[0,T]}\, \mathcal{H}(S^*, Z^*, P^*, u^*, \lambda_S(t), \lambda_P(t), \lambda_Z(t), \lambda_0, t) \\ &\geq \mathcal{H}(S^*, Z^*, P^*, u, \lambda_S(t), \lambda_P(t), \lambda_Z(t), \lambda_0, t). \end{aligned} \tag{11}$$

But if $\lambda_0 = 0$, (10) is violated at $t = T$, so $\lambda_0 = 1$.

1) Structure of the Optimal Control: If we define:

$$\varphi_P = (\lambda_P - \lambda_S)\beta GS \tag{12a}$$

$$\varphi_Z = (\lambda_Z - \lambda_S)\beta GS, \tag{12b}$$

then, the Hamiltonian becomes:

$$\begin{aligned} \mathcal{H}(t) = f(Z+P) - g(Z) + \varphi_P u_P + \varphi_Z u_Z \\ + (\lambda_Z - \lambda_S)\gamma\beta ZS. \end{aligned} \tag{3}$$

The maximization of the Hamiltonian (11), added to the sum constraints for the controls (2a), leads to the following optimality conditions for the controls:[1]

$$(u_P, u_Z) = \begin{cases} (0,0) & \varphi_P < 0,\ \varphi_Z < 0 & \text{(14a)} \\ (1,0) & \varphi_P > 0,\ \varphi_P > \varphi_Z & \text{(14b)} \\ (0,1) & \varphi_Z > 0,\ \varphi_Z > \varphi_P & \text{(14c)} \\ (?,?) & \varphi_Z = \varphi_P \geq 0 & \text{(14d)} \\ (?,0) & \varphi_P = 0,\ \varphi_Z < 0 & \text{(14e)} \\ (0,?) & \varphi_Z = 0,\ \varphi_P < 0 & \text{(14f)} \end{cases}$$

From (12) and the state (1) and costate (7) evolution equations and after some manipulations, we have:[2]

$$\begin{aligned} \dot{\varphi}_P &= \beta[Gu_Z(\varphi_Z - \varphi_P) + \gamma Z(\varphi_Z - \varphi_P) - GSf'(Z+P)] \\ \dot{\varphi}_Z &= \beta[GS(g'(Z) - f'(Z+P)) + Gu_P(\varphi_P - \varphi_Z) - \gamma S\varphi_Z] \end{aligned} \tag{15a}$$

$$\begin{aligned} \dot{\varphi}_P - \dot{\varphi}_Z = -(\varphi_P - \varphi_Z)(\beta Gu_Z + \gamma\beta Z + \beta Gu_P) \\ -\beta GSg'(Z) + \gamma\beta S\varphi_Z, \end{aligned} \tag{15b}$$

2) Proof Methodology Outline: From here on, we will use the necessary optimality conditions to obtain timing conditions for phase transitions among the conditions in (14). We show that a time t^* exists such that, for $t \in (t^*, T)$, we have $u_P(t) = 1$ and $u_Z(t) = 0$ (§ IV-D3). If $t^* = 0$, we have finished characterizing optimal controls. If not (i.e., $t^* > 0$), we prove that a time t'' exists such that for $t \in (t'', t^*)$, we have $u_P(t) = 0$ and $u_Z(t) = 1$ (in § IV-D4). Finally, we show that t'' must be equal to zero (in § IV-D5), leading to all possible optimal controls agreeing with the structure laid out in Theorem 2.

3) Time Interval Leading Up to T and the Existence of t^*: We now follow the evolution of φ_Z and φ_P for a time interval leading to T in order to characterize necessary conditions for the optimal controls and to prove the existence of t^*. From the terminal time costate conditions (8): $\varphi_P(T) = \varphi_Z(T) = 0$, $\dot{\varphi}_P(T^-) = -f'((Z+P)(T^-))\beta GS(T^-) < 0$, $\dot{\varphi}_P(T^-) - \dot{\varphi}_Z(T^-) = -\beta GS(T^-)g'(Z(T^-)) < 0$. Therefore, $\varphi_P(t) > max\{\varphi_Z(t), 0\}$ for some interval leading up to T due to the continuity of the states and costates and using the definition of a left derivative. Let (t^*, T) be the largest interval over which this holds for $t \in (t^*, T)$ for some $t^* < T$, leading to the fact that for all such t, $u_P(t) = 1$ and $u_Z(t) = 0$ due to (14b).

For $t \in (t^*, T)$, (15) becomes:

$$\dot{\varphi}_P = -\beta GSf'(Z+P) + \gamma\beta Z(\varphi_Z - \varphi_P) \tag{16a}$$

$$\begin{aligned} \dot{\varphi}_Z &= \beta GS(g'(Z) - f'(Z+P)) + \beta G(\varphi_P - \varphi_Z) - \gamma\beta S\varphi_Z \\ \dot{\varphi}_P - \dot{\varphi}_Z &= \gamma\beta S\varphi_Z - (\varphi_P - \varphi_Z)(\gamma\beta Z + \beta G) - \beta GSg'(Z). \end{aligned} \tag{16b}$$

[1] The question marks (?) denote singular controls, where the control has no effect on the Hamiltonian maximizing condition of the PMP on an interval.

[2] $g'(Z) := \frac{dg(Z)}{dZ}$, $f'(Z+P) := \frac{\partial f(Z+P)}{\partial Z} = \frac{\partial f(Z+P)}{\partial P}$

Recall that $\varphi_P(t) > 0$ for $t \in (t^*, T)$, so due to continuity, we either have $\varphi_P(t^*) > 0$ or $\varphi_P(t^*) = 0$. We now rule out $\varphi_P(t^*) = 0$. If $\varphi_P(t^*) = 0$, Rolle's Mean Value Theorem [29, p. 215] applies over the interval (t^*, T): as $\varphi_P(t^*) = \varphi_P(T) = 0$ and φ_P is continuous and differentiable over this interval, there must exist $\tau \in (t^*, T)$ such that $\dot{\varphi}_P(\tau) = 0$. However, from (16a), it can be seen that $\dot{\varphi}_P(t) < 0$ for $t \in (t^*, T)$, a contradiction. Therefore, $\varphi_P(t^*) > 0$.

Thus, either $t^* = 0$ or $\varphi_Z(t^*) = \varphi_P(t^*)$. If $t^* = 0$, due to (14b), we have $u_P(t) = 1$ and $u_Z(t) = 0$ for all t which agrees with the structure in Theorem 2, so henceforth we focus on **the case where** $\varphi_Z(t^*) = \varphi_P(t^*) > 0$.

First, we derive a property that will prove useful later on. We have $\dot{Z}(t) \geq 0$ from (1b) and Theorem 1, and thus due to the convexity of $g(\cdot)$ for $t < t^*$:

$$\frac{Gg'(Z(t^*))}{\gamma} \geq \frac{Gg'(Z(t))}{\gamma}. \tag{17}$$

Next, $Z(t^*)$ can either be equal to zero or strictly positive. We first show that if $Z(t^*) = 0$, the structure holds.

If $Z(t^*) = 0$, we have $\dot{Z} = \gamma\beta SZ$ for $t \in (t^*, T)$ as $u_Z(t) = 0$ in this interval. Consider $M_1 > 0$ to be an upper-bound on the continuous $\gamma\beta S$ in this interval, so we must have $Z(t) \leq Z(t^*)e^{M_1(t-t^*)} = 0$, and therefore $Z(T) = 0$ due to continuity and the uniqueness of solutions of first-order initial value problems. Thus, as $\dot{Z} \geq 0$ for $t \in (0, T)$, we must have $\dot{Z} = 0$ over this interval, which from (1b) and Theorem 1 leads to $u_Z(t) = 0$ for $t \in (0, T)$ and $Z_0 = 0$. This also means that from (16a), $\dot{\varphi}_P(t) = -\beta GSf'(Z + P) < 0$ in this interval, leading to $\varphi_P(t) > \varphi_P(T) = 0$, and from (14), to $u_P(t) = 1$ over this interval. Thus, again $t^* = 0$, agreeing with the structure predicted by Theorem 2. So from now on we will **consider** $Z(t^*) > 0$.

Now, we examine $g'(Z(t^*)) - f'((Z + P)(t^*))$, noting that it can either be positive or strictly negative, and investigate both cases in turn.

If $g'(Z(t^*)) - f'((Z + P)(t^*)) \geq 0$, then $g'(Z(t)) - f'((Z + P)(t)) \geq 0$ for all $t \in (t^*, T)$. This is because from (1), $\dot{P}(t) + \dot{Z}(t) \geq 0$ and $\dot{Z}(t) \geq 0$ over this interval, which coupled with the convexity of $g(\cdot)$ and $-f(\cdot)$ in their arguments gives the aforementioned result. From (16b) and the definition of t^*, $\dot{\varphi}_Z > -\gamma\beta S\varphi_Z \geq -M_2\varphi_Z$ in this interval, with $M_2 > 0$ being an upper-bound on $\gamma\beta S$. Therefore, $\varphi_Z(t^*) \leq \varphi_Z(T)e^{-M_2(t^*-T)} = 0$ due to an integral argument, which means that $\varphi_P(t^*) > 0 \geq \varphi_Z(t^*)$. Note that this would contradict the starting assumption of this segment, which was $\varphi_P(t^*) = \varphi_Z(t^*)$

Therefore, from here on we will **examine the case of** $g'(Z(t^*)) < f'((Z + P)(t^*))$.

4) Time Interval Leading Up to $t^*>0$ and the Existence of t'': We now look at the evolution of φ_Z and φ_P for a time interval leading to $t^* > 0$, and show that t'' exists such that t for $t \in (t'', t^*)$, we have $u_P(t) = 0$ and $u_Z(t) = 1$. Furthermore, in these cases we showed $\varphi_Z(t^*) = \varphi_P(t^*)$, $Z(t^*) > 0$, and $g'(Z(t^*)) < f'((Z + P)(t^*))$. At such a point t^*, from (15a) and the continuity of the states and co-states:

$$(\dot{\varphi}_P(t^{*+}) - \dot{\varphi}_Z(t^{*+})) = \beta S(t^*)[\gamma\varphi_Z(t^*) - Gg'(Z(t^*))]. \tag{18}$$

Now, (18) should be positive, because if this derivative was strictly negative, the definition of the right-derivative would show that $\varphi_Z(t) > \varphi_P(t)$ for t in an interval starting from t^*, a contradiction. Because from Theorem 1, $S(t^*) > 0$, so $\beta S(t^*)[\gamma\varphi_Z(t^*) - Gg'(Z(t^*))] \geq 0$ and:

$$\varphi_Z(t^*) \geq \frac{Gg'(Z(t^*))}{\gamma}. \tag{19}$$

Now, we can see from a continuity argument on (15a) (given that $\varphi_Z(t^*) = \varphi_P(t^*) > 0$) that $\dot{\varphi}_Z(t^{*-}) < 0$. Thus $\varphi_Z(t) > \varphi_Z(t^*)$ for some interval leading up to t^* due to the definition of a left-derivative.

From (15a), (17), and (19), we must have: $\varphi_Z(t) > \frac{Gg'(Z(t))}{\gamma}$ for t in some interval leading up to t^*. Let (t', t^*) be the maximal such interval. In this interval, from (15b), $\dot{\varphi}_P - \dot{\varphi}_Z > -(\varphi_P - \varphi_Z)(\gamma\beta Z + \beta G) \geq -M_3(\varphi_P - \varphi_Z)$, where $M_3 > 0$ is an upper-bound on the continuous expression $\gamma\beta Z + \beta G$. So for any t in this interval, $(\varphi_P(t) - \varphi_Z(t)) < (\varphi_P(t^*) - \varphi_Z(t^*))e^{-M_3(t-t^*)} = 0$. Thus, $\varphi_P(t) < \varphi_Z(t)$ for $t \in (t', t^*)$. As $\varphi_Z(t^*) > 0$, due to the continuity of the states and co-states, there exists a maximal interval (t'', t^*) such that $\varphi_Z(t) > \max\{\varphi_P(t), 0\}$. Following from (14c), for $t \in (t'', t^*)$ we must have $u_P(t) = 0$ and $u_Z(t) = 1$.

5) Proof That $t''=0$: If $t'' = 0$, the above concludes our specification of the structure, which agrees with Theorem 2. Thus, henceforth we assume $t'' > 0$, and thus **either** $\varphi_Z(t'') = \varphi_P(t'')$ or $\varphi_Z(t'') = 0$.

For $t \in (t'', t^*)$, (15) becomes:

$$\begin{aligned}
\dot{\varphi}_P &= \beta[-GSf'(Z + P) + G(\varphi_Z - \varphi_P) + \gamma Z(\varphi_Z - \varphi_P)] \\
\dot{\varphi}_Z &= \beta[GS(g'(Z) - f'(Z + P)) - \gamma S\varphi_Z] \\
\dot{\varphi}_P - \dot{\varphi}_Z &= \beta[\gamma S\varphi_Z - (\varphi_P - \varphi_Z)(G + \gamma Z) - GSg'(Z)],
\end{aligned} \tag{20a}$$

Now, for $t \in (t'', t^*)$, $g'(Z(t)) - f'((Z + P)(t)) < g'(Z(t^*)) - f'((Z + P)(t^*)) < 0$. This is because $\dot{Z}(t) > 0$ as $u_Z(t) = 1$, and $\dot{P}(t) = 0$ as $u_P(t) = 0$, so $g(\cdot) - f(\cdot)$ is convex in the strictly increasing Z in this interval. So from (20a), $\dot{\varphi}_Z < -\gamma\beta S\varphi_Z \leq -M_4\varphi_Z$ with $M_4 > 0$ being the upper-bound of the continuous $\gamma\beta S$, and therefore for all $t \in (t'', t^*)$, $\varphi_Z(t) \geq \varphi_Z(t^*)e^{-M_4(t-t^*)}$, and therefore by continuity, $\varphi_Z(t'') \geq \varphi_Z(t^*)e^{-M_4(t''-t^*)}$. Thus, we can conclude that $\varphi_Z(t'') > 0$, as $\varphi_Z(t^*) > 0$.

So for $t'' > 0$, **we must have** $\varphi_P(t'') = \varphi_Z(t'')$. In this case, $(\dot{\varphi}_P(t''^+) - \dot{\varphi}_Z(t''^+)) \leq 0$, as if it is strictly positive, an integral argument will lead to a contradiction with $\varphi_P(t) < \varphi_Z(t)$ for $t \in (t'', t^*)$. From Theorem 1, $S(t'') > 0$, and using the continuity of the states and co-states, (20a) becomes:

$$\begin{aligned}
\dot{\varphi}_P(t''^+) - \dot{\varphi}_Z(t''^+) = \beta S(t'')[\gamma\varphi_Z(t'') - Gg'(Z(t''))] \leq 0 \\
\Rightarrow \quad \varphi_Z(t'') \leq \frac{Gg'(Z(t''))}{\gamma},
\end{aligned} \tag{21}$$

We know that for all $t \in (t'', t^*)$, $g'(Z(t)) - f'(Z + P(t)) < 0$, so from (20a), $\dot{\varphi}_Z(t) < -\gamma\beta S\varphi_Z < -M_5\varphi_Z < 0$, where $M_5 > 0$ is an upper-bound on the continuous $\gamma\beta S$. Thus,

$$\varphi_Z(t'') > \varphi_Z(t^*). \tag{22}$$

But (17), (21), and (22) lead to $\varphi_Z(t^*) < \frac{Gg'(Z(t^*))}{\gamma}$, which contradicts (19). Thus $t'' = 0$, and this concludes our specification of the structure of the optimal controls which conform to the structure set out in Theorem 2. ■

V. Future Directions

The current work is an abstraction of practical cybersecurity problems mainly due to the homogeneous mixing assumption. Another possible direction is to look at the optimal control of such an epidemic in sub-populations with differentiating characteristics (e.g., location, contact rate) as a way to relax the homogeneous mixing assumption (e.g., by following the roadmap in [20]). Such a generalization would better model Stuxnet in particular, with the goal being to maximize the number of infected agents in a particular region, while minimizing the total number of detectable zombies.

APPENDIX A
PROOF OF THEOREM 2 FOR ADAPTIVE DEFENSE MODEL

As before, define the continuous co-states $(\lambda_S, \lambda_P, \lambda_Z, \lambda_0)$ such that at points of continuity of the controls:

$$\begin{aligned}\dot{\lambda}_S &= \beta(Z)[(\lambda_S - \lambda_P)Gu_P + (\lambda_S - \lambda_Z)(Gu_Z + \gamma Z)]\\ \dot{\lambda}_Z &= -\lambda_0 f'(Z+P) + (\lambda_S - \lambda_Z)\gamma\beta(Z)S\\ &\quad + \beta'(Z)[(\lambda_S - \lambda_P)GSu_P + (\lambda_S - \lambda_Z)GSu_Z\\ &\quad + (\lambda_S - \lambda_Z)\gamma ZS]\\ \dot{\lambda}_P &= -\lambda_0 f'(Z+P), \end{aligned} \tag{23}$$

with final co-state constraints:

$$\lambda_S(T) = \lambda_Z(T) = \lambda_P(T) = 0. \tag{24}$$

To characterize optimal controls, we define the *Hamiltonian*:

$$\begin{aligned}\mathcal{H}(t) := \lambda_0 f(Z+P) + (\lambda_P - \lambda_S)\beta(Z)GSu_P\\ + (\lambda_Z - \lambda_S)\beta(Z)GSu_Z + (\lambda_Z - \lambda_S)\gamma\beta(Z)ZS \end{aligned} \tag{25}$$

Pontryagin's Maximum Principle [27, p.182] gives us the following necessary conditions for optimality for an optimal control vector u^*:

$$(\lambda_S, \lambda_P, \lambda_Z, \lambda_0) \neq \vec{0}, \quad \lambda_0 \in \{0, 1\}, \tag{26}$$

$$\begin{aligned}&\forall_{u\in\mathcal{U}, t\in[0,T]}\, \mathcal{H}(S^*, Z^*, P^*, u^*, \lambda_S(t), \lambda_P(t), \lambda_Z(t), \lambda_0, t) \geq\\ &\mathcal{H}(S^*, Z^*, P^*, u, \lambda_S(t), \lambda_P(t), \lambda_Z(t), \lambda_0, t). \end{aligned} \tag{27}$$

But if $\lambda_0 = 0$, $(\lambda_S(T), \lambda_P(T), \lambda_Z(T), \lambda_0) = \vec{0}$, a contradiction, so $\lambda_0 = 1$.

A. General Structure of the Optimal Control

If we define:

$$\varphi_P = (\lambda_P - \lambda_S)\beta(Z)GS \tag{28a}$$

$$\varphi_Z = (\lambda_Z - \lambda_S)\beta(Z)GS, \tag{28b}$$

then, the Hamiltonian becomes:

$$\mathcal{H}(t) = f(Z+P) + \varphi_P u_P + \varphi_Z u_Z + (\lambda_Z - \lambda_S)\gamma\beta(Z)ZS.$$

The maximization of the Hamiltonian (27), added to the sum constraints for the controls (2a), leads to (14) as the optimality conditions for the controls:

$$\varphi_Z(t) > 0 \text{ or } \varphi_P(t) > 0 \Rightarrow u_P(t) + u_Z(t) = 1, \tag{29}$$

as if that is not true, we can add to the instantaneous value of $\mathcal{H}(t)$ by adding to either $u_P(t)$ or $u_Z(t)$, a contradiction with the Hamiltonian maximization condition (27).

From (28) and the state (5) and costate (23) evolution equations and after some manipulation, we have:

$$\begin{aligned}\dot{\varphi}_P &= -\beta(Z)GSf'(Z+P) + \beta'(Z)S\varphi_P[Gu_Z + \gamma Z]\\ &\quad - (\varphi_P - \varphi_Z)\beta(Z)[Gu_Z + \gamma Z] \end{aligned} \tag{30a}$$

$$\begin{aligned}\dot{\varphi}_Z &= -\beta(Z)GSf'(Z+P) - \varphi_P Gu_P\beta'(Z)S\\ &\quad - \varphi_Z\beta(Z)\gamma S + (\varphi_P - \varphi_Z)\beta(Z)Gu_P, \end{aligned} \tag{30b}$$

$$\begin{aligned}\dot{\varphi}_P - \dot{\varphi}_Z &= -(\varphi_P - \varphi_Z)\beta(Z)[G(u_Z + u_P) + \gamma(Z+S)]\\ &\quad + \varphi_P S\big[\gamma\beta(Z) + \beta'(Z)[G(u_Z + u_P) + \gamma Z]\big] \end{aligned} \tag{30c}$$

Again, the proof follows the outline laid out in § IV-D2 (i.e., proving the existence of t^* and t', which are, however, defined differently, and proving $t' = 0$ for $t^* > 0$), with the difference that the algebraic expressions for $\dot{\varphi}_Z$ and $\dot{\varphi}_P$, and therefore all subsequent analytical arguments, will change.

1) Time Interval Leading Up to T and the Existence of t^*: We follow the evolution of φ_Z and φ_P for a time interval leading to T and prove the existence of t^* such that we have $u_P(t) = 1$, and $u_Z(t) = 0$ for all $t \in (t^*, T)$.

From the terminal time costate conditions (24) and their directional derivatives (30), we have:

$$\varphi_P(T) = \varphi_Z(T) = 0, \tag{31a}$$

$$\dot{\varphi}_P(T^-) = \dot{\varphi}_Z(T^-) = -\beta(Z)GSf'(Z+P) < 0. \tag{31b}$$

So, due to continuity of the states and co-states, there is an interval leading up to T, over which we have $\varphi_P(t) > 0$ and $\varphi_Z(t) > 0$. Let (t^*, T) be the maximal length interval with this property. For $t \in (t^*, T)$, equation (29) leads to

$$u_Z(t) + u_P(t) = 1. \tag{32}$$

Now, for $t \in (t^*, T)$, (30c) becomes:

$$\begin{aligned}\dot{\varphi}_P(t) - \dot{\varphi}_Z(t) &= -(\varphi_P - \varphi_Z)\beta(Z)[G + \gamma(Z+S)]\\ &\quad + \varphi_P S\big[\gamma\beta(Z) + \beta'(Z)[G + \gamma Z]\big] \end{aligned} \tag{33}$$

The rest of the analysis depends on the $\beta(Z)$ function—we present the arguments for $\beta(Z)$'s that are sigmoid. We use different analytical arguments to prove the result depending on whether $e^{\alpha(Z(T)-Z_{th})}(1 - \frac{\alpha}{\gamma}G - \alpha Z(T)) + 1$ is less than, equal to, or greater than zero. For the affine case, the analysis needs to be broken down into different cases according to the value of $Z(T)$ in relation to the constant $\frac{1}{2}[\frac{\beta_{\max}}{a} - \frac{G}{\gamma}]$ but follows the same structure (see [28]). For the simple case of constant $\beta(Z)$, no such conditional arguments are needed and the proof is straightforward.

Assume $\beta_Z = \frac{\beta_0}{1+e^{\alpha(Z-Z_{th})}}$, with $0 < Z_{th} < 1$ being a fixed threshold and $\alpha > 0$ denoting the sharpness of the cut-off. This simulates a threshold-like detection of zombies by a network administrator. In this case, (30c) becomes:

$$\begin{aligned}\dot{\varphi}_P - \dot{\varphi}_Z &= -(\varphi_P - \varphi_Z)\beta(Z)[G(u_Z + u_P) + \gamma(Z+S)]\\ &\quad + \frac{\beta_0\gamma\varphi_P S\big[e^{\alpha(Z-Z_{th})}(1 - \frac{\alpha}{\gamma}G(u_z + u_P) - \alpha Z) + 1\big]}{(1+e^{\alpha(Z-Z_{th})})^2} \end{aligned} \tag{34}$$

Define: $\Psi(Z, u_Z + u_P) := e^{\alpha(Z-Z_{th})}(1 - \frac{\alpha}{\gamma}G(u_z + u_P) - \alpha Z) + 1$. Then (34) becomes:

$$\begin{aligned}\dot{\varphi}_P - \dot{\varphi}_Z &= -(\varphi_P - \varphi_Z)\beta(Z)[G(u_Z + u_P) + \gamma(Z+S)]\\ &\quad + \frac{\beta_0\gamma\varphi_P S}{(1+e^{\alpha(Z-Z_{th})})^2}\Psi(Z, u_Z + u_P) \end{aligned} \tag{35}$$

Now, for possible intervals where $u_Z + u_P$ is a constant $c \in [0, 1]$, $\Psi(Z, c)$ is a function of one variable (Z). We can see that at points of continuity of the controls and in intervals where it is defined, $\Psi(Z, c)$ is also continuous and differentiable. Furthermore, we can see that at points of continuity of the controls in these intervals, we have:

$$\frac{d\Psi(Z,c)}{dZ} = -\alpha^2 e^{\alpha(Z-Z_{th})}\left(\frac{G}{\gamma}c + Z\right) < 0 \tag{36}$$

Now we break down the situations that can arise based on the value of $\Psi(Z(T), 1)$:

2) $\Psi(Z(T),1)>0$**:** From $\dot{Z}\geq 0$ ((5) and Theorem 1) and the continuity of the states, we have $Z(t)\leq Z(T)$ for all t. Now for $t\in(t^*,T)$, as the sum of the controls is constant and equal to one due to (32), we will have $\Psi(Z(t),1)\geq\Psi(Z(T),1)>0$ due to (36). Thus from (35) and for all $t\in(t^*,T)$ at which the controls are continuous: $\dot{\varphi}_P(t)-\dot{\varphi}_Z(t)>-(\varphi_P-\varphi_Z)\beta(Z)[G+\gamma(Z+S)]\geq-(\varphi_P-\varphi_Z)M_{14}$, for some $M_{14}>0$ which is an upper-bound to the continuous $\beta(Z)[G+\gamma(Z+S)]$. Therefore, for $t\in(t^*,T)$, $\varphi_P(t)-\varphi_Z(t)<[\varphi_P(T)-\varphi_Z(T)]e^{-M_{14}(t-T)}=0$, and thus $\varphi_P(t)<\varphi_Z(t)$ for $t\in(t^*,T)$.

Due to the continuity of the states and co-states and from the definition of t^*, there exists an interval (t',T), with $t'\leq t^*$ such that $\varphi_Z(t)>\varphi_P(t)$ and $\varphi_Z(t)>0$. These conditions, coupled with (14c) lead to $u_P(t)=0$ and $u_Z(t)=1$ for all $t\in(t',T)$, with the corollary that $u_P(t)+u_Z(t)=1$.

We now prove $t'=0$. If this does not hold, either $\varphi_Z(t')=0$ or $\varphi_Z(t')=\varphi_P(t')>0$ for $t'>0$ due to continuity of the states and co-states.

For $t\in(t',T)$, as $u_P(t)=0$, (30b) becomes: $\dot{\varphi}_Z(t)=-\beta(Z)GSf'(Z+P)-\varphi_Z\beta(Z)\gamma S<0$, as each term in the right hand side is strictly positive in the interval. Now, if we have $\varphi_Z(t')=0$, from this time-derivative and continuity of the states and co-states we must have $\varphi_Z(t')>\varphi_Z(T)=0$. Thus, $\varphi_Z(t')=0$ is ruled out.

On the other hand, if $\varphi_Z(t')=\varphi_P(t')>0$, then from (35) and the continuity of the states and co-states: $\left(\dot{\varphi}_P-\dot{\varphi}_Z\right)(t'^+)=\frac{\beta_0\gamma\varphi_P(t')S(t')}{(1+e^{\alpha(Z(t')-Z_{th})})^2}\Psi(Z(t'),1)>0$, leading to the existence of an interval (t',t'') over which $\varphi_P(t)>\varphi_Z(t)$, a contradiction with the definition of t'.

Thus, $t'=0$ and $u_Z(t)=1$ and $u_P(t)=0$ for all t, which agrees with the statement of Theorem 2.

3) $\Psi(Z(T),1)=0$ ***and*** $Z(T)>0$**:** We have $\dot{Z}(T^-)>0$ (from (5), Theorem 1, and continuity) which leads to $Z(t)<Z(T)$ for an interval leading up to t. As $\dot{Z}\geq 0$, we can extend $Z(t)<Z(T)$ to all t. Now for $t\in(t^*,T)$, from (32), we will have $\Psi(Z(t),1)>\Psi(Z(T),1)=0$ due to (36). We now prove $t'=0$ and $u_Z(t)=1$ and $u_P(t)=0$ for all t.

From (32), (35), for all $t\in(t^*,T)$ (over which $\varphi_P(t)>0$): $\dot{\varphi}_P(t)-\dot{\varphi}_Z(t)>-(\varphi_P-\varphi_Z)\beta(Z)[G+\gamma(Z+S)]\geq-(\varphi_P-\varphi_Z)M_{12}$ for some $M_{12}>0$ which is an upper-bound to the continuous $\beta(Z)[G+\gamma(Z+S)]$ over this interval. Therefore, for $t\in(t^*,T)$, $\varphi_P(t)-\varphi_Z(t)<[\varphi_P(T)-\varphi_Z(T)]e^{-M_{12}(t-T)}=0$, and thus $\varphi_P(t)<\varphi_Z(t)$ for $t\in(t^*,T)$.

Due to the continuity of the states and co-states and because for $t\in(t^*,T)$, $\varphi_Z(t)>0$, there exists an interval (t',T), with $t'\leq t^*$ such that both $\varphi_Z(t)>\varphi_P(t)$ and $\varphi_Z(t)>0$. These conditions, coupled with (14c) lead to $u_P(t)=0$ and $u_Z(t)=1$ for all $t\in(t',T)$.

We now prove $t'=0$. If this does not hold, either (i) $\varphi_Z(t')=0$ or (ii) $\varphi_Z(t')=\varphi_P(t')$ for some $t'>0$ due to continuity of the states and co-states.

For $t\in(t',T)$ (30b) becomes: $\dot{\varphi}_Z(t)=-\beta(Z)GSf'(Z+P)-\varphi_Z\beta(Z)\gamma S<0$, which leads to $\varphi_Z(t')>\varphi_Z(T)=0$.

So for $t'>0$ we must have $\varphi_Z(t')=\varphi_P(t')$. From (35) and the continuity of the states and co-states: $\left(\dot{\varphi}_P-\dot{\varphi}_Z\right)(t'^+)=\frac{\beta_0\gamma\varphi_P(t')S(t')}{(1+e^{\alpha(Z(t')-Z_{th})})^2}\Psi(Z(t'),1)=\frac{\beta_0\gamma\varphi_Z(t')S(t')}{(1+e^{\alpha(Z(t')-Z_{th})})^2}\Psi(Z(t'),1)>0$, leading to the existence of an interval (t',t'') over which $\varphi_P(t)>\varphi_Z(t)$, a contradiction with the definition of t'.

Thus, $t'=0$ and $u_Z(t)=1$ and $u_P(t)=0$ for all t, which agrees with the statement of Theorem 2. ■

4) $\Psi(Z(T),1)=0$ ***and*** $Z(T)=0$**:** We must have $\dot{Z}(t)=0$ for all t as $\dot{Z}\geq 0$ and as states are continuous. The only way for $\dot{Z}(t)=0$ for all t is for us to have $Z_0=0$ and $u_Z(t)=0$ for all $t<T$ (due to Theorem 1). This leads to (30a) becoming $\dot{\varphi}_P(t)=-\beta(0)GS(t)f'(P(t))<0$ for all $t<T$, and thus $\varphi_P(t)>0$. This fact, combined with $u_Z(t)=0$ for all t and (14b) leads to $u_P(t)=1$ for all t.

5) $\Psi(Z(T),1)<0$**:** Due to the continuity of the states, $\Psi(Z(t),1)<0$ for $t\in(t_1,T)$ for some t_1. Thus, (35) leads to $\dot{\varphi}_P(t)-\dot{\varphi}_Z(t)<-(\varphi_P-\varphi_Z)\beta(Z)[G+\gamma(Z+S)]\leq-(\varphi_P-\varphi_Z)M_{12}$, for $t\in(t_2,T)$, where $t_2=\max\{t^*,t_1\}$ and with M_{12} defined as before (an upper-bound to the continuous $\beta(Z)[G+\gamma(Z+S)]$ over this interval). Therefore, in this interval, $\varphi_P(t)-\varphi_Z(t)>[\varphi_P(T)-\varphi_Z(T)]e^{-M_{12}(t-T)}=0$, and thus $\varphi_P(t)>\varphi_Z(t)$ and $\varphi_P(t)>0$ for $t\in(t_2,T)$.

Now, due to the continuity of the states and co-states, define (t_3,T) to be the maximal length interval over which $\varphi_P(t)>\varphi_Z(t)$ and $\varphi_P(t)>0$. Note that for $t\in(t_3,T)$ we have (due to (14b)) $u_Z(t)=0$ and $u_P(t)=1$.

Due to continuity of the states and co-states, either $t_3=0$, in which case $u_Z(t)=0$ and $u_P(t)=1$ for all t, or we have a $t_3>0$ such that (i) $\varphi_P(t_3)=0$ or (ii) $\varphi_P(t_3)=\varphi_Z(t_3)>0$.

From (30a), Theorem 1, and from the definition of t_3, for $t\in(t_3,T)$ we have: $\dot{\varphi}_P=-\beta(Z)GSf'(Z+P)\ -(\varphi_P-\varphi_Z)\beta(Z)\gamma Z-\frac{\alpha\beta_0\gamma e^{\alpha(Z-Z_{th})}}{(1+e^{\alpha(Z-Z_{th})})^2}S\varphi_P Z<-\frac{\alpha\beta_0\gamma e^{\alpha(Z-Z_{th})}SZ}{(1+e^{\alpha(Z-Z_{th})})^2}\varphi_P\leq-M_{15}\varphi_P$, for some $M_{15}>0$ that is an upper-bound to the continuous $\frac{\alpha\beta_0\gamma e^{\alpha(Z-Z_{th})}SZ}{(1+e^{\alpha(Z-Z_{th})})^2}$. Thus, $\varphi_P(t_3)>\varphi_P(T)e^{-M_{15}(t_3-T)}=0$.

So for $t_3>0$ we must have $\varphi_P(t_3)=\varphi_Z(t_3)>0$. From the continuity of the states and co-states, there must exist an interval leading up to t_3 such that $\varphi_Z(t)>0$ and $\varphi_P(t)>0$. Let (t_4,t_3) be the maximal-length interval with such a property. Notice that (29) also applies, leading to $u_P(t)+u_Z(t)=1$ for $t\in(t_4,t_3)$.

Furthermore, also from continuity, (35) becomes:

$$\dot{\varphi}_P(t_3^+)-\dot{\varphi}_Z(t_3^+)=\frac{\beta_0\gamma\varphi_P(t_3)S(t_3)}{(1+e^{\alpha(Z(t_3)-Z_{th})})^2}\Psi(Z(t_3),1)\qquad(37)$$

But if $\dot{\varphi}_P(t_3^+)-\dot{\varphi}_Z(t_3^+)<0$, then due to continuity and the definition of the derivative, we must have an interval starting from t_3 where $\varphi_Z(t)>\varphi_P(t)$, which contradicts the definition of t_3. So we must have $\dot{\varphi}_P(t_3^+)-\dot{\varphi}_Z(t_3^+)\geq 0$. From (33) this is equivalent to $\Psi(Z(t_3),1)\geq 0$. Following the same arguments presented in §A.A.2, §A.A.3, and §A.A.4 for the case of $\Psi(Z(T),1)\geq 0$ and retracing them for $\Psi(Z(t_3),1)\geq 0$ (with t_3 replacing T) shows Theorem 2's structure holds.

Thus, Theorem 2 holds for all possible trajectories.

REFERENCES

[1] W. H. Murray, "The application of epidemiology to computer viruses," *Computers & Security*, vol. 7, no. 2, pp. 139–145, 1988.

[2] Symantec, "Regin: Top-tier espionage toolenables stealthy surveillance," *White Paper, Symantec Corp., Security Response*, 2014.

[3] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White Paper, Symantec Corp., Security Response*, 2011.

[4] R. Langner, "To kill a centrifuge: A technical analysis of what stuxnets creators tried to achieve," tech. rep., 2013.

[5] D. Sanger, "Obama order sped up wave of cyberattacks against iran," *New York Times*, Jun. 1st, 2012.

[6] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, "The cousins of stuxnet: Duqu, flame, and gauss," *Future Internet*, vol. 4, no. 4, pp. 971–1003, 2012.

[7] H. W. Hethcote and P. Waltman, "Optimal vaccination schedules in a deterministic epidemic model," *Mathematical Biosciences*, vol. 18, no. 3, pp. 365–381, 1973.

[8] R. Morton and K. Wickwire, "On the optimal control of a deterministic epidemic," *Adv. Appl. Probability*, pp. 622–635, 1974.

[9] K. Wickwire, "Optimal isolation policies for deterministic and stochastic epidemics," *Mathematical Biosciences*, vol. 26, no. 3, pp. 325–346, 1975.
[10] K. Wickwire, "Optimal control policies for reducing the maximum size of a closed epidemic: I. deterministic dynamics," *Mathematical Biosciences*, vol. 30, no. 1, pp. 129–137, 1976.
[11] H. Behncke, "Optimal control of deterministic epidemics," *Optimal Control Appl. Methods*, vol. 21, no. 6, pp. 269–285, 2000.
[12] J. Kim, S. Radhakrishnan, and S. K. Dhall, "Measurement and analysis of worm propagation on internet network topology," in *Proc. IEEE 13th Int. Conf. Comp. Commun. Netw. (ICCCN'04)*, pp. 495–500, IEEE, 2004.
[13] C. C. Zou, W. Gong, and D. Towsley, "Code red worm propagation modeling and analysis," in *Proc. 9th ACM Conf. Comp. Commun. Security*, pp. 138–147, ACM, 2002.
[14] M. Garetto, W. Gong, and D. Towsley, "Modeling malware spreading dynamics," in *Proc. IEEE 22nd Annu. Joint Conf. IEEE Comp. Commun. Societies (INFOCOM'03)*, vol. 3, pp. 1869–1879, , IEEE, 2003.
[15] Z. Lu, W. Wang, and C. Wang, "How can botnets cause storms? understanding the evolution and impact of mobile botnets," *IEEE INFOCOM*, 2014.
[16] K. J. Hall, *Thwarting Network Stealth Worms in Computer Networks Through Biological Epidemiology*. Ph.D. Thesis, Citeseer, 2006.
[17] H. C. Schramm and D. P. Gaver, "Lanchester for cyber: The mixed epidemic-combat model," *Naval Research Logistics (NRL)*, vol. 60, no. 7, pp. 599–605, 2013.
[18] M. Khouzani and S. Sarkar, "Maximum damage battery depletion attack in mobile sensor networks," *IEEE Trans. Autom. Control*, vol. 56, no. 10, pp. 2358–2368, 2011.
[19] D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko, "Botcoin: Monetizing stolen cycles," in *NDSS*, Citeseer, 2014.
[20] S. Eshghi, M. Khouzani, S. Sarkar, N. Shroff, and S. S. Venkatesh, "Optimal energy-aware epidemic routing in dtns," *IEEE Trans. Autom. Control*, vol. 60, no. 6, pp. 1554–1569, 2015.
[21] C. Singh, A. Kumar, and R. Sundaresan, "Delay and energy optimal two-hop relaying in delay tolerant networks," in *Proc. 8th Int. Symp. Modeling Optim. Mobile, Ad Hoc Wireless Networks (WiOpt)*, pp. 256–265, IEEE, 2010.
[22] K. Kandhway and J. Kuri, "How to run a campaign: Optimal control of sis and sir information epidemics," *Appl. Math. Computation*, vol. 231, pp. 79–92, 2014.
[23] M. Khouzani and S. Sarkar, "Dynamic malware attack in energy-constrained mobile wireless networks," in *Proc. Inform. Theory Appl. Workshop (ITA'10)*, pp. 1–11, IEEE, 2010.
[24] T. Kurtz, "Solutions of ordinary differential equations as limits of pure jump markov processes," *J. Appl. Probability*, pp. 49–58, 1970.
[25] N. Gast, B. Gaujal, and J. Le Boudec, "Mean field for Markov decision processes: From discrete to continuous optimization," *Arxiv Preprint arXiv:1004.2342*, 2010.
[26] M. Khouzani, S. Sarkar, and E. Altman, "A dynamic game solution to malware attack," in *Proc. IEEE INFOCOM'11*, pp. 2138–2146, IEEE, 2011.
[27] A. Seierstad and K. Sydsaeter, *Optimal Control Theory with Economic Applications*, vol. 20. North-Holland, 1987.
[28] S. Eshghi, S. Sarkar, and S. S. Venkatesh, "Visibility-aware optimal contagion of malware epidemics," *arXiv Preprint arXiv:1507.03528*, 2015.
[29] J. Stewart, "Calculus early transcendentals, 6e," Belmont, CA: Thompson Brooks/Cole, 2006.