Maximum Damage Malware Attack in Mobile Wireless Networks

M. H. R. Khouzani, *Student Member, IEEE*, Saswati Sarkar, *Member, IEEE*, and Eitan Altman, *Fellow, IEEE*

***Abstract*—Malware attacks constitute a serious security risk that threatens to slow down the large-scale proliferation of wireless applications. As a first step toward thwarting this security threat, we seek to quantify the maximum damage inflicted on the system due to such outbreaks and identify the most vicious attacks. We represent the propagation of malware in a battery-constrained mobile wireless network by an epidemic model in which the worm can dynamically control the rate at which it kills the infected node and also the transmission ranges and/or the media scanning rates. At each moment of time, the worm at each node faces the following tradeoffs: 1) using larger transmission ranges and media scanning rates to accelerate its spread at the cost of exhausting the battery and thereby reducing the overall infection propagation rate in the long run; or 2) killing the node to inflict a large cost on the network, however at the expense of losing the chance of infecting more susceptible nodes at later times. We mathematically formulate the decision problems and utilize Pontryagin Maximum Principle from optimal control theory to quantify the damage that the malware can inflict on the network by deploying optimum decision rules. Next, we establish structural properties of the optimal strategy of the attacker over time. Specifically, we prove that it is optimal for the attacker to defer killing of the infective nodes in the propagation phase until reaching a certain time and then start the slaughter with maximum effort. We also show that in the optimal attack policy, the battery resources are used according to a decreasing function of time, i.e., most aggressively during the initial phase of the outbreak. Finally, our numerical investigations reveal a framework for identifying intelligent defense strategies that can limit the damage by appropriately selecting network parameters.**

***Index Terms*—Communication systems security, epidemic modeling, mean-field convergence, optimal control.**

I. Introduction

A. Motivation

MALICIOUS self-replicating codes, known as malware, pose substantial threat to the wireless computing infrastructure. Malware can be used to launch attacks that vary from the less intrusive confidentiality or privacy attacks, such as traffic analysis and eavesdropping, to the more intrusive methods. Namely, they can either disrupt the normal functions of nodes such as relaying data and establishing end-to-end routes (e.g., sinkhole attacks [2]), or even alter the network traffic and hence destroy the integrity of the information, such as unauthorized access and session hijacking attacks , . Malware outbreaks such as Slammer and Code Red worms [3], [4] in the Internet inflicted expenses of billions of dollars in repair after the viruses rapidly infected thousands of hosts within a few hours. New investments have increasingly been directed toward wireless infrastructure thanks to the rapid growth of consumer demands and advancements in wireless technologies. The economic viability of these investments is, however, contingent on designing effective security countermeasures.

The first step in devising efficient countermeasures is to anticipate malware hazards and understand the threats they pose before they emerge in the hands of the attackers . Recognizing the above, specific attacks that utilize vulnerabilities in the routing protocols in a wireless sensor network such as the wormhole [5], sinkhole [2], and Sybil [6], and their countermeasures have been investigated before they were actually launched. We pursue the following complementary but closely related goals: 1) quantifying fundamental limits on the damage that the attack can inflict by intelligently choosing their actions; and 2) identifying the optimal actions that inflict the maximum damage on the network. Such a quantification is motivated by the fact that while attackers can pose serious threats by exploiting the fundamental limitations of wireless network, such as limited energy, unreliable communication, and constant changes in topology owing to mobility , their capabilities may be limited by the above as well since they rely on the same network for propagating the malware.

B. Decision Problems of the Attackers

Worms spread during data or control message transmission from nodes that are infected (i.e., *infectives*) to those that are vulnerable but not yet infected (i.e., *susceptibles*). We consider a pernicious worm that may: 1) eavesdrop; 2) analyze; 3) alter or destroy traffic; and 4) disrupt the infective host's normal functions (such as relaying data or establishing routes), and even *kill* the host, that is, render it completely dysfunctional (i.e., *dead*). This killing process may be triggered by executing a code that inflicts irretrievable hardware damage. For instance, Chernobyl virus [7] could reflesh the BIOS, corrupting the bootstrap program required to initialize the system. The worm can determine the time to kill a host, or equivalently the rate of killing the hosts, by regulating the time at which it triggers such codes.

Countermeasures can be launched by installing security patches that either *immunize* susceptible nodes against future attacks, by rectifying their underlying vulnerability, or *heal* the infectives of the infection and render them robust against

Manuscript received September 26, 2010; revised May 13, 2011; accepted November 12, 2011; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor S. Lu. Date of publication March 14, 2012; date of current version October 11, 2012. Parts of this paper were presented at the IEEE International Conference on Computer Communications (INFOCOM), San Diego, CA, March 15–19, 2010.

M. H. R. Khouzani is with the Dreese Laboratories, The Ohio State University, Columbus, OH 43210 USA (e-mail: khouzani@ece.osu.edu).

S. Sarkar is with the Electrical and Systems Engineering Department, University of Pennsylvania, Philadelphia, PA 19104 USA (e-mail: swati@seas.upenn.edu).

E. Altman is with INRIA, Sophia Antipolis 06902, France (e-mail: altman@sophia.inria.fr).

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/TNET.2012.2183642

future attacks. For instance, for SQL-Slammer worms [3], while StackGuard programs [8] immunize the susceptibles by removing the buffer overflow vulnerability that the worms exploit, specialized security patches [9] are required to remove the worm from (and thereby heal) the infectives. Nodes that have been immunized or healed are denoted as *recovered*. Thus, depending on whether the worm kills the infective before it fetches a security patch, the state of an infective changes to dead or recovered. States of susceptible nodes change to infective or recovered depending on whether they communicate with infectives before installing the security patches. Note that the countermeasures incur costs since the patches must be obtained through the bandwidth-limited wireless media involving energy-expensive communications, and potentially, different patches incur different costs depending on whether they treat susceptibles or infectives. Thus, such countermeasures must be resorted to judiciously.

The goal of the attacker is to infect as many nodes as possible, and use the worms to disrupt the hosts as well as the network functions, while being cognisant of the countermeasures . Killing an infective host sooner maximally disrupts its functions and thereby inflicts a damage on the network right away, but also prevents it from propagating the infection as well as eavesdropping, analyzing, altering, or destroying network traffic. Deferral of killing, on the other hand, may result in the host to be healed of the infection before it can be killed or infect other hosts. It is therefore nontrivial to determine the instantaneous rate of killing that maximizes the damage inflicted by the worm. Another important decision of the worm pertains to its optimal use of the available energy of the infective nodes. The infectives can accelerate the rate of spread of the worm by increasing their contact rates with susceptibles through selecting higher transmission gains and media scanning rates. Such a choice, however, depletes their limited energy reserves, which in turn restricts the spread of the infection and their other malicious functionalities.

C. Contributions

First, we construct a mathematical framework that cogently models the effect of the decisions of the attackers on the state dynamics and their resulting tradeoffs through a combination of epidemic models and damage functions (Section II). Specifically, we assume that the damage inflicted by the worm is a cumulative function increasing in the number of infective and dead hosts, both of which change with time. We allow the function to be fairly general, in that it can be either linear or nonlinear, and consider that the worm seeks to maximize the damage subject to satisfying certain constraints on the energy consumption of its hosts by dynamically selecting its killing rates and energy usages of its hosts while assuming full knowledge of the network parameters and the countermeasures. The maximum value of the aggregate damage function then quantifies the fundamental limits on the efficacy of the worm, particularly, since we assume that the worm has complete knowledge of all the contributing factors, and uses optimal dynamic strategies. The damage maximization turns out to be an elegant joint optimal control problem that can be solved numerically by applying Pontryagin's Maximum Principle [10], [11] (Section III).

Second, we answer the natural next question of whether in practice the worm can indeed inflict the damage quantified above, or the above quantifications constitute only theoretical upper bounds. Specifically, if the optimal policies that inflict the above maximum damage are complex to execute, then the worm may not be able to execute them since they are limited by the capabilities of their resource-constrained hosts. Toward this end, we investigate structures of the optimum policies for the worms. Our results are surprising and have negative connotations from the countermeasures point of view: We show that an attacker can inflict the maximum damage by using very simple decisions. We prove (Section V-A) that the optimal killing rate has the following simple structure: Until a certain time (which can be zero depending on the network and countermeasure parameters), the worm does not kill any host, and right after that, it annihilates its hosts at the maximum rate until the end of the optimization period (Theorem 1). Thus, the first phase is to *amass* the infectives, and then arrives the *slaughter* time. The result carries a qualitative cautionary message for countermeasures as well: An apparently inoffensive malware with little to no disruptive behavior might well be stacking infective hosts for an imminent carnage. In optimal control terminology, we have proven that the optimal strategy has a *bang-bang* structure; that is, at any given time, the killing rate is either at its minimum or maximum possible values. In addition, it has at most one jump that necessarily culminates at the maximum possible value. Optimality of this simple strategy for this nonlinear and nontrivial problem is indeed inauspicious from the defense point of view.

We next prove that when the energy consumption costs are strictly convex, the worm's optimal energy consumption rate is a decreasing function of time (Theorem 2). Thus, the worm seeks to infect as many hosts as possible early on by selecting the maximum possible values of the media scanning rates and transmission ranges, and thereafter starts to behave more conservatively so as to satisfy the energy consumption constraints. This inevitably slows the further spread of the worm toward the end of the optimization period, but then a large fraction of nodes have already been infected due to the choice of large values of these parameters early on. When the energy consumption costs are concave, the structure results are even more specific: The optimal media scanning rates and transmission ranges are not only decreasing functions of time, but also have a bang-bang nature with at most one jump from the maximum possible value to the minimum possible value.

Finally, we demonstrate how an understanding of the maximum value of the damage function can facilitate the design of suitable countermeasures. Our numerical computations confirm the intuition that the damage can be reduced if the nodes fetch the security patches at the maximum possible rate, and select the minimum possible reception gains so as to limit the communication rates between the infective and susceptible nodes (Section VI). However, both of the above incur costs for the system: the former owing to the energy-expensive communication of the patches through bandwidth-limited wireless media, and the latter owing to the disruption of desired data communications brought about by indiscriminate quarantining.[1] We devise a framework for determining the above parameters so as to minimize the overall network cost that increases with the

[1]A susceptible node does not know whether the node it is communicating with is infective or not, hence it cannot selectively reduce its reception gain.

damage and the costs associated with security patch installation and quarantining through reduction of reception gain.

D. Related Literature

Epidemic modeling based on the classic Kermack–McKendrick model [12] has extensively been used to analyze the spread of malware in wired networks [4], [13]–[18], etc., and more recently in wireless networks [19]–[21]. These works show, through simulations and matching with actual data, that when the number of nodes in a network is large, the deterministic epidemic models can successfully approximate the dynamics of the spread of the malware.

Dynamic control of parameters of the network or the worm have been investigated in several papers. Most of them, however, do not identify the optimal policies nor provide provable performance guarantees. Instead, they propose heuristic dynamic policies and evaluate through simulations the efficiencies and tradeoffs of the policies they propose. For example, [17] proposes heuristics for dynamic quarantining of nodes in wired networks that appear suspicious through traffic analysis, and [22] introduces heuristic strategies for dynamically adjusting the transmission power of attacker nodes in wireless networks. Relatively fewer works [23]–[26] have used analytical tools from optimal control theory to investigate network security, References [23]–[25] and [27] all adopt the viewpoint of the system (defense) and formulate the tradeoff for optimal treatment of the infective nodes. Reference [23] proposes reduction of reception gain of wireless nodes as a countermeasure for containing the spread of malware in wireless networks while imposing additional delays. References [25] and [26] investigate the tradeoffs regarding dissemination of security patches in a resource-constrained network. Only [26] focuses on the viewpoint of an attacker, but in contrast to this paper, considers only power consumption in transmission rate of the nodes as its control parameter. In our current work, we consider the transmission range of the infective nodes and the rate of killing as separate dynamic control functions of the worm that are, unlike [26], *jointly* optimized in order to inflict the maximum damage.

II. System Model

A. Dynamics of State Evolution

A *susceptible* node is a mobile device that is not contaminated by the worm, but is prone to infection. A node is *infective* if it is contaminated by the worm. An infective spreads the worm to a susceptible while transmitting data or control messages. The worm can *kill* an infective host, i.e., render it completely dysfunctional—we refer to such nodes as *dead*. A functional node that is immune to the worm is referred to as *recovered*. Installation of appropriate security patches can *immunize* susceptibles and *heal* infectives to the recovered states. Different security patches may be required for immunization and healing, as the first involves rectification of the vulnerability that the worm exploits, whereas the second entails the removal of the worm as well.

Let the total number of nodes in the network be N. Let the number of susceptible, infective, recovered, and dead nodes at time t be denoted by $n_S(t)$, $n_I(t)$, $n_R(t)$, and $n_D(t)$, respectively, and the corresponding fractions be $S(t) = n_S(t)/N$, $I(t) = n_I(t)/N$, $R(t) = n_R(t)/N$, and $D(t) = n_D(t)/N$, respectively (Table I). Then, $S(t) + I(t) + R(t) + D(t) = 1$. At the onset of the epidemic outbreak, i.e., at $t = 0$, some but not all nodes are infected: $0 < I(0) = I_0 < 1$. For simplicity, we assume $R(0) = D(0) = 0$. Thus, $S(0) = 1 - I_0$.

TABLE I
List of Notations of Measures

$S(t)$	measure of the Susceptible
$I(t)$	measure of the Infective
$R(t)$	measure of the Recovered
$D(t)$	measure of the Dead

We now model the dynamics of infection propagation in a mobile wireless network using epidemic models. Such epidemic models have been extensively verified for spread of a malware using experiments as well as network simulations (see, e.g., [19]–[21]). We elucidate the model using specific examples of delay-tolerant networks (DTNs) and 3G/4G networks with Multimedia Messaging Service (MMS). Infectives spread the malware during communication with susceptible nodes. An infective initiates communication with a susceptible when it generates a valid ID in cellular networks with MMS or detects the presence of a susceptible node in its communication range in a DTN. Each pair of infective-susceptible nodes at time t initiates communication at rate $\hat{\beta}u(t)$, where $u(t)$ is a (dynamic) parameter of control of the malware. The property that this rate is equal for each pair is a consequence of *homogenous mixing*. Nodes are assumed to be uniformly roaming the region. Hence, in the case of DTNs, a node is equally likely to enter the communication range of any of the other nodes, thus justifying the homogenous mixing assumption. Also, in a 3G/4G network, homogenous mixing property can arise when infective nodes generate the IDs of potential susceptibles uniformly randomly from a space of valid IDs.[2] Note that when an infective node searches for a new node, distinction between whether the nodes in its neighborhood are infective, susceptible, or recovered is difficult *a priori*.[3] Indeed, we assume that from an infective node's point of view, specific information about the state of the nodes in its neighborhood is not available to that infective node or to any other infective node. Hence, this information at best represents statistics about the average state of the whole network, which is identical for all infective nodes. Hence, at any given time t, the infective nodes use the same $u(t)$, as opposed to an individual-based strategy. The worm at an infective node kills the host (by invoking specific codes) at rate $\nu(t)$, another dynamically controlled parameter of the worm.

We now model the dynamics of healing and immunization. When the security patches are installed at an infective (susceptible, respectively), they are transformed into recovered. The rates of installation at any given time t are $B(I(t))$ and $Q(S(t))$, for infectives and susceptibles, respectively, where $B(\cdot)$, $Q(\cdot)$ are arbitrary functions that satisfy the following mild assumptions: $\lim_{x\to 0} B(x)$, $\lim_{x\to 0} Q(x)$ are finite, and

[2]Each pairwise communication involves two wireless hops between mobile nodes and access points (APs) or base stations (BSs), and one fast wireline backbone between the APs or BSs. The relative location of communicating nodes determines the number of hops in the fast backbone network for which, in comparison to the wireless channel, the delays are often negligible. Thus, the rate of intercontact times is not affected by the relative location of pairs.

[3]Unless the infective nodes exchanged information about their state, but that would make them vulnerable to detection.

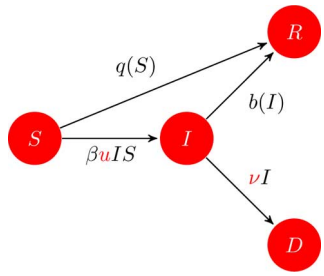

Fig. 1. Transitions. S, I, R, D respectively represent fraction of the susceptible, infective, recovered, and dead. $u(t)$ and $\nu(t)$ are the control parameters of the malware.

for $0 < x < 1$, $B(x)$, $Q(x)$ are positive and differentiable, $xB(x)$ is a concave nondecreasing function of x, and $xQ(x)$ is a nondecreasing function of x. These rates are associated with delays in detection of infection and fetching the appropriate security patch. Note that the functions $B(\cdot)$ and $Q(\cdot)$ are likely to be constants (e.g., $B(x) = B_0$, $Q(x) = Q_0$ for all x) in practice, and any constant function satisfies all of the above properties. Nevertheless, we allow more general functions (such as $Q(x) = x^\alpha$ for $\alpha > -1$ and $B(x) = x^\alpha$ for $-1 < \alpha < 0$) so as to accommodate more general cases such as where the detection delays decrease (and hence recovery rates increase) with increase in the number of infectives, which may lead to unusually high death rates and media access. Let

$$\beta = \lim_{N\to\infty} N\hat{\beta} \quad q(S) = Q(S)S \quad b(I) = B(I)I. \tag{1}$$

Our discussions lead to[4] the following system of differential equations representing the dynamics of the system:[5]

$$\dot{S}(t) = -\beta u(t) I(t) S(t) - q\left(S(t)\right) \quad S(0) = 1 - I_0 \tag{2a}$$
$$\dot{I}(t) = \beta u I(t) S(t) - b\left(I(t)\right) - \nu(t) I(t) \quad I(0) = I_0 \tag{2b}$$
$$\dot{D}(t) = \nu(t) I(t) \quad D(0) = 0 \tag{2c}$$

and also satisfy the following constraints at all t:

$$0 \le S(t), I(t), D(t) \tag{3a}$$
$$S(t) + I(t) + D(t) \le 1. \tag{3b}$$

Henceforth, wherever not ambiguous, we drop the dependence on t and make it implicit. Fig. 1 illustrates the transitions between different states of nodes.

Finally, owing to the technical assumptions we made on $B(\cdot)$ and $Q(\cdot)$, the functions $b(\cdot)$, $q(\cdot)$ exhibit the following properties: $b(0) = q(0) = 0$, and for $0 < I < 1$, $b(I)$, $q(S) > 0$, $b'(I) = db/\,dI \ge 0$, $q'(S) = dq/\,dS \ge 0$, and $b''(I) = d^2b/\,dI^2 \le 0$.

[4]The introduction of the set of differential equations system as the dynamics of the system can be made rigorous if further technical assumptions are made. Specifically, if $(n_S(t), n_I(t), n_D(t))$ constitutes a continuous-time Markov chain (CTMC), then according to the results of , as N grows, $S(t)$, $I(t)$, and $D(t)$ *converge* to the solution of the system of differential equation in the following sense:

$$\forall\, \epsilon > 0 \forall\, t > 0, \qquad \lim_{N\to\infty} \Pr\left\{\sup_{\tau \le t} \left| \frac{n_S(\tau)}{N} - S(\tau) \right| > \epsilon \right\} = 0.$$

Likewise for $I(t)$ and $D(t)$. Note that the CTMC property entails assuming that the intercontact times are exponentially distributed. For DTN networks, this property is shown for by Groenevelt *et al.* [29] under a number of mobility models such as random waypoint or random direction model .

[5]Variables with dot marks (e.g., $\dot{S}(t)$) will represent their time derivatives (e.g., time derivative of $S(t)$), and the prime signs (e.g., $q'(S)$) designate their derivatives with respect to their argument (e.g., S).

TABLE II
CONTROL VARIABLES OF THE WORM

$\nu(t)$	the rate of killing the infectives
$u(t)$	the transmission range times the scanning rate of the infectives

B. Maximum Damage Attack

We consider an attack that seeks to inflict the maximum possible damage in a time window $[0, T]$ of its choice. An attack can benefit over time from the infected hosts by using the worms to: 1) eavesdrop and analyze traffic that is generated or relayed by the infected hosts, or the traffic that traverses in the hosts' vicinity; and 2) alter or destroy the traffic that is generated or relayed by the infected hosts. An attacker also benefits by inflicting a large death-toll by the end of the desired time window. These motivate the following damage function:

$$J = \kappa D(T) + \int_0^T f\left(I(t)\right)\, dt. \tag{4}$$

where κ is an arbitrary nonnegative constant, and $f(\cdot)$ is an arbitrary nondecreasing, convex function such that $f(0) = 0$. Note that the assumptions on κ, $f(\cdot)$ are mild and natural, and a large class of functions, e.g., $f(I) = KI^\alpha$ for $\alpha \ge 1$ and $K \ge 0$, $f(I) = K(e^{\alpha I} - 1)$ for $\alpha, K \ge 0$, satisfy them. Finally, an attacker that simply seeks to maximize the final tally of the dead without any other agenda is readily representable by taking $f \equiv 0$.

The attacker seeks to maximize the aggregate damage by appropriately regulating its killing rate, $\nu(t)$, and the product of the transmission range and the scanning rate of the infective nodes, $u(t)$ (Table II), subject to

$$0 \le \nu(t) \le \nu_{\max} \quad 0 \le u_{\min} \le u(t) \le u_{\max} \tag{5a}$$
$$\int_0^T h\left(u(t)\right)\, dt \le C. \tag{5b}$$

The bound (5a) on $\nu(t)$ is imposed by limitations on the worm's speed of killing an infective host. The bound (5a) on $u(t)$ is dictated by the physical constraints of the transmitters and also for ensuring that the interference and hence collisions between simultaneous transmissions remain limited. In addition, the upper bounds on $\nu(t)$, $u(t)$ in (5a) have also been motivated by the fact that unusually high death rates or media access rates of nodes (i.e., infectives) expose anomalies that may lead to earlier detection of the malware. This may in turn motivate nodes to fetch appropriate security patches and therefore expedite the recovery of the nodes. The second constraint (5b)—referred to as the *battery* constraint—arises because enhancing $u(t)$ depletes the infective's battery, and the worm needs to ensure that the infective's battery lasts and it can continue to use it and to infect susceptibles for the time period of its operation $[0, T]$ (should it choose not to kill the host earlier). For appropriate functions, $h(\cdot)$ (e.g., $h(u) = K_1 u^r$, for $r \ge 2$), $\int_0^T h(u(t))\, dt$ is the energy consumed by the host if it is infected at $t = 0$ and is not killed before $t = T$—this is therefore an upper bound on the energy consumption of any infective while it remains infected.

We assume that the energy consumption in media scanning and malware transmission by the infective nodes is much larger than the energy expenditure as a result of other activities of the nodes, and therefore, the energy consumed by a host before it is infected is relatively insignificant. Thus, the worm chooses $u(t)$ so that the above upper bound does not exceed its maximum energy reserve, C.

It is natural to assume that $h(u)$ is nondecreasing and nonnegative. We allow $h(u)$ to be either convex or concave for $0 \leq u \leq u_{\max}$. We assume that $h(.)$ is differentiable. Note that when $h(u)$ represents power dissipation associated with u, $h(u)$ must be $K_1 u^r$, for $r \geq 2$ and some nonnegative K_1, and is therefore convex. However, if $h(u)$ represents a cost associated with power dissipation, then it may be concave as well. Finally, without loss of generality, $h(u_{\min}) = 0$, because if $h(u_{\min}) > 0$, we can equivalently consider $h(u_{\min}) = 0$, and reduce the bound C appropriately. Any pair of piecewise continuous functions $(\nu, u) : [0, T] \rightarrow \mathbb{R}^2$ such that the left- and right-hand limits exist and that satisfy the above constraints belongs to the *control region* denoted by Ω.

We next show that for any $(\nu, u) \in \Omega$, the state constraints in (3) are automatically satisfied throughout $(0 \ldots T]$. Thus, we ignore (3) henceforth.

Lemma 1: For any $(\nu, u) \in \Omega$, the state functions $(S, I, D) : [0, T] \rightarrow \mathbb{R}^3$ that satisfy the state equations and initial states in (2) also satisfy the state constraints in (3). Moreover, $S(t) \geq (1 - I_0)e^{-K_1 t} > 0$, $I(t) \geq I_0 e^{-K_2 t} > 0$ for $t \in [0, T]$ and some finite K_1, K_2.

The proof, provided in Appendix A, reveals that $K_1 = \beta u_{\max} + \max_{0 \leq x \leq 1} q'(x)$, $K_2 = \max_{0 \leq x \leq 1} b'(x)$.

Once the control (ν, u) is selected, the system state vector (S, I, D) is specified at all t as a solution to (2), and hence the value of the damage function J is determined as well. Thus, the control (ν, u) is considered only as a function of time rather than that of the system states, and since the value of J is determined only by the selection of (ν, u), we will henceforth denote J as $J(\nu, u)$ instead.

The state and control functions pair $((S, I, D), (\nu, u))$ is called an *admissible pair* if: 1) (ν, u) is in Ω; and 2) equations in (2) hold. The function (ν, u) is then called an admissible control. Let $((S, I, D), (\nu, u))$ be an admissible pair. If

$$J(\nu, u) \geq J(\underline{\nu}, \underline{u}) \qquad \text{for any admissible control } (\underline{\nu}, \underline{u})$$

then $((S, I, D), (\nu, u))$ is called an *optimal solution* and (ν, u) is called an *optimal control* of the problem.

In order to obtain fundamental bounds on the efficacy of the attack, we assume that the attacker computes its optimal control assuming full knowledge of the network and defense parameters, such as β, $b(\cdot)$, $q(\cdot)$, etc. We also assume that the system selects the above parameters *a priori* and does not change them with time. The damage can only be equal or lower if the countermeasures are adaptive or the attacker does not know the above parameters.

III. Worm's Optimal Control

We now present a framework using which the worm can determine its *optimal control* functions (ν, u) and also compute the maximum value of the damage function.

The main challenge in computing the optimal control is that the differential (2) can be solved provided that the functions (ν, u) are known. Thus, the only approach seems to be that of an exhaustive search on all functions (ν, u) in Ω. This will require the evaluation of the damage function $J(\nu, u)$ for each pair of such functions where the corresponding (I, D) functions required in evaluating $J(\nu, u)$ are obtained by solving (2) for each such pair. However, Ω consists of an uncountably infinite number of such pairs, which rules out an exhaustive search. Pontryagin's Maximum Principle, however, provides an elegant tool for solving this seemingly impossible problem, which we apply next.

First, we introduce a new state variable E to transform the constraint in (5b) to a more analytically amenable form

$$\dot{E}(t) = -h(u) \quad E(0) = 0 \tag{6}$$

$$\text{with the final constraint:} \qquad E(T) \geq -C. \tag{7}$$

Now, note that (6) and (7) are together equivalent to (5b). Thus, the optimal control problem posed in Section II can now be modified to augment (2) with (6) and (7), and omit (5b), without any alteration in the set of optimal solutions and in the maximum value of the damage function. We consider this version henceforth.

Let $((S, I, D), (\nu, u))$ be an optimal solution. Consider the *Hamiltonian* H, and *co-state* or *adjoint* functions $\lambda_1(t)$ to $\lambda_4(t)$, and a scalar $\lambda_0 \geq 0$ defined as follows:

$$\begin{aligned} H :=& \lambda_0 f(I) + (\lambda_2 - \lambda_1)\beta u I S - \lambda_1 q(S) - \lambda_2 b(I) \\ &+ (\lambda_3 - \lambda_2)\nu I - \lambda_4 h(u). \end{aligned} \tag{8}$$

$$\begin{aligned} \dot{\lambda}_1 &= -\frac{\partial H}{\partial S} = -(\lambda_2 - \lambda_1)\beta u I + \lambda_1 q' \\ \dot{\lambda}_2 &= -\frac{\partial H}{\partial I} = -\lambda_0 f' - (\lambda_2 - \lambda_1)\beta u S + \lambda_2 b' - (\lambda_3 - \lambda_2)\nu \\ \dot{\lambda}_3 &= -\frac{\partial H}{\partial D} = 0 \\ \dot{\lambda}_4 &= -\frac{\partial H}{\partial E} = 0 \end{aligned} \tag{9}$$

along with the transversality conditions (i.e., constraints on the final values of the co-state functions)

$$\lambda_1(T) = 0 \quad \lambda_2(T) = 0 \quad \lambda_3(T) = \lambda_0 \kappa \tag{10a}$$

$$\lambda_4(T) \geq 0 \tag{10b}$$

$$\lambda_4(T)(E(T) + C) = 0. \tag{10c}$$

Then, according to Pontryagin's maximum principle with terminal constraints ([10, Theorem 3.14, p.111]), there exist continuous and piecewise continuously differentiable co-state functions $\lambda_1, \lambda_2, \lambda_3$, and λ_4, and constant $\lambda_0 \geq 0$ that, at every point $t \in [0 \ldots T]$ where $(\nu(\cdot), u(\cdot))$ is continuous, satisfy (9) and the transversality conditions (10), and we have

$$\vec{\lambda} \not\equiv \vec{0} \tag{11a}$$

$$(\nu, u) \in \arg \max_{(\underline{\nu}, \underline{u}) \in \Omega} H(\vec{\lambda}, (S, I, D), (\underline{\nu}, \underline{u})). \tag{11b}$$

Referring to (9), $\dot{\lambda}_4 = 0$, and thus λ_4 is a constant, which, according to (10), is nonnegative. Now assume that $\lambda_4 > 0$, then by scaling the Hamiltonian and the co-states by $1/\lambda_4$, the equations are still satisfied with $\lambda_4 = 1$. Thus, if $\lambda_4 > 0$, we

can take $\lambda_4 = 1$ without loss of generality. The case for $\lambda_4 = 0$ can be handled very easily and is discussed in Sections V-A and V-B as remarks.

Here, we show that the constant λ_0 is positive. This is because if otherwise $\lambda_0 = 0$, then (9) for $(\lambda_1, \lambda_2, \lambda_3)$ constitutes a *linear autonomous ordinary differential equation* (ODE) with the final constraint of $(\lambda_1, \lambda_2, \lambda_3)(T) = \vec{0}$ that, from vector space theory [30], has the unique solution of $(\lambda_1, \lambda_2, \lambda_3)(t) = \vec{0}$. Also, from (9) and (10b), λ_4 is a nonnegative constant. Thus, either $\lambda_4 = 0$ or $\lambda_4 = \text{constant} t > 0$ for all t. The case of $\lambda_4 = 0$ contradicts the necessary condition of $\vec{\lambda} \not\equiv \vec{0}$ of (11a). Now consider the case of $\lambda_4 = \text{constant} > 0$ for all t. The Hamiltonian in (8) reduces to $H = -\lambda_4 h(u)$. Thus, maximization of Hamiltonian leads to $u(t) = u_{\min}$ for all $0 \le t \le T$. This means $\int_0^T h(u)\,dt < C$ or $E(T) > -C$, and thus $\lambda_4(T)(E(T) + C) > 0$, which contradicts (10c). Therefore, λ_0 cannot be zero.

Define the switching function φ as the following:

$$\varphi := (\lambda_3 - \lambda_2) I \tag{12}$$

which is a continuous and piecewise continuously differential function of time and, referring to (10), has the following final value:

$$\varphi(T) = \lambda_0 \kappa I(T) > 0. \tag{13}$$

The positivity comes from the facts $\lambda_0 > 0$, $\kappa > 0$, and $I > 0$ according to Lemma 1. Also let ψ be defined as follows:

$$\psi := (\lambda_2 - \lambda_1)\beta I S \tag{14}$$

which too is a continuous and differential function of time and according to (10) has zero final value

$$\psi(T) = 0. \tag{15}$$

Introduction of φ and ψ, along with $\lambda_4 = 1$, allow us to rewrite the Hamiltonian in (8) as follows:

$$H = \lambda_0 f(I) - h(u) + \psi u - \lambda_1 q - \lambda_2 b + \varphi\nu. \tag{16}$$

According to Pontryagin's Maximum Principle in (11b), we have

$$H(S, I, D, \nu, u, \lambda_1, \lambda_2, \lambda_3) \ge H(S, I, D, \underline{\nu}, \underline{u}, \lambda_1, \lambda_2, \lambda_3) \quad \text{over all admissible } \underline{\nu}, \underline{u}. \tag{17}$$

Hence, the optimal ν satisfies $\varphi\nu \ge \varphi\underline{\nu}$, where $\underline{\nu}$ is any admissible controller, i.e., $\underline{\nu} \in [0 \dots \nu_{\max}]$. Thus, to find the optimal controller, one needs to maximize the linear function $\varphi\nu$ over the admissible set $\nu \in [0 \dots \nu_{\max}]$, which yields

$$\nu = \begin{cases} 0, & \varphi < 0 \\ \nu_{\max}, & \varphi > 0 \end{cases} \tag{18}$$

hence the name switching function. An immediate observation of the above property is the following important property:

$$\varphi\nu \ge 0. \tag{19}$$

Also note that according to (13), $\varphi(T) > 0$, and thus by continuity of φ and following (18), $\nu = \nu_{\max}$ over an interval of nonzero length toward the end of $(0 \dots T)$ interval that extends until time T.

Again, from (16) and according to (17), the optimal u satisfies $\psi u - h(u) \ge \psi\underline{u} - h(\underline{u})$, where $\underline{u}$ is any admissible controller, i.e., $\underline{u} \in [u_{\min} \dots u_{\max}]$. Thus, to find the optimal u, one needs to maximize the function $\psi u - h(u)$ over the admissible set $u \in [0 \dots u_{\max}]$. We separately consider the cases of strictly convex $h(\cdot)$ and concave $h(\cdot)$:

1) Strictly Convex $h(u)$: The function $\psi u - h(u)$ is strictly concave in u over the admissible interval, and the maximizer is found by comparing the values of three candidates of $u_{\min}$, $u_{\max}$, and the $u \in (u_{\min} \dots u_{\max})$ at which the derivative of this expression becomes zero. This yields

$$u = \begin{cases} u_{\min}, & \psi \le h'(u_{\min}) \\ h'^{-1}(\psi), & h'(u_{\min}) < \psi \le h'(u_{\max}) \\ u_{\max}, & h'(u_{\max}) < \psi. \end{cases} \tag{20}$$

This shows that u is a continuous function of ψ, and thus according to the continuity of the ψ, u is a continuous function of time. Therefore, the co-state functions are differentiable at every point at which the other control, i.e., ν, is continuous.

2) Concave $h(u)$: For this case, $\psi u - h(u)$ is convex in u, and a maximizer u is found by comparing the only two candidates $u_{\min}$ and $u_{\max}$. This readily yields the following:

$$u = \begin{cases} u_{\min}, & \psi < \rho \\ u_{\max}, & \psi > \rho \end{cases} \tag{21}$$

where $\rho := \frac{h(u_{\max})}{u_{\max} - u_{\min}} \ge 0$.

For both strictly convex and concave $h(u)$, referring to (15) and following (20) and (21), we have $u(T) = u_{\min}$.

Implementing (18), (20), and (21) into (2), (9), and (10), we obtain a system of (nonlinear) differential equations with specified initial or final values that involve only the state and co-state functions (and not the control (ν, u)). Functions λ_1 to λ_4 and scalar λ_0 that satisfy the above differential equations and boundary values can therefore be obtained using standard numerical procedures that solve differential equations [30]. Now, the optimal control (ν, u) can be obtained using the above solutions in (18) and (20) and (21).

IV. Structure of the Maximum Damage Attack

Whether in practice the worm can indeed inflict the maximum damages developed in this paper depends on implementability of the optimal strategies. Specifically, if the optimal policies that inflict the maximum damage are complex, then the worm may not be able to execute them since they are limited by the capabilities of their resource constrained hosts as well. Inauspiciously, though, we show that optimal attack strategies follow simple structures (Theorems 1 and 2) that make them conducive to implementation. Fig. 2 provides visualization of the theorems.

Recall that one of the basic tradeoffs that the attacker was faced with was the perfect timing to kill an infective node. Specifically, should an attacker kill a node as soon as it is infected so as to have claimed a casualty and secured a large damage on the network? Theorem 1 states the opposite.

Theorem 1: Consider an optimal solution pair (ν, u) that jointly maximizes the worm's damage function in (4) subject to the constraints in (5a) and (5b). Then, $\nu(t)$ has the following characteristics: $\exists t_1 \in [0 \dots T)$ such that $\nu(t) = 0$ for $0 < t < t_1$ and $\nu(t) = \nu_{\max}$ for $t_1 < t < T$.

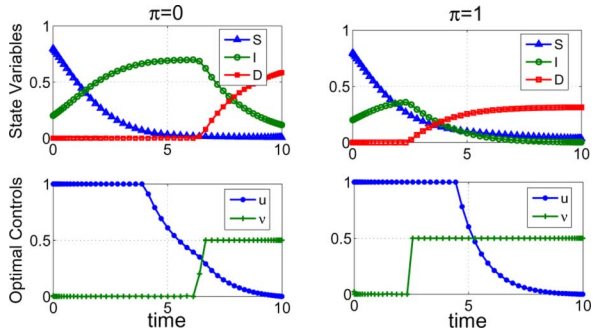

Fig. 2. Evaluation of the optimal controllers and the according states as functions of time. Here, $h(u) = u^2$, $\beta = 0.9$, $u_{\max} = 1$, $\gamma = 0.2$, and *(left)* $\pi = 0$ and *(right)* $\pi = 1$. Thus, $\beta u_{\max} = 0.9 > 0.4 \geq (\gamma + \pi\gamma)$. Therefore, the fast-healing regime does not hold. However, as we can see, the pattern for optimal u is consistent with the statement of Theorem 2 and strictly convex $h(u)$.

In other words, an optimal $\nu(\cdot)$ is of *bang-bang* form; that is, it possesses only two possible values $\nu_{\max}$ and 0 and switches abruptly between them. It has at most one such jump, which necessarily culminates at $\nu_{\max}$. Thus, the theorem says that although killing a node early on would ensure partial damage, the overall damage is more if this decision is deferred until toward the end of the attacking period despite the risk of recovery of the infective node by the system. Specifically, at the start of the outbreak, the number of susceptibles is high, and infective nodes can be used to further propagate the infection. Subsequently, the level of susceptibles drops due to both spread of infection and immunization effort by the system. At a certain threshold, the risk of recovery of the infective nodes in the remaining time outweighs the potential benefit by spreading the infection. At this point, whose exact value depends on the parameters of the case, the malware starts killing the nodes with the maximum possible rate. This will ensure that infective nodes are maximally used for spread of the infection and for the attacker's malicious activities.

Recall that $b(0) = q(0) = 0$, and $b(I)$, $q(S)$ are increasing functions of I, S for I, $S \in [0 \dots 1]$. In order to derive structural properties for optimal u, we assume further that there exist positive constants $\hat{b}$ and $\hat{q}$ such that

$$\forall I, S \in [0 \dots 1], \quad b(I) \geq \hat{b} I \text{ and } q(S) \geq \hat{q} S \tag{22}$$

and

$$\hat{b} + \hat{q} \geq \beta u_{\max}. \tag{23}$$

$\beta u_{\max}$ is the maximum rate of the spread of the infection, and intuitively, the above condition describes the scenario in which the recovery rate $(\text{healing} + \text{immunization})$ is larger than the maximum rate of the spread of the infection. We will refer to this assumption as *fast-recovery* regime assumption.

Theorem 2: Assuming fast-recovery regime, any optimal $u(t)$ for the case of strictly convex $h(u)$ consists of the following *phases*:

1) $u = u_{\max}$ on $0 < t \leq t_0 < T$ for some $t_0 \geq 0$;
2) u strictly and continually decreases on $t_0 < t \leq t_1 < T$ for some $t_1 \geq t_0$;
3) $u = u_{\min}$ on $t_1 < t \leq T$.

For the case of a concave $h(u)$, any optimal u consists of only phase 1 followed by phase 2, i.e., $u = u_{\max}$ until time t_0 and subsequently $u = u_{\min}$.

Although Theorem 2 is presented assuming fast-recovery regime, our numerical results show that these structural results hold even when this assumption is relaxed (Section VI).

According to Theorem 2, the product of the optimal media scanning rate and transmission range is always a nonincreasing function of time. Specifically, the most intense (battery-consuming) spreading effort of malware should take place at the start of the outbreak. Intuitively, this is because initially the number of susceptibles is high, and hence an infective contacts more susceptibles by using the same u initially than later. Moreover, if a node is infected earlier, it will have more time to further propagate the infection. Subsequently, owing to the overall energy limitations, as the level of susceptibles as potential preys drop, infectives should reduce their media scanning rates so as not to exhaust their spreading battery budget. The structure of an optimal u turns out to subtly depend on whether the h function is strictly convex or concave. We can have an intuitive explanation for this phenomenon: a slight reduction in the value of u results in a higher decrease in the instantaneous power for a strictly convex $h(u)$ than for a concave $h(u)$. Therefore, in the case of strictly convex $h(u)$, it is beneficial to reduce u continuously (instead of keeping u at $u_{\max}$ before a threshold time) and prolong the battery lifetime for malicious activities of the malware.

In summary, Theorems 1 and 2 provide the joint optimal attack as follows: Initially, the highest effort of the malware is focused on spreading the malware and amassing infectives without killing any. Subsequently, the reverse course of action is taken: Battery is used at lower rates, and at a threshold time, the amassed nodes are slaughtered at the highest rate that lasts till the end of the interval.

Note that the optimal killing policy (ν), as well as the spreading effort (u) for the case of concave $h(u)$, are completely specified by the (only possible) jump points. Also, the optimal media scanning strategy (u) for a strictly convex h can be simply divided into at most three phases, characterized by at most two time epochs. Therefore, no continuous global coordination of attack is necessary. In particular, the threshold times can be computed once an estimate of the parameters of the network $(\beta, q(S), b(I), C)$ is made, and can be subsequently incorporated into the code of the malware. Given the flexibility provided by software-driven devices, the infective nodes can subsequently execute these strategies without coordinating any further among themselves or with any central entity. The transition times can be determined by solving a system of differential equations, as described in previous sections. Such systems can be solved very fast due to the existence of efficient numerical algorithms for solving differential equations, and the computation time is constant in that it does not depend on the number of nodes N. Note also that our algorithms do not require any local or global information as time progresses and only the initial information is sufficient to determine the decision of infective nodes for the entire interval.

In Section V, we provide the proofs for both of the theorems.

V. Proofs of Theorems 1 and 2

We first obtain some properties of the Hamiltonian and system states that we subsequently use to establish Theorems 1 and 2.

Lemma 2: $H = \text{constant} > 0$.

Proof: First, the system is autonomous, i.e., the Hamiltonian and the control region do not have an explicit dependency on the independent variable t. Hence, ([11, p. 236])

$$H(S(t), I(t), D(t), \nu(t), u(t), \lambda_1(t), \lambda_2(t), \lambda_3(t)) \equiv \text{constant}. \tag{24}$$

Therefore, from (16)

$$H = H(T) = \lambda_0 f(I(T)) + \lambda_0 \kappa \nu(T) I(T). \tag{25}$$

We showed [after (11)] that $\lambda_0 > 0$, and following Lemma 1, $I(T) > 0$; also $\nu(T) = \nu_{\max} > 0$, as we argued after (18). Thus, $H(T) > 0$. ∎

The second observation is that I satisfies the following condition.

Lemma 3: $(f'(I)I - f(I)) \geq 0$ and $(b(I) - b'(I)I) \geq 0$ for all $t \in [0 \ldots T]$.

Proof: By Lemma 1, I and S are nonnegative. Define $\xi(I) = f'(I)I - f(I)$. Since $f(0) = 0$, we have $\xi(0) = 0$. Also

$$\frac{d}{dI}\xi(I) = \xi' = f''(I)I + f'(I) - f'(I) = f''(I)I.$$

Following Lemma 1 and properties of f, we observe that $\xi' \geq 0$ for all $t \in [0 \ldots T]$. Thus, since $\xi(0) = 0$, $\xi(I) = f'(I) - f(I)I \geq 0$ for all $t \in [0 \ldots T]$. Likewise for b. ∎

We will also use the following key lemma in the sequel.

Lemma 4: For all $t \in (0 \ldots T)$, we have $\lambda_1 \geq 0$ and $(\lambda_2 - \lambda_1) > 0$.

The proof of this lemma is in Appendix D. We are now ready to proceed to the proofs of the theorems.

A. Proof of Theorem 1: Optimal Rate of Killing

Proof: To establish the statement of the theorem, we will show that the switching function φ is equal to zero at at most one time epoch. The theorem subsequently follows from the relation between φ and ν given by (18).

Let us begin by stating two simple real analysis properties that we prove in Appendixes B and C, respectively.

Property 1: Let $f(t)$ be a continuous and piecewise continuously differentiable function of t. Assume $f(t_0) > L$. Now if $f(t_1) = L$ for the first time before t_0, i.e., $f(t_1) = L$ and $f(t) > L$ for all $t \in (t_1 \ldots t_0]$, then $\dot{f}(t_1^+) \geq 0$.[6]

Property 2: Let $f(t)$ be a continuous and piecewise continuously differentiable function of t. Assume t_1 and t_2 to be its two consecutive L-crossing points, that is, $f(t_1) = f(t_2) = L$ and $f(t) \neq L$ for all $t_1 < t < t_2$. Now if $\dot{f}(t_1^+) \neq 0$ and $\dot{f}(t_2^-) \neq 0$, then $\dot{f}(t_1^+)$ and $\dot{f}(t_2^-)$ must have opposite signs.

Let us calculate the time derivative of the φ function wherever (ν, u) is continuous

$$\begin{aligned}
\dot{\varphi} &= (\dot{\lambda}_3 - \dot{\lambda}_2)I + \dot{I}\frac{\varphi}{I} && [\because (12)] \\
&= (\lambda_0 f' + (\lambda_2 - \lambda_1)\beta u S - \lambda_2 b' \\
&\quad + (\lambda_3 - \lambda_2)\nu)I + \dot{I}\frac{\varphi}{I} && [\because (9)] \\
&= \lambda_0 f' I + \psi u - \lambda_2 b' I + \varphi\nu + \dot{I}\frac{\varphi}{I} \\
&\quad + (H - \lambda_0 f - \psi u + \lambda_1 q \\
&\quad + \lambda_2 b - \varphi\nu + h(u)) && [\because (16)] \\
&= H + \lambda_1 q + \lambda_0(f'I - f) \\
&\quad + \lambda_2(b - b'I) + h(u) + \dot{I}\frac{\varphi}{I}. && (26)
\end{aligned}$$

Let a time at which $\varphi = 0$ be denoted by τ. From (26), we obtain

$$\begin{aligned}
\dot{\varphi}(\tau^+) = \dot{\varphi}(\tau^-) &= H + \lambda_1 q + \lambda_0(f'I - f) \\
&\quad + \lambda_2(b - b'I) + h(u). && (27)
\end{aligned}$$

Equation (27), positivity of λ_0, and Lemmas 1–4 show that $\dot{\varphi}(\tau^-)$, $\dot{\varphi}(\tau^+) > 0$ wherever (ν, u) is continuous. First, this shows that φ cannot be equal to zero over an interval of nonzero length. To see this, note that otherwise, due to piecewise continuity of ν and u, there exists a subinterval inside the interval of $\varphi = 0$ over which (ν, u) is continuous. Thus, φ is differentiable over this subinterval, and $\dot{\varphi} = 0$ in this subinterval, which is not possible. Thus, referring to (18), ν is bang-bang, i.e., $\nu \in \{0, \nu_{\max}\}$ except in a set of measure 0.

Second, referring to Property 2, we conclude that $\varphi = 0$ at at most one point inside $(0 \ldots T)$ interval. Since [from (13)] $\varphi(T) > 0$ and because φ is a continuous function of time, $\varphi(t) > 0$ for an interval of nonzero length toward the end of $(0 \ldots T)$. If $\varphi(t) > 0$ for all $0 \leq t \leq T$, then $\nu = 0$ throughout the interval. Otherwise, there exists a $t_0 \in [0 \ldots T]$ such that $\varphi(t) < 0$ for $t_1 < t \leq T$ and $\varphi(t) > 0$ for $0 \leq t < t_1$. Theorem 1 now follows from the relation between optimal ν and φ in (18). ∎

Remark on the Case of $\lambda_4 = 0$: The Hamiltonian in (16) for this case turns into

$$H = \lambda_0 f(I) + \psi u - \lambda_1 q - \lambda_2 b + \varphi\nu.$$

Note that maximization of H with respect to ν [as stated in (17)] does not change at all, and hence the same arguments in the proof apply.

B. Proof of Theorem 2: Optimal Scanning Rate/Tx Range

The optimal u is given by (20) and (21) in terms of $\psi(t)$. We first show that function ψ is a strictly decreasing function of time (Lemma 5). Subsequently, we establish the statement of the theorem by investigating the implication of Lemma 5 on the structure of u for cases of strictly convex $h(u)$ and concave $h(u)$ separately.

Lemma 5: $\psi(t)$ is a strictly decreasing function of time for $0 \leq t \leq T$.

Proof: Let us calculate the time derivative of the ψ function wherever it exists (that is, wherever (ν, u) is continuous)

$$\begin{aligned}
\dot{\psi} &= (\dot{\lambda}_2 - \dot{\lambda}_1)\beta I S + \dot{I}\frac{\psi}{I} + \dot{S}\frac{\psi}{S} && [\because (14)] \\
&= [-\lambda_0 f' - (\lambda_2 - \lambda_1)\beta u S + \lambda_2 b' \\
&\quad - \frac{\varphi}{I}\nu + (\lambda_2 - \lambda_1)\beta u I - \lambda_1 q']\beta I S \\
&\quad + (\beta u I S - b - \nu I)\frac{\psi}{I}
\end{aligned}$$

[6]For a general function $f(x)$, the notations $f(x_0^+)$ and $f(x_0^-)$ are defined as $\lim_{x \downarrow x_0} f(x)$ and $\lim_{x \uparrow x_0} f(x)$, respectively. We denote $\dot{f}(t^+)$ as the right-side time derivative of f at time t.

$$
\begin{aligned}
&+(-\beta uIS-q)\frac{\psi}{S} && [\because (2),(9)]\\
&=-\lambda_0 f'\beta IS+\lambda_2 b'\beta IS\\
&\quad-\varphi\nu\beta S-\lambda_1 q'\beta IS\\
&\quad+(-b-\nu I)\frac{\psi}{I}+(-q)\frac{\psi}{S}\\
&\quad+\Big\{-H\beta S+[\lambda_0 f-h+\psi u-\lambda_1 q\\
&\qquad-\lambda_2 b+\varphi\nu]\beta S\Big\} && [\because (16)]\\
&=-H\beta S+(f-f'I)\lambda_0\beta S\\
&\quad+\lambda_2(b'I-b)\beta S-\lambda_1 q'\beta IS-\lambda_1 q\beta S\\
&\quad\left(-\frac{b}{I}-\frac{q}{S}+u\beta S\right)\psi-\nu\psi-\beta Sh. && (28)
\end{aligned}
$$

In Lemmas 2 and 4, we showed that H is a positive constant and $\lambda_1 \geq 0$ for all $t \in [0 \dots T]$. From Lemma 4, λ_2 is also nonnegative. Also recall that by definition, $\psi = (\lambda_2 - \lambda_1)\beta IS$. By Lemmas 1 and 4, $\psi(t) \geq 0$ for all t, $0 \leq t \leq T$. These facts along with the assumptions in (22) and (23) and Lemmas 1 and 3 show that $\dot{\psi} < 0$ wherever (ν, u) is continuous (fact-I). Recall that (ν, u) is continuous except potentially at finite number of time epochs. From Pontryagin Maximum Principle, states and co-states and hence ψ are continuous functions of time (fact-II). The lemma now follows from fact-I and fact-II. ■

We are now ready to prove Theorem 2. We consider the cases of strictly convex $h(\cdot)$ and concave $h(\cdot)$ separately.

1) Strictly Convex $h(u)$:

Proof: Since by Lemma 5 ψ is a strictly decreasing (and continuous) function of time and since for a strictly convex h, $h'(u_{\min}) < h'(u_{\max})$, there exist t_0 and t_1, $0 \leq t_0 < t_1 \leq T$, such that $\psi \geq h'(u_{\max})$ for $t \in [0 \dots t_0]$, $h'(u_{\min}) < \psi < h'(u_{\max})$ for $t \in [t_0 \dots t_1)$ and $\psi \leq h'(u_{\max})$ for $t \in [t_1 \dots T]$. From (20), $u = u_{\max}$ over the first interval and $u = u_{\min}$ over the last interval. According to (10), $\psi(T) = 0$, and due to continuity of ψ, the last interval is of nonzero length. Thus, we only need to show that u is a strictly decreasing function of time during $[t_0 \dots t_1)$. From (20), for this interval we have $u = h'^{-1}(\psi)$. For a strictly convex h, $h'^{-1}(\psi)$ is strictly increasing in its argument, i.e., ψ. Hence, from Lemma 5, $h'^{-1}(\varphi)$ is a strictly decreasing function of time. This concludes the proof. ■

2) Concave $h(u)$:

Proof: Since according to Lemma 5, ψ is a strictly decreasing (continuous) function of time, $\psi = \rho$ at at most one time epoch, t_0. Specifically, $\psi > \rho$ for $t \in [0 \dots t_0)$ and $\psi < \rho$ for $t \in (t_0 \dots T]$. The theorem now readily follows from (21). ■

Remark on the Case of Concave $h(\cdot)$ and $u_{\min} = 0$: When $u_{\min} = 0$ (which is not unnatural to assume), then Theorem 2 for concave $h(.)$ holds without the fast-healing assumption, which we explain briefly here. The idea is to show ψ has negative (right and left) time derivatives at ρ-crossing points, and hence arguing similar to the proof of Theorem 1. This can be shown by referring to (28) and rearranging to obtain the term $\beta S(\psi u - h(u))$ where all of the other terms are negative. Let a ρ-crossing time epoch of ψ be denoted by τ. Since u is piecewise continuous except for finite number of time epochs, $u(\tau^+)$ and $u(\tau^-)$ is either $u_{\min} = 0$ or $u_{\max}$, for both of which we have $(\rho u - h(u)) = 0$, and hence the term $\beta S(\psi u - h(u))$ vanishes from the equation, proving that ψ has negative side time derivatives at its ρ-crossing points. We can now apply Property 2, as we did in proof of Theorem 1, to derive the statement of Theorem 2 for concave $h(\cdot)$.

Remark on the Case of $\lambda_4 = 0$: The Hamiltonian in (16) for this case turns into

$$H = \lambda_0 f(I) + \psi u - \lambda_1 q - \lambda_2 b + \varphi\nu.$$

Thus, according to (17), an optimal u needs to maximize ψu. By definition in (14), $\psi = (\lambda_2 - \lambda_1)\beta IS$, which according to Lemmas 1 and 4 is always strictly positive, and thus the optimal u is trivially $u = u_{\max}$ for the entire interval of $[0 \dots T]$. Intuitively, when the battery reserve is sufficient to use $u_{\max}$ throughout the interval, it is trivially optimal to do so.

VI. Numerical Computations

Our numerical computations are designed to complement our analysis in Sections IV and V. We compare the efficacy of our dynamic policy against two heuristic policies for a variety of parameters. We investigate the effect of some of the issues related to implementation of optimal dynamic attacks such as approximate parameter estimation and imperfect timings. We use the insights revealed by these computations in designing efficient countermeasures.

We chose[7] $T = 10$, $I_0 = 0.1$, $\beta = 0.4$, $u_{\max} = 1$, $\nu_{\max} = 0.5$, $u_{\min} = 0$, $f(I) = 0.1I$, $\kappa = 1$, $h(u) = u^2$ (which is strictly convex), and $C = 5$. We have selected C such that the choice of $u(t) = u_{\max}$ for all $t \in [0, T]$ violates the battery constraint of (5b). Also, we take $Q(x) = \gamma$ and $B(x) = \pi\gamma$ for all $x \in [0, 1]$, i.e., $q(S) = \gamma S$ and $b(I) = \pi\gamma I$. Here, $\pi \in \{0, 1\}$ determines whether the countermeasure involve only immunizing the susceptibles ($\pi = 0$) or the same security patch can successfully remove the infection, if any, and immunize a node against future infection ($\pi = 1$). We refer to γ as the recovery rate and take $\gamma = 0.2$.

Our first observation is that for all ranges of parameters that will follow in this section, the structural results of Theorems 1 and 2 for the optimal solution hold, even when the regime is not fast-recovery, which we assumed while proving Theorem 2. One example is Fig. 2, which depicts the optimal controllers as well as the states as functions of time.

Next, we investigate the effects that changing different parameters of the system have on the optimal controllers. According to Figs. 3 and 4, we observe that increasing the recovery rate (γ) generally does the following:

- decreases the jump time in the ν (Fig. 3);
- extends the initial period during which $u = u_{\max}$ and makes the subsequent descent in u sharper (Fig. 4).

Intuitively, this phenomenon can be explained in the following manner: In a system with a large recovery rate, both the susceptible and infective nodes recover rapidly. Hence, the worm should use more of its power resources early on and also starts killing them earlier in order not to lose many nodes to the pool of recovered. Note also that the starting time of the killing is more sensitive to the value of recovery rate when

[7]For our numerical calculations, we used the PROPT software designed by Tomlab Optimization, Inc. Specifically, each instance of our optimal control problems took 1 s, using an Intel Xeon CPU X5355, 2.66 GHz 8 GB RAM, 2 GB swap memory machine.

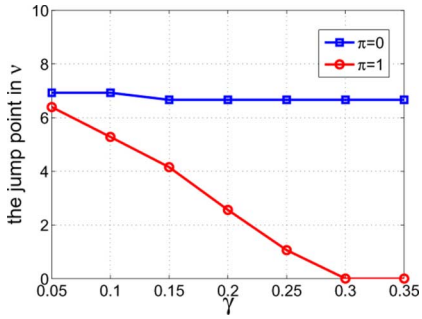

Fig. 3. Jump points of optimal ν (starting time of the slaughter period) versus γ for both $\pi = 0$ and $\pi = 1$. Note that for $\pi = 1$ and for $\gamma \geq 0.30$, malware starts killing the infectives from time zero.

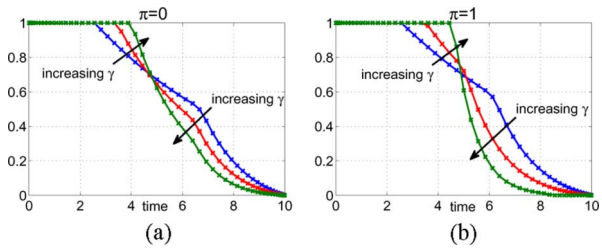

Fig. 4. Optimal u (media scanning rate times the transmission rates of infectives) for different values of γ for both (a) $\pi = 0$ and (b) $\pi = 1$.

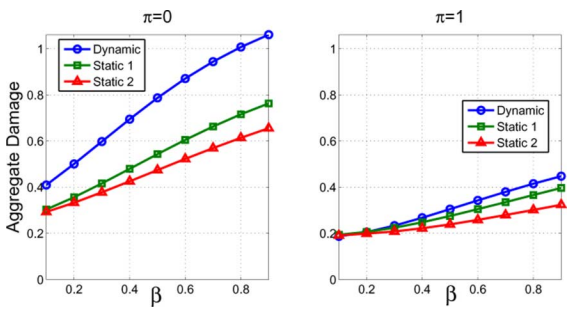

Fig. 5. Comparison of the aggregate damage inflicted by our dynamic policy versus two heuristic policies: Static 1 and Static 2. Varying β.

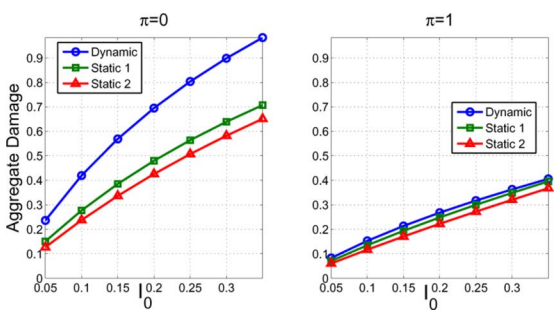

Fig. 6. Comparison of the aggregate damage inflicted by our dynamic policy versus two heuristic policies: Static 1 and Static 2. Varying I_0.

$\pi = 1$. This is because for $\pi = 0$, the security patches can only immunize the susceptibles, and once a node is infective, it will not be recovered by the system.

Next, we compare the efficacy of our dynamic policies against two heuristic policies for various ranges of parameters. In the first heuristic policy, u starts initially at $u_{\max}$ until

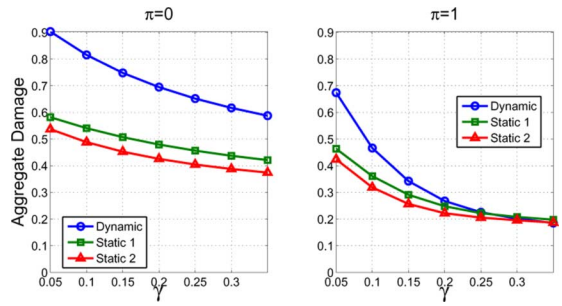

Fig. 7. Comparison of the aggregate damage inflicted by our dynamic policy versus two heuristic policies: Static 1 and Static 2. Varying γ.

time $\min(C/u_{\max}^2, T)$,[8] after which it switches off to zero. The value of the ν is fixed throughout. The fixed value of ν is varied *a priori*, and the one that yields the maximum damage is selected. We call this policy *Static 1*. In the second heuristic policy, both u and ν are set to fixed *a priori* values throughout the operation interval. u is set to the fixed value of $\min(u_{\max}, \sqrt{C/T})$,[9] so that throughout the interval, the battery condition is not violated but is maximally used. The fixed value of the ν is then selected similar to Static 1. We refer to this new policy as *Static 2*. As we observe in Figs. 5–9, for all ranges of changing β, I_0, γ, C, and $\nu_{\max}$, the order of maximum inflicted damage is as follows: *Dynamic* > *Static 1* > *Static 2*. The advantage of dynamic attacks over heuristic attack is more pronounced for $\pi = 0$ and can exceed 50% increase. The trend of damage with change of each parameter is intuitive. Interestingly, when $\pi = 1$, that is when the security patches can heal and immunize the infectives as well as the susceptibles, not only is the overall damage lower, but also the dynamic efficacy of the attacker (i.e., the advantage of using optimal dynamic policies) is reduced.

Robustness of our dynamic policy is the subject of the next investigation. In practice, the malware may not accurately know the network and defense parameters (e.g., β, γ, π), and only have access to rough estimates.[10] We assess the drop in the efficacy of the attack as a result of inaccurate parameter estimations. We apply our dynamic policies as well as heuristic policies that are calculated based on estimations of one parameter with potential inaccuracy of 50% and assuming that the estimates are identical across infectives. We then depict (Fig. 10) the total cost incurred by applying these suboptimal policies. The horizontal axis is the estimated value of the parameters where the center point is the value of the parameter in reality. Specifically, in Fig. 10(a), the real value of β is 0.4, and in Fig. 10(b), the real value of γ is 0.2. As we can observe, the decrease in the aggregate damage as a result of 50% inaccuracy in the estimation of the value of β [Fig. 10(a)] and γ [Fig. 10(b)] is less than

[8]Note that for our numerical calculations, $h(u) = u^2$. Thus, the battery constraint [in (5b)] for this heuristic policy is translated to $\int_0^T u_{\max}^2 \mathbf{1}_{t<t^*}\, dt \leq C$, where t^* is the threshold time. This yields $t^* = \min(C/u_{\max}^2, T)$, as provided in the text.

[9]To see this, note that the battery constraint [in (5b)] is now $\int_0^T u_0^2\, dt \leq C$, which gives $u_0 = \min(u_{\max}, \sqrt{C/T})$, as stated in the text.

[10]For instance, in DTNs, each initial infective may measure the number of nodes it detects per unit time if it scans the medium at a rate u_0. This number is $(N-1)\beta u_0 \approx N\beta u_0 \approx \beta u_0$ [refer to (1)]. Thus, each infective can estimate β using its knowledge of u_0. If the infectives subsequently average their estimate, all of them will have the same estimate for β.

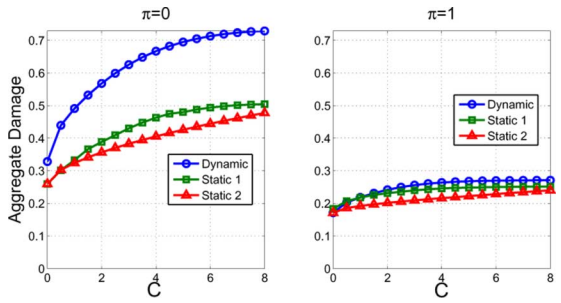

Fig. 8. Comparison of the aggregate damage inflicted by our dynamic policy versus two heuristic policies: Static 1 and Static 2. Varying C.

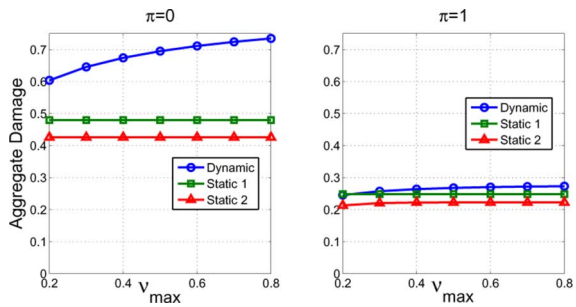

Fig. 9. Comparison of the aggregate damage inflicted by our dynamic policy versus two heuristic policies: Static 1 and Static 2. Varying $\nu_{\max}$.

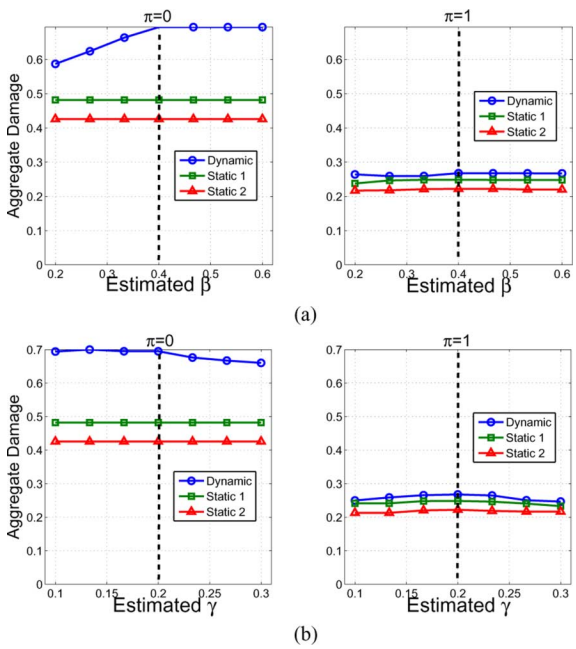

Fig. 10. Robustness of the optimal dynamic policy against parameter estimation when the estimation errors are identical across all infectives. The dotted line designates the real value of the parameters (the center of the x-axis). (a) Estimating β. (b) Estimating γ

15%. Also, the dynamic policy consistently outperforms both the static policies despite the estimation errors.

We now consider the case that different infectives have different estimates of the network and defense parameters and calculate the optimal control based on their own estimations. First, each infective has an estimate for γ that differs from the real value (e.g., 0.2) by an error term that is uniformly distributed

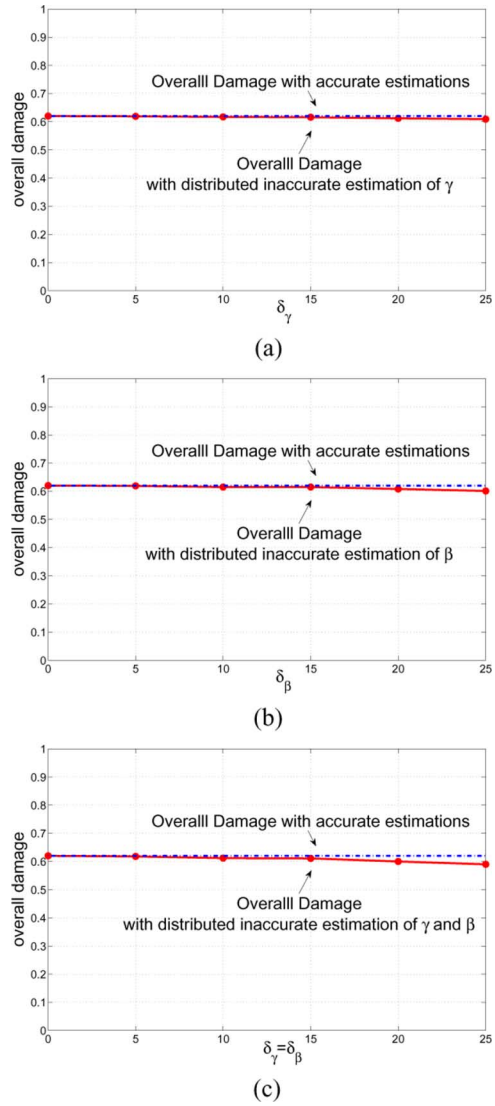

Fig. 11. Robustness of the optimal dynamic policy against parameter estimation when the estimation errors are independently distributed across the infectives. (a) Estimating γ. (b) Estimating β. (c) Estimating both β, γ.

between $-\delta_\gamma/100 \times 0.2$ and $+\delta_\gamma/100 \times 0.2$ (hence δ_γ is the percentage of error). The estimation errors for different infectives are independent. The resulting overall damage (averaged over 50 runs) is depicted in Fig. 11(a). A similar experiment is conducted for individual erroneous estimations of β with error percentages of δ_β and the real value as 0.4 [Fig. 11(b)]. Finally, the case where both β and γ are estimated by each node with error $(\delta_\gamma = \delta_\beta)$ is considered [Fig. 11(c)]. The estimation errors only marginally reduce the overall efficacy of the attack.

In practice, drifts in local clocks of the nodes make exact timing of the execution of the dynamic policies difficult and may affect the overall damages that a malware can inflict on the network. Here, we evaluate the overall damage when infective nodes' clocks drift from the global clock by different amounts, and hence they choose dynamic policies that are shifted aside in time from the global control by their individual (additive) drifts. We chose clock drifts that are statistically independent and uniformly distributed between $-\Delta \times T$ and $\Delta \times T$. Fig. 12 depicts the overall damage versus Δ averaged over 100 simulation runs where the number of nodes is 50. Note that even for Δ as large

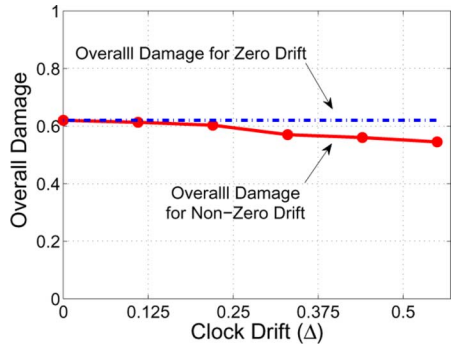

Fig. 12. Robustness of the dynamic attack strategy with respect to clock drift.

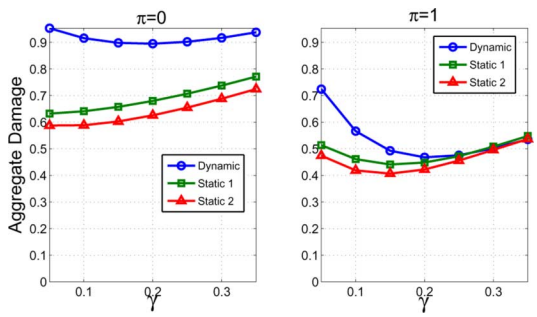

Fig. 13. System cost (malware's damage + the cost of patching) versus γ (rate of patching).

as 0.5, the decrease in the overall damage as compared to the zero-drift case is less than 11%.

Finally, we examine how the identification of the maximum damage attack facilitates the design of effective countermeasures. Specifically, we investigate how the system can choose the countermeasure parameters, i.e., the recovery rates and the reception gains of the nodes, while planning for the worst-case scenario that the attacker chooses the optimal dynamic attack policy assuming full knowledge of the values of the above parameters. As anticipated, our numerical computations reveal that higher recovery rates (larger γ) and lower reception gains of the nodes (smaller β) reduce the damage due to the attack (Figs. 7 and 5, respectively). However, increasing the recovery rate is achieved through greater usage of costly resources such as bandwidth and power, and thereby inflicts a recovery cost on the system. Likewise, decreasing the reception gain of the nodes, thus indiscriminate quarantining of nodes, disrupts the functionality of networks by introducing delay and hence deteriorating the quality of service (note that a susceptible node does not know whether the node it is communicating with is infective or otherwise *a priori*, hence it cannot selectively reduce its reception gain). We consider the overall system cost as the sum of the following: 1) the damage caused by the worm; 2) the expense of providing the immunization and healing rates of γ; and 3) the cost due to deterioration of the QoS, which is inversely proportional to the intercontact rates β. The system faces a tradeoff in choosing the least costly recovery and quarantining (reduced intercontact) rates, which we resolve numerically. In Fig. 13, we have plotted the overall system cost assuming a simple linear recovery cost induced by γ (specifically $1 \times \gamma$). In Fig. 14, we adopt $0.1/\beta$ as the QoS cost, inspired by the work in [29] in which the authors show the

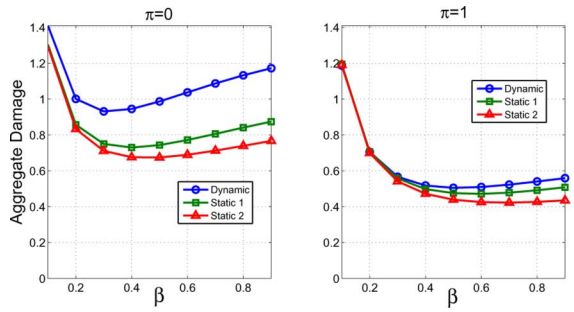

Fig. 14. System cost (malware's damage + the cost of quarantining) versus β.

average delay in a DTN is proportional to β^{-1}. In each case, the overall cost is minimized at unique values of γ and β that constitute robust choices for the countermeasure.

VII. Conclusion, Discussion, and Future Research

We considered a future malware that can dynamically change its parameters in response to the changes in the state of the network in order to maximize its overall damage. We constructed an optimal-control framework that models the effect of the decisions of the attackers on the state dynamics and their resulting tradeoffs through a combination of epidemic models and damage functions. Specifically, we considered a worm that can decide the killing time of the nodes and the transmission rate from infected nodes, subject to a total energy expenditure budget. Next, using Pontryagin's Maximum Principle and simple real analysis arguments, we showed that an attacker can inflict the maximum damage by using very simple decisions. Finally, we demonstrated how an understanding of the maximum value of the damage function can facilitate the design of robust countermeasures.

The epidemiological differential (2) captures the state evolution in any network provided the infectives and susceptibles mix homogenously. In the Internet, this occurs when infectives uniformly randomly generate IP addresses of susceptibles, and the communication times between different node pairs do not significantly differ based on the topology. The latter holds in most topologies owing to the presence of high-speed links that have substantially reduced communication times between node pairs irrespective of their geographical distance. The constraint (5b) does not, however, arise in wireline networks because nodes are typically not battery-powered. Equivalently, we can consider constraint (5b) with a C that is so large that (5b) holds even when $u(t) = u_{\max}$ at all t, and thus our theorems still can be applied. Specifically, using Theorem 1, the optimal killing strategy, $\nu(\cdot)$, is fully specified once the optimum switching time t_1 is computed, which may be accomplished using the numerical computation framework developed in Section III.

In practice, the attacker may only be able to estimate the network and countermeasure parameters, such as β, $b(\cdot)$, $q(\cdot)$, which may also dynamically evolve depending on the congestion and interference levels in the network and also the network's response to the attack. Our simulations reveal that the attack is robust to estimation errors. Nevertheless, identifying attack strategies that are provably robust to errors in estimation of the network and defense parameters, e.g., a control function that maximizes the minimum damage over a range of values of the parameters, remains open. It is not *a priori* clear whether

such strategies exhibit the simple structures as established when the attacker knows the exact values of these parameters. Formulating stochastic optimal control problems that consider the above parameters as random processes and lend to optimal control strategies that seamlessly adapt to their dynamic fluctuations over time constitutes an interesting direction for future research.

APPENDIX A
PROOF OF LEMMA 1

Proof: All S, I, and D, resulting from (2), and thus any continuous functions of them, are continuous functions of time. We first show that if there exists t_0 such that we have $0 < S$, I throughout $(0, t_0)$, then $S(t_0) \geq S(0)e^{-K_1 t_0}$, where $K_1 = \beta u_{\max} + \max_{0\leq x\leq 1} q'(x)$, and $I(t_0) \geq I(0)e^{-K_2 t_0}$, where $K_2 = \max_{0\leq x\leq 1} b'(x)$. The second statement will now follow if we can prove the first and since $0 < S(0) = 1 - I(0) < 1$. Now, let $0 < S$, I throughout $(0, t_0)$. For $0 \leq t < t_0$, from (2a) we have $\dot{S} \geq -\beta u S - q(S) \geq -K_1 S$. Hence, $S(t) \geq S(0)e^{-K_1 t} \geq S(0)e^{-K_1 t_0}$ for all $0 \leq t < t_0$. Since S is continuous, $S(t_0) \geq S(0)e^{-K_1 t_0}$. Similarly, we can show that $I(t_0) \geq I(0)e^{-K_2 t_0}$. The result follows.

We now prove the first statement. Since $0 < I_0 < 1$, the initial conditions in (2) ensure that the state constraints (3) are strictly met at $t = 0$. The continuity of S and I functions ensures that there exists an interval of nonzero length starting at $t = 0$ on which both S and I are strictly positive. Thus, from (2c) and since $\nu(t) \geq 0$, $\dot{D} \geq 0$ in the above interval. Thus, since $D(0) = 0$, $0 \leq D$ in this interval as well. Since $\frac{d}{dt}(S + I + D)|_{t=0} = -q(S_0) - b(I_0) < 0$ and $S(0) + I(0) + D(0) = 1$, there exists an interval after $t = 0$ over which the constraint in (3b) is strictly met.

Suppose the first statement does not hold. Now, let $t_0 \leq T$ be the first time after $t = 0$ at which at least one of the constraints of $0 \leq S, I$ and $S+I+D \leq 1$ becomes active, or $0 \leq D$ becomes violated right after it. That is, at t_0, we have: 1) $S = 0$ OR 2) $I = 0$ OR 3) $S+I+D = 1$ OR 4) there exists an $\epsilon > 0$ such that $D < 0$ on $(t_0 \dots t_0 + \epsilon)$; AND throughout $(0, t_0)$, we have $0 < S, I$ and $S+I+D < 1$ and $D \geq 0$. Thus, from the first paragraph in this proof, $S(t_0) \geq S(0)e^{-K_1 t_0} > 0, I(t_0) \geq I(0)e^{-K_2 t_0} > 0$. Thus, since $S(0) > 0$, $I(0) > 0$, neither 1) nor 2) could have happened. Let $P_1 = S(0)e^{-K_1 t_0}$, $P_2 = I(0)e^{-K_1 t_0}$. Also, $\frac{d}{dt}(S + I + D) = -q(S) - b(I) \leq -q(P_1) - b(P_2) < 0$ throughout $[0 \dots t_0]$. Since $S(0) + I(0) + D(0) = 1$ we have $(S+I+D)|_{t=t_0} < 1$, showing that 3) is impossible. Moreover, from (2a), and since $I(t_0) > 0$, and I is continuous, there exists an ϵ' such that $\dot{D} \geq 0$ over $(t_0 \dots t_0 + \epsilon')$. From continuity of D, $D(t_0) \geq 0$. Thus, $0 \leq D$ over $(t_0 \dots t_0 + \epsilon')$, dismissing 4). This negates the existence of t_0. Thus, the first statement holds by contradiction. ∎

APPENDIX B
PROOF OF PROPERTY 1

Proof: Proof by contradiction. Suppose that Property 1 did not hold, thus $f(t_1) = L$, $\dot{f}(t_1^+) < 0$, and hence $\exists \delta_1 \in (0 \dots t_0)$ such that $f(t_1 + \delta_1) < L$. However, by the Intermediate Value Theorem (IVT), there must exist a time $t_1 + \delta_1 < \tau < t_0$ such that $f(\tau) = L$. This contradicts the assumption that $f(t) \neq L$ for all $t_1 < t < t_0$. ∎

APPENDIX C
PROOF OF PROPERTY 2

Proof: We prove the property for $\dot{f}(t_1^+) > 0$. The proof follows similarly if $\dot{f}(t_1^+) < 0$. We have, $f(t_1) = L$, $\dot{f}(t_1^+) > 0$, and hence $\exists \delta_1 \in \left(0 \dots \frac{1}{2}(t_2 - t_1)\right)$ such that $f(t_1 + \delta_1) > L$. Suppose that Property 2 did not hold, and $\dot{f}(t_2^-) > 0$. Then, $f(t_2) = L$, $\dot{f}(t_2^-) > 0$, which implies $\exists \delta_2 \in \left(0 \dots \frac{1}{2}(t_2 - t_1)\right)$ such that $f(t_2 - \delta_2) < L$. However, now by the IVT, there must exist a time $t_1 + \delta_1 < \tau < t_2 - \delta_2$ such that $f(\tau) = L$. This contradicts the assumption that $f(t) \neq L$ for all $t_1 < t < t_2$. ∎

APPENDIX D
PROOF OF LEMMA 4

Proof:

Step 1: Following (10), $\lambda_2(T) = (\lambda_2(T) - \lambda_1(T)) = 0$ and from (9) and (10) and the discussion following (20), $(\dot{\lambda}_2(T) - \dot{\lambda}_1(T)) = -\lambda_0 f'(I(T)) - \kappa\nu(T)$, that is strictly negative. Thus, there exists an $\epsilon_1 > 0$ such that on the interval of $(T - \epsilon_1 \dots T)$, we have $(\lambda_2 - \lambda_1) > 0$. Also recall from (10) that $\lambda_1(T) = 0$.

Step 2: Proof by contradiction. Let t^* be defined as follows:

$$t^* := \inf_{0\leq t\leq T} \Bigg\{ t | \lambda_1(t) \geq 0, \text{ and } (\lambda_2(t) - \lambda_1(t)) > 0. \text{ on the interval } (t \dots T) \Bigg\}.$$

If $t^* = 0$, then we are done. Suppose $t^* > 0$. According to the continuity of λ_1 and λ_2, and following Step1, we must have

$$\lambda_2(t^*) - \lambda_1(t^*) = 0 \text{ OR, } \lambda_1(t^*) = 0.$$

Case 1: $\lambda_2(t^*) - \lambda_1(t^*) = 0$. From the continuity of λ_1, $\lambda_1(t^*) \geq 0$. We have

$$\begin{aligned}
&\left[\frac{d}{dt}(\lambda_2 - \lambda_1)](t^{*+}) = \frac{d}{dt}(\lambda_2 - \lambda_1)\right](t^{*-}) \\
&= -\lambda_0 f' + \lambda_2 b' - \frac{\varphi}{I}\nu - \lambda_1 q' && [\because (9)] \\
&= -\lambda_0 f' + \lambda_2 b' - \frac{\varphi}{I}\nu - \lambda_1 q' \\
&\quad - \frac{H}{I} + \lambda_0 \frac{f}{I} - \frac{\lambda_1 q}{I} - \frac{\lambda_2 b}{I} + \frac{\varphi}{I}\nu - \frac{h}{I} && [\because (16)] \\
&= \frac{\lambda_0}{I}[f - f'I] + \frac{\lambda_2}{I}[b'I - b] - \lambda_1 q' \\
&\quad - \frac{\lambda_1 q}{I} - \frac{H}{I} - \frac{h}{I}. && (29)
\end{aligned}$$

From Lemma 3, $[f - f'I] \leq 0$ and $[b'I - b] \leq 0$. Also in this case, $\lambda_2(t^*) = \lambda_1(t^*)$ (by assumption of the case), and $\lambda_1(t^*) \geq 0$. Now following Lemmas 1 and 2, (29), and properties of $q(S)$, we observe that $\left[\frac{d}{dt}(\lambda_2 - \lambda_1)\right](t^{*+}) = \frac{d}{dt}(\lambda_2 - \lambda_1)](t^{*-}) < 0$. According to Property 1, this is a contradiction. Thus, Case 1 could not occur.

Case 2: $\lambda_2(t^*) - \lambda_1(t^*) > 0$, and $\lambda_1(t^*) = 0$, and $\forall \delta > 0$, there exists $t_1 \in (t^* - \delta \dots t^*)$ such that $\lambda_1(t_1) < 0$. From continuity of λ_1 and λ_2, $\exists \epsilon > 0$ such that on $(t^* - \epsilon \dots t^*)$, $\lambda_2 - \lambda_1 > 0$, and hence according to (9) and Lemma 1, wherever (ν, u) is continuous, $\dot{\lambda}_1 \leq \lambda_1 q'$. Now consider a $\delta < \epsilon$, and

define $\hat{t}$ to be the point that has the lowest value of λ_1 on the interval of $[t^* - \delta \ldots t^*]$. According to the assumption of Case 2, $\lambda_1(\hat{t})$ is strictly negative. Thus, $\dot{\lambda}_1(\hat{t}^+) \leq \lambda_1(\hat{t}^*)q'(S(\hat{t}^+)) < 0$. This, along with continuity of λ_1, implies that in the right neighborhood of $\hat{t}$, λ_1 has lower values than $\lambda_1(\hat{t})$. This contradicts the definition of $\hat{t}$.

Therefore, none of the two cases could occur, which contradicts the existence of t^*. Hence, the lemma follows. ■

REFERENCES

[1] M. Khouzani, S. Sarkar, and E. Altman, "Maximum damage malware attack in mobile wireless networks," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Netw.*, vol. 1, no. 2–3, pp. 293–315, 2003.

[3] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," *IEEE Security & Privacy*, vol. 1, no. 4, pp. 33–39, Jul.–Aug. 2003.

[4] C. Zou, W. Gong, and D. Towsley, "Code red worm propagation modeling and analysis," in *Proc. 9th ACM Conf. Comput. Commun. Security*, 2002, pp. 138–147.

[5] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. IEEE INFOCOM*, 2003, vol. 3, pp. 1976–1986.

[6] J. Douceur, "The sybil attack," in *Proc. 1st IPTPS*, Cambridge, MA, Mar. 7–8, 2002, pp. 251–260.

[7] F.-S. C. T. Page, "F-secure virus descriptions: Cih," 2009 [Online]. Available: http://www.f-secure.com/v-descs/cih.shtml

[8] C. Cowan, C. Pu, D. Maier, H. Hintony, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, and Q. Zhang, "Stackguard: Automatic adaptive detection and prevention of buffer-overflow attacks," in *Proc. 7th USENIX Security Symp.*, 1998, vol. 7, pp. 5–5.

[9] Symantec, "W32.sqlexp.worm," 2007.

[10] D. Grass, A. Vienna, J. Caulkins, and P. Rand, *Optimal Control of Nonlinear Processes*. Berlin, Germany: Springer-Verlag, 2008.

[11] D. Kirk, *Optimal Control Theory: An Introduction*. Upper Saddle River, NJ: Prentice-Hall, 1970.

[12] D. Daley and J. Gani, *Epidemic Modelling: An Introduction*. Cambridge, U.K.: Cambridge Univ. Press, 2001.

[13] J. Kephart, S. White, I. Center, and Y. Heights, "Directed-graph epidemiological models of computer viruses," in *Proc. IEEE Comput. Soc. Symp. Res. Security Privacy*, 1991, pp. 343–359.

[14] J. Kephart, S. White, I. Center, and Y. Heights, "Measuring and modeling computer virus prevalence," in *Proc. IEEE Comput. Soc. Symp. Res. Security Privacy*, 1993, pp. 2–15.

[15] A. Wagner, T. Dübendorfer, B. Plattner, and R. Hiestand, "Experiences with worm propagation simulations," in *Proc. ACM Workshop Rapid Malcode*, 2003, pp. 34–41.

[16] Z. Chen, L. Gao, and K. Kwiat, "Modeling the spread of active worms," in *Proc. IEEE INFOCOM*, 2003, vol. 3, pp. 1890–1900.

[17] C. Zou, W. Gong, and D. Towsley, "Worm propagation modeling and analysis under dynamic quarantine defense," in *Proc. ACM Workshop Rapid Malcode*, 2003, pp. 51–60.

[18] G. Kesidis, I. Hamadeh, and S. Jiwasurat, "Coupled Kermack-Mckendrick models for randomly scanning and bandwidth saturating internet worms," in *Proc. 3rd QoS-IP*, 2005, pp. 101–109.

[19] S. Tanachaiwiwat and A. Helmy, "Encounter-based worms: Analysis and defense," *Ad Hoc Netw.*, vol. 7, no. 7, pp. 1414–1430, 2009.

[20] R. Cole, "Initial studies on worm propagation in MANETs for future army combat systems," Tech. Rep., DTIC Doc., 2004.

[21] S. Tanachaiwiwat and A. Helmy, "VACCINE: War of the worms in wired and wireless networks," in *Proc. IEEE INFOCOM*, 2006, pp. 05–859.

[22] V. Karyotis and S. Papavassiliou, "Risk-based attack strategies for mobile Ad Hoc networks under probabilistic attack modeling framework," *Comput. Netw.*, vol. 51, no. 9, pp. 2397–2410, 2007.

[23] M. H. R. Khouzani, E. Altman, and S. Sarkar, "Optimum quarantining of wireless malware through reception gain control," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 49–61, Jan. 2012.

[24] M. Khouzani, S. Sarkar, and E. Altman, "Optimal propagation of security patches in mobile wireless networks: Extended abstract," in *Proc. ACM SIGMETRICS*, 2010, pp. 355–356.

[25] M. Khouzani, S. Sarkar, and E. Altman, "Dispatch then stop: Optimal dissemination of security patches in mobile wireless networks," in *Proc. 49th IEEE CDC*, 2010, pp. 2354–2359.

[26] 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, Oct. 2011.

[27] X. Yan and Y. Zou, "Optimal Internet worm treatment strategy based on the two-factor model," *ETRI J.*, vol. 30, no. 1, p. 81, 2008.

[28] T. Kurtz, "Solutions of ordinary differential equations as limits of pure jump Markov processes," *J. Appl. Probab.*, vol. 7, no. 1, pp. 49–58, 1970.

[29] R. Groenevelt, P. Nain, and G. Koole, "The message delay in mobile ad hoc networks," *Perform. Eval.*, vol. 62, no. 1–4, pp. 210–228, 2005.

[30] M. Hirsch and S. Smale, *Differential Equations, Dynamical Systems, and Linear Algebra*. New York: Academic, 1974.

M. H. R. Khouzani (S'11) received the B. Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2006, and the M.S.E. and Ph.D. degrees in electrical and systems engineering from the University of Pennsylvania, Philadelphia, in 2008 and 2011, respectively, under a fellowship award and the supervision of Prof. Saswati Sarkar.

Since August 2011, he has been doing postdoctoral research with Prof. Ness B. Shroff with the Dreese Laboratories, Electrical and Computer Engineering Department, The Ohio State University, Columbus. His research interests are in stochastic optimization, optimal control, and dynamic games in wireless networks.

Saswati Sarkar (S'98–M'00) received the M.E. degree in electrical communication engineering from the Indian Institute of Science, Bangalore, India, in 1996, and the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park, in 2000.

She joined the Electrical and Systems Engineering Department, University of Pennsylvania, Philadelphia, as an Assistant Professor in 2000, and is currently an Associate Professor. Her research interests are in stochastic control, resource allocation, dynamic games, and economics of networks.

Dr. Sarkar was an Associate Editor of the IEEE TRANSACTION ON WIRELESS COMMUNICATIONS from 2001 to 2006. She is currently an Associate Editor of the IEEE/ACM TRANSACTIONS ON NETWORKING. She received the Motorola Gold Medal for the best Master's student in the division of electrical sciences at the Indian Institute of Science and a National Science Foundation (NSF) Faculty Early Career Development Award in 2003.

Eitan Altman (M'93–SM'00–F'10) received the B.Sc. degree in electrical engineering, B.A. degree in physics, and Ph.D. degree in electrical engineering from the Technion—Israel Institute of Technology, Haifa, Israel, in 1984, 1984, and 1990, respectively, and the B.Mus. degree in music composition from Tel-Aviv University, Tel-Aviv, Israel, in 1990.

Since 1990, he has been a Researcher with the National Research Institute in Computer Science and Control (INRIA), Sophia-Antipolis, France. His areas of interest include networking, stochastic control, and game theory. More information can be found at http://www-sop.inria.fr/members/Eitan.Altman/.

Dr. Altman has been on the Editorial Boards of several scientific journals: *Wireless Networks*, *Computer Networks*, *Computer Communications*, *Journal of Discrete Event Dynamic Systems* , *SIAM Journal of Control and Optimisation*, *Stochastic Models*, and *Journal of Economy Dynamic and Control*. He received the Best Paper Award in the Networking 2006, IEEE GLOBECOM 2007, and IFIP Wireless Days 2009 conferences. He is a coauthor of two papers that have received the Best Student Paper awards (at QoFis 2000 and at Networking 2002).