Optimal Quarantining of Wireless Malware Through Reception Gain Control

MHR. Khouzani, Eitan Altman, Saswati Sarkar

***Abstract*—Containment of worms constitutes an important challenge in mobile wireless networks as recent outbreaks have revealed actual vulnerabilities. We introduce a defense strategy that quarantines the malware by reducing the communication range. This counter-measure confronts us with a trade-off: reducing the communication range suppresses the spread of the malware, however, it also deteriorates the network performance. We model the propagation of the malware as a deterministic epidemic. Using an optimal control framework, we select the optimal communication range that captures the above trade-off by minimizing a global cost function. Using Pontryagin's Maximum Principle, we derive structural characteristics of the optimal communication range as a function of time for general cost functions. Our numerical computations reveal that the dynamic optimal control of the communication range significantly outperforms static choices and is also robust to errors in estimation of the network and attack parameters.**

I. Introduction

Malicious computer softwares, in the form of worms, have inflicted enormous damages on computer networks. For instance, during an outbreak of Code Red on July 19, 2001, hundreds of thousands of computers were infected in a blazing speed, inflicting repair costs of billions of dollars [2]. Worms, as self-replicating codes, have the potential of exploiting their infected hosts to infect other nodes and exponentially multiply the number of their victims: a phenomenon that we call epidemic. Thus detection and containment of malware have drawn substantial attention among the Internet research community ([2]–[5] etc). However, a new battle-field has emerged: personal mobile devices such as cell-phones, smart-phones and pocket-PCs are acquiring more computation and communication capabilities, and hence, new vulnerabilities are introduced. The sprouting popularity of these mobile devices combined with their new capabilities have created an ideal prey-ground for future malware [3], [6]. In wireless networks, since resources are scarce, worms can cause new forms of havoc above and beyond those in wired networks. For instance, as the media in wireless networks is common, bandwidth is severely limited. The increased rate of attempts to access the media by infected nodes can jam the media and thereby disrupt network functionalities [7]. The dimensions of the threat become more alarming when we consider the huge investments that have been directed towards wireless communication infrastructure and the economic liability that is built upon it. The viability of these investments is contingent upon designing effective detection and containment strategies.

In this paper, we focus on the containment of infection in a mobile wireless network. As we pointed out, several wireless properties enhance the severity of the infection. However, these unique features can also be utilized to contrive new counter-measures against the spread of infection. An infected node can transmit its infection to another node only if they are in communication range of each other. We propose to quarantine the infection by regulating the communication range of the nodes. Specifically, the reception gain of the healthy nodes can be reduced to abate the frequency of contacts between the mobile nodes and thus suppress the spread of the infection. In fact, there is an interesting analogy between the spread of a worm in mobile wireless networks and a biological epidemic in a human community. During a biological virus outbreak, individuals might choose to restrain their contacts with the rest of the society. This abstinence decreases the chance of getting infected at the expense of deterioration in the quality of life: a decrease in the rate of communication between the members of the society hampers their ability to fully perform their daily tasks [8]. Such a trade-off also exists in the case of a mobile wireless network: reducing the communication range of nodes can deteriorate the QoS offered by the network, as the end-to-end communication delay increases.

We present a containment strategy based on power control. We propose an optimal control framework to characterize the trade-off between the containment efficacy and communication capabilities of the nodes (section III). Using Pontryagin's Maximum Principle, we devise a framework for computing the dynamically evolving optimal communication range. We identify several structural characteristics of the optimal control by examining the analytical properties of the solution (section V). Specifically, for a general concave cost function (subsection V-A), we show that the optimal solution has the classical bang-bang structure, i.e., it is only at its minimum or maximum values. We prove that the optimal solution in this case has at most two (abrupt) transitions between these extreme values. Subsequently, we establish that the optimal solution follows a similar structure for a strictly convex cost function, with the exception that transitions are continuous and smooth instead of being abrupt (subsection V-B). Finally, we demonstrate that dynamic optimal control of the communication range significantly outperforms static choices, and is also robust to errors in estimation of the network and attack parameters (Section VIII).

Parts of this work were presented in Fourth Symposium on Information Theory and Applications (ITA'09), University of San Diego, 2009 [1].

MHR. Khouzani and S. Sarkar are with the department of Electrical and Systems Engineering at University of Pennsylvania, Philadelphia, PA 19104 USA. Their emails are khouzani@seas.upenn.edu and swati@seas.upenn.edu. E. Altman is with INRIA, the French national institute for research in computer science and control, Sophia-Antipolis. His email is Eitan.Altman@sophia.inria.fr.

The contributions of MHR. Khouzani and Saswati Sarkar have been supported by NSF grants NSF-CNS-0914955, NSF-CNS-0915203 and NSF-CNS-0915697.

II. Literature Review

Most of the literature on worm propagation traditionally assume a wired network framework and also chiefly, the underlying network is the internet. An engaging historical review of major recent malware outbreaks in networks may for instance be found in [9]. Deterministic epidemiological frameworks have been used to model the propagation of malware in the internet [2], [3], [10]–[14]. [15] combined a deterministic worm propagation model with a game theoretic process that involves learning, in order to incorporate decisions of users about whether to install or uninstall a security patch in a wired network. Game theoretic techniques for the analysis of network security have been used in [16], [17], among others.

Controlling the spread of the worm by reducing the rate of communication of nodes [18], [19], or the number of communications [4], are the closest analogs in wired networks to reducing the communication range of the nodes in wireless networks. The work in [18] is based on heuristics and simulations. Next, unlike our work, [19] does not propose a formal framework for attaining desired trade-offs, and considers only a static choice of the communication rate, whereas we allow the communication range of the nodes to dynamically evolve over time as the infection level fluctuates. Recently, [4] has proposed to contain a worm in the initial phase of infection by limiting the total number of distinct contacts per node over the containment cycle, and models the growth of the worm using a stochastic branching process. However, this work only applies to the initial phase of infection and their countermeasure is ineffective once the epidemic starts.

Control theoretic tools have been used in [20] to propose a feedback-based (but heuristic) strategy for containment of malware in a wired network. [21]–[24] adopt malware propagation models to investigate an optimal dynamic response based on a quantified cost function in communication networks. [21], [22] assume the viewpoint of an attacker and propose a maximum damage malware attack in an energy-constrained network. This work differs from [23], [24] in that (i) we propose and investigate reduction of reception gain of nodes in a wireless network as a countermeasure rather than dynamically changing the settings of firewall softwares [23], or rate of recovery [24], and (ii) we consider cost functions which are only assumed to be either concave or convex and are therefore more general than quadratic functions. Also unlike [23] we do not use any linearization of the system which can be inadequate in the context of epidemic behavior. Optimal control has also been used as an effective tool to develop immunization and/or screening strategies to counter the spread of a biological or social epidemic [25]–[28]. Introduction of our new countermeasure policy in the framework of mobile wireless network results in a new optimal control problem that requires an original analysis and previous results in [23]–[28] do not apply here.

III. System Model

To begin, let us introduce some terminologies. A node is called **susceptible** if it is not contaminated by the worm, but is prone to infection. A node is **infective** if it has the worm. Infective nodes can propagate the worm through communication with susceptible nodes. Upon detection of an infective node, either the user of an infected device or the network operator removes the infection of the node by installing a security patch, which also grants the node permanent immunity against that threat. However, this does not take place immediately upon infection, but rather after an exponentially distributed random delay with mean $1/\gamma$. This delay is associated with detection of the malware before obtaining the appropriate patch. Each node obtains the security patch directly from a trusted source, such as a server, or authorized access points, or trained human agents. In section VI we consider an alternative setting for obtaining these security patches. We use the term **recovered** for the infective nodes which receive the patch.

Transmission of a packet between a pair of nodes is successful if the received SNR is above the minimum level necessary to decode the signal. The signal power at the receiver node is:

$$\frac{\text{transmission gain} \times \text{reception gain}}{\text{distance}^{\text{propagation loss factor}}} \times \text{base signal power} \quad (1)$$

in which the base signal power is the power of the signal at the output of the transmitter antenna when the transmission gain is unity, and the propagation loss factor is a constant no less than 2, determined by the type of media and geographical features of the network [29], [30]. Thus two nodes can communicate only if they are within a certain distance from each other, which we refer to as their communication range. When two nodes are in communication range of each other, we say they are in *contact.*

Here, we investigate the effect of changing the communication range on the propagation dynamics. Nodes are moving in a vast region (of area A) and according to mobility models such as random waypoint or random direction model [31]. Also, the communication range (u) is small compared to A, and speed of the movement is sufficiently high. It is shown (e.g. in [32]) that under such circumstances, the pairwise inter-contact time is nearly exponentially distributed, and the contact rate of a given pair of nodes is estimated as $\hat{\beta}u$ where $\hat{\beta} = \frac{2wE[V^*]}{A}$, w is a constant factor pertaining to the specific mobility model, and $E[V^*]$ is the average relative speed between two nodes. When a susceptible and an infective node are in contact, the infection is transmitted to the former with a certain probability. We assume that $\hat{\beta}$ does not change with time.

Let N be the total number of nodes, and $n_S(t)$, $n_I(t)$ and $n_R(t)$ respectively represent the total number of susceptible, infective and recovered nodes at time t. Following the conditions we assumed for the model, the state $(n_S(t), n_I(t), n_R(t))$ of the system evolves according to a pure jump Markov chain. Let the rate between the states $\sigma_1(t)$ and $\sigma_2(t)$ in that Markov chain be denoted by $\rho(\sigma_1(t), \sigma_2(t))$. Thus, we have:

$$\begin{aligned}\rho[(n_S(t), n_I(t), n_R(t)), (n_S(t)-1, n_I(t)+1, n_R(t))] \\ = \hat{\beta}u n_S(t) n_I(t) \quad \text{and,} \\ \rho[(n_S(t), n_I(t), n_R(t)), (n_S(t), n_I(t)-1, n_R(t)+1)] \\ = \gamma n_I(t).\end{aligned}$$

Let the fraction of the infective, susceptible and recovered nodes at time t be denoted by $I(t), S(t), R(t)$ re-

spectively, i.e., $I(t) = n_I(t)/N$, $S(t) = n_S(t)/N$ and $R(t) = n_R(t)/N$. Now, if $S_0 = \lim_{N\to\infty} n_S(0)/N, I_0 = \lim_{N\to\infty} n_I(0)/N, R_0 = \lim_{N\to\infty} n_I(0)/N$ and $\beta = \lim_{N\to\infty} N\hat{\beta}$ exist, it may be shown using the results of [33] that as N grows, $S(t), I(t), R(t)$ converge to the solution of the differential equations[1]

$$\dot{S} = -\beta u I S, \quad \dot{I} = \beta u I S - \gamma I, \quad \dot{R} = \gamma I$$

with initial states (S_0, I_0, R_0). The convergence is in the following sense:

$$\forall\ \epsilon > 0,\ t \geq 0, \quad \lim_{N\to\infty} \Pr\{\sup_{\tau \leq t} |\frac{n_S(\tau)}{N} - S(\tau)| > \epsilon\} = 0$$

and likewise for I and R. Recall that $\hat{\beta} \propto \frac{1}{A}$; hence $\lim_{N\to\infty} N\hat{\beta}$ exists as long as $\lim_{N\to\infty} N/A$, the node density on the plane, exists. We assume that at time zero, a nonzero portion (I_0) of the nodes, but not all of them, are infective: $0 < I(0) = I_0 < 1$. Similarly, $0 < S_0 < 1$. Moreover, in general, some fraction of the nodes may be previously immunized to the infection, i.e., $0 \leq R(0) = R_0 < 1$. Using the fact that $S + I + R = N/N = 1$, the system of differential equations presented above may be reduced to the following 2-dimensional system

$$\dot{S} = -\beta u I S \qquad S(0) = 1 - I_0 - R_0 \qquad \text{(2a)}$$

$$\dot{I} = \beta u I S - \gamma I \qquad I(0) = I_0 \qquad \text{(2b)}$$

with the state constraints

$$0 \leq S, I, \qquad S + I \leq 1. \qquad (3)$$

As we can see from the system dynamics in (2), reduction of the communication range between susceptible and infective nodes, u, can repress the propagation of the malware. Recall from (1) that the communication range between an infective transmitter and a susceptible receiver is governed both by the transmission gain of the infective and the reception gain of the susceptible node. This motivates a defense policy for wireless networks: upon detection of malicious behavior, susceptible nodes can reduce their reception gains. Effectively, this results in a reduction of their communication range, which lessens the frequency of contacts between the infective and susceptible nodes. This in turn reduces the rate of propagation of the infection. Thus, the reception gain of the susceptible nodes and hence the communication range $u(t)$ can be a control variable, which is bounded between a maximum and minimum value:

$$u_{\min} \leq u \leq 1. \qquad (4)$$

These bounds are imposed by the physical constraints of the device as well as the MAC protocol and the minimum acceptable QoS. Note that the actual bounds of the communication range can always be re-scaled and normalized, and their impact can be captured by an appropriate β, so that $u_{\max} = 1$. Any $u(t)$ that satisfies the above constraint is called *admissible,* and the range $[u_{\min} \ldots 1]$ is referred to as the *admissible range.* We make the technical assumption that $u_{\min} > 0$.

[1]Henceforth, whenever not ambiguous, the dependency on t is made implicit for brevity.

On the other hand, in most practical cases, the malware might not have controllable access to the parameters of the MAC, and in such cases, the transmission gain of the infective nodes is unchanged. However, if the malware could indeed modify the transmission gain of the infective nodes, irrespective of the choice of the reception gain of the susceptibles, it is apt to use the maximum transmission range and scanning rate that is physically realizable by the devices, so as to accelerate its spread. The resulting increase in the transmission range of the infectives can be effectively captured through appropriate scaling of β, and the model for the dynamics of the system does not change. In particular, note that the malware has no incentive to vary the transmission range over time.[2]

We now construct a meaningful cost function which captures the advantages and disadvantages of changing the communication range. Our cost functions are naturally integration of an instantaneous cost over an operation period. Infective nodes can be used by the malware to perform various forms of malicious activities, such as eavesdropping, analyzing the data traversing the network, accessing privileged information, hijacking sessions, disrupting network functionalities such as routing, *etc.* Hence, the instantaneous cost grows larger with an increase in the fraction of the infective nodes. We naturally assume a linear dependence on $I(t)$. Let us now explore the relation between the instantaneous cost and the communication range. Note that $u_{\max}$ (which is considered to be 1 after appropriate scaling) is the normal communication range of the nodes and constitutes the optimum operating point in absence of malware. Reducing the communication range below $u_{\max}$ undermines the ability of the nodes to deliver their own traffic and increases delays in the end-to-end delivery of messages related to the normal function of the network. This is more so because nodes can not selectively reduce their communication ranges based on whether they are receiving from an infective or a susceptible node. This is because an infected node does not detect that it is infected for some time, and upon detection it is immediately recovered by the system. Thus, information about whether or not a node is infective or susceptible, is not available to that node and to any other nodes. Therefore, the reduction of communication range affects communication of packets between all pairs, and thus deteriorates the overall QoS.[3] We model the effect of changing u on the QoS through a double differentiable cost function $h(u)$ that increases with decrease in u, i.e., $h'(u) \leq 0$ for $u_{\min} \leq u \leq 1$ and, without loss of generality, $h(1) = 0$. To simplify the technical arguments, we further assume $h'(1)$ is *strictly* negative. Since the characterization of $h(\cdot)$ depends on the implemented MAC and routing policies, we consider two classes of $h(\cdot)$ function: (i) concave h, i.e., $h''(u) \leq 0$ for $u_{\min} \leq u \leq 1$, and strictly convex h, i.e., $h''(u) > 0$ for $u_{\min} \leq u \leq 1$.

[2]When battery lifetimes are limited, which we do not consider in this paper, malware may have an advantage in dynamically varying the propagation range of the infective nodes. This scenario may be analyzed by considering a dynamic game, which is beyond the scope of this paper.

[3]Assuming bi-directional communication, u is in fact the communication range between a susceptible and an infective node or between two susceptible nodes. Specifically, the control of u may not alter the communication range between the infective nodes. However, as far as QoS is concerned, only the communication range between the susceptible nodes counts.

The overall cost incurred by the network therefore can be represented as follows:

$$J = \int_0^T (CI + h(u))\, dt + KI(T). \tag{5}$$

Coefficient $C \geq 0$ determines the relative importance (hazard) of the infection. The term $KI(T)$, where $K \geq 0$, represents the cost associated with the final tally of the infectives at the end of the operation period. The decision process of the susceptibles may now be represented as a dynamic control problem, that of determination of the $u(\cdot)$ that minimizes the network cost over all admissible $u(\cdot)$s subject to satisfaction of the system dynamics in (2) - such a $u(\cdot)$ is denoted as the optimal control.

Finally, note that we allow u to vary as a function of time, i.e., it is selected dynamically, though identically for individual nodes. Particularly, susceptibles may initially choose a lower value of the reception gain to suppress the spread of contagion and to *buy time* for the recovery process of the nodes to eliminate a safe number of infectives, and subsequently choose higher values of u so as to minimally disrupt the network communication. Note that all susceptibles choose the same $u(t)$ at each t since information about the state of the nodes in a susceptible node's neighborhood is either nonexistent or at best represent a statistics about the average state of the whole network, which is identical for all nodes. In addition, inter-contact times are exponentially distributed, and the memoryless property of the exponential distribution implies that each node is equally likely to meet any node in the future irrespective of its prior contact history.

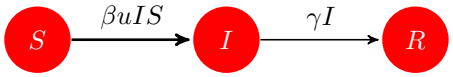


Fig. 1. $u(t)$ is the reception gain of the susceptible nodes at time t.

S	fraction of susceptible nodes
I	fraction of infective nodes
R	fraction of recovered nodes
u	communication range of susceptible nodes
γ	recovery rate of infective nodes

TABLE I
TABLE OF IMPORTANT NOTATIONS

IV. OPTIMAL u

We develop a framework for numerical computation of the optimal control u. Note that classical control techniques do not provide the optimal control in closed form since the state dynamics (2) is non-linear, the overall cost function (5) is not necessarily linear or quadratic in u, and the level of infectives is not monotonic, i.e., it can be increasing or decreasing over different intervals of time. We start by proving lemmas 1 and 2.

lemma 1. *I and S are continuous functions of time.*

Proof: According to (2), both S and I are integrals of bounded functions and thus are continuous functions of time. ■

Note that as a consequence, any continuous function of I and S is also a continuous function of time.

lemma 2. *For any admissible $u(\cdot)$, states (S, I) strictly satisfy the state constraints* (3) *for the entire interval of $(0 \ldots T)$.*

This lemma allows us to deal with an optimal control problem without any state constraints, since the state constraints are never active - thus, constraints (3) are ignored henceforth.

Proof: Note that at $t = 0$, by assumption we have $0 < I = I_0 < 1$, and also $0 < S = S_0 = 1 - I_0 - R_0 < 1$. Hence, from lemma 1, the first two constraints in (3), i.e., $0 \leq S, I$ are strictly satisfied on an interval starting from $t = 0$. The last constraint, i.e., $S + I \leq 1$ is active at $t = 0$, however, by summing equations (2a) and (2b) we have $\frac{d}{dt}(S + I)$ at time zero is equal to $-\gamma I_0$, which, following the assumptions, is negative. Therefore, there exists an interval after time zero on which the constraint $S + I \leq 1$ is strictly met. Now suppose that the statement of the lemma is not true. Then, let t_0 where $0 < t_0 \leq T$, be the first time that (at least) one of the three state constraints in (3) becomes active. Thus, the constraints are strictly met in $(0 \ldots t_0)$. For $0 < t < t_0$, from (2a) we have $\dot{S} \geq -\beta S$, thus $S \geq S_0 e^{-\beta t}$, for all $0 \leq t < t_0$ and therefore, due to continuity of $S(\cdot)$, $S(t_0) > 0$. Similarly, for $0 < t < t_0$ from (2b) we have $\dot{I} \geq -\gamma I$, thus $I(t_0) > 0$ as well. Now by summing (2a) and (2b), we obtain $\frac{d}{dt}(S + I) = -\gamma I$. Hence at t_0, $S + I < S_0 + I_0 = 1$. Thus, none of the constraints could have become active, a contradiction. ■

We can now apply the *Pontryagin's Maximum Principle* [34, P.232] on the un-constrained optimal control problem. Consider a piecewise continuous control $u(\cdot)$ and the corresponding state functions (S, I). The *Hamiltonian* H is the following scaler function of the *co-state* or *adjoint* variables[4] λ_1 and λ_2:

$$H = CI + h(u) + (\lambda_2 - \lambda_1)\beta u I S - \lambda_2 \gamma I. \tag{6}$$

Here, except at the discontinuity epochs of $u(\cdot)$,

$$\begin{aligned} \dot{\lambda}_1 &= -\frac{\partial H}{\partial S} = -(\lambda_2 - \lambda_1)\beta u I \\ \dot{\lambda}_2 &= -\frac{\partial H}{\partial I} = -C - (\lambda_2 - \lambda_1)\beta u S + \lambda_2 \gamma. \end{aligned} \tag{7}$$

Also, λ_1, λ_2 have the following final value constraints

$$\lambda_1(T) = 0, \quad \lambda_2(T) = K. \tag{8}$$

Then, according to Pontryagin's Maximum Principle, any optimal controller u, minimizes the Hamiltonian (6) over all admissible controls at each time epoch:

$$u \in \arg \min_{u_{\min} \leq \underline{u} \leq 1} H(\lambda_1, \lambda_2, S, I, \underline{u}), \tag{9}$$

where the state and co-state variables $(S, I, \lambda_1, \lambda_2)$ are absolutely continuous functions of time that satisfy (2), (7) and (8) with the optimum u. Let

$$\varphi \triangleq \beta I S(\lambda_2 - \lambda_1), \tag{10}$$

[4]In the terminology of Pontryagin's Maximum Principle, $S, I, \lambda_1, \lambda_2$ are often referred to as variables, though they are functions of time in reality.

which is a continuous function of states and co-states and thus, a continuous function of time. This allows us to rewrite the Hamiltonian (in (6)) as follows:

$$H = CI + h(u) + \varphi u - \lambda_2 \gamma I. \tag{11}$$

Thus according to (9), the optimal solution u satisfies

$$h(u) + \varphi u \leq h(\underline{u}) + \varphi \underline{u}, \tag{12}$$

where $\underline{u}$ is any admissible controller, i.e., $\underline{u} \in [u_{\min} \dots 1]$. Thus, to find the optimal controller, one needs to minimize the function $h(\underline{u}) + \varphi \underline{u}$ over the admissible set $\underline{u} \in [u_{\min} \dots 1]$.

For strictly concave h, $h(\underline{u}) + \varphi \underline{u}$ is a strictly concave function of $\underline{u}$, and is therefore minimized at either $\underline{u} = u_{\min}$ or $\underline{u} = 1$. Let $\kappa \triangleq \dfrac{h(u_{\min})}{1 - u_{\min}} > 0$. Comparing the values of the function at $\underline{u} \in \{u_{\min}, 1\}$, we obtain the optimal u as

$$u(t) = \begin{cases} u_{\min}, & \varphi(t) > \kappa \\ 1, & \varphi(t) < \kappa \\ u_{\min} \text{ or } 1, & \varphi(t) = \kappa. \end{cases} \tag{13}$$

For linear $h(u)$, i.e., for $h(u) = 1 - u$, $\kappa = 1$, and the optimal u can assume any value in $[u_{\min}, 1]$ if $\varphi(t) = 1$. Thus, we just have:

$$u(t) = \begin{cases} u_{\min}, & \varphi(t) > 1 \\ 1, & \varphi(t) < 1. \end{cases} \tag{14}$$

On the other hand, for strictly convex h, $h(\underline{u}) + \varphi \underline{u}$ can be minimized at $\underline{u} = u_{\min}$, or at $\underline{u} = 1$ or at $\underline{u} = x \in (u_{\min}, 1)$ at which $\dfrac{\partial}{\partial x}(h(x) + \varphi x) = 0$. This yields the following relation for an optimal u :

$$u(t) = \begin{cases} u_{\min}, & -h'(u_{\min}) \leq \varphi(t) \\ h'^{-1}(-\varphi), & -h'(1) < \varphi(t) < -h'(u_{\min}) \\ 1, & \varphi(t) \leq -h'(1). \end{cases} \tag{15}$$

We have therefore expressed the optimum u as a function of the state (S, I) and co-state (λ_1, λ_2) functions. Now, (2) and (7), provide a system of differential equations involving only the state and co-state functions, and not the control function. Using the initial and final values on the state and co-state functions, this system can be solved numerically to obtain the optimum state and co-state functions, which can then be used to compute u via (13), (14), (15), and the overall cost via (5).

V. Structural results

In this section, we show that for a concave h, any optimal communication range is a *bang-bang* function of time, that is, it possesses only two possible values $u_{\min}$ and 1 (theorem 1). Moreover, it switches abruptly between the extreme values and has at most two such jumps. An optimal solution for a strictly convex h again has at most two switches between $u_{\min}$ and 1, but the transitions are smooth and traverses through all intermediate values (theorem 2). We first observe the following monotonicity result:

Corollary 1. *For any admissible control function, S is a strictly decreasing function of time, i.e., $S \searrow S(T)$.*

A. Concave $h(u)$:

Theorem 1. *For concave h, the optimal $u(\cdot)$ has the following structure:*

- $u(t) = 1$ *for* $0 \leq t < t_1$ *for* $0 \leq t_1 \leq T$;
- $u(t) = u_{\min}$ *for* $t_1 < t \leq t_2$ *for* $t_1 \leq t_2 \leq T$;
- $u(t) = 1$ *for* $t_2 < t \leq T$.

Thus, optimal $u(t)$ has one of these five forms: it either has no jump and is fixed at $u_{\min}$ or 1 throughout $[0 \dots T]$ ($t_1 = 0, t_2 = T$ or $t_1 = T$, respectively); or has only one jump of the form $u = u_{\min} \uparrow 1$ or $u = 1 \downarrow u_{\min}$ ($0 = t_1 < t_2 < T$ or $0 < t_1 < t_2 = T$, respectively); or has only two jumps which is necessarily of the form $u = 1 \downarrow u_{\min} \uparrow 1$ ($0 < t_1 < t_2 < T$). We first develop some intuition behind the occurrence of each case. If the malware is highly contagious (large β), or highly dangerous (large C, K), or the recovery process is slow (small γ), or the cost inflicted by reducing u is low (small $h(u)$), then susceptibles should maintain $u = u_{\min}$ throughout. The other extreme arises for small β, high γ, small C, K or large $h(u)$: deviation from the normal $u = 1$ is then sub-optimal. The structure of u in cases that lie between these two extremes is not apriori clear. The cost $\int_0^T h(u)\, dt$ due to the deterioration of QoS depends on the duration and the extent of the reduction of u, but not on the timing of such reductions. If u is reduced early on and subsequently restored to its normal value of 1, infectives start growing only later and thus the time-accumulative cost $C \int_0^T I\, dt$ due to the growth of the infectives is low. But then since the infection starts spreading later, not enough infectives would be detected and recovered by the end of the operation interval $[0, T]$. Hence, the final tally of the infectives $I(T)$ may be high as compared to when the reduction of u starts (and also ends) later. The timing of the reduction must therefore be chosen depending on the relative values of C and K and also the spread rate β and the recovery rate γ. The one jump case arises if the reduction is either applied at the beginning or at the end, and the two jump case corresponds to when the reduction is applied in an intermediate interval. Note that the theorem establishes that the reductions must be applied in one contiguous interval and also u is never reduced to an intermediate value between $u_{\min}$ and 1 - facts that may not be anticipated based on intuition.

Proof: We first consider h to be strictly concave, and use the optimal control characterization in (13). The proof is organized as follows:

Step 1 First we prove that the optimal controller is bang-bang (i.e., it assumes only its maximum and minimum values), by arguing that φ cannot be equal to κ on an interval of nonzero length.

Step 2 Next we show that φ can have at most two *κ-crossing points* (the time epochs at which $\varphi - \kappa$ changes its sign). From (13) these are the time epochs at which u switches between its extreme values, and therefore, the optimal controller has at most two jumps.

Step 3 Finally, we use the terminal value condition of φ to evince the nature of the jumps of the optimal controller.

Proof of Step 1. From the definition of φ in (10), and state and co-state equations respectively in (2) and (7), at any

t at which $u(t)$ is continuous we have

$$\begin{aligned}\frac{\dot{\varphi}}{\beta} &= \dot{I}S(\lambda_2-\lambda_1) + I\dot{S}(\lambda_2-\lambda_1) + IS(\dot{\lambda_2}-\dot{\lambda_1}) \\ &= (\beta uIS-\gamma I)S(\lambda_2-\lambda_1) + I(-\beta uIS)(\lambda_2-\lambda_1) \\ &\quad + IS(-C-(\lambda_2-\lambda_1)\beta uS + \lambda_2\gamma + (\lambda_2-\lambda_1)\beta uI) \\ &\text{Thus, } \dot{\varphi} = -\beta IS(C-\lambda_1\gamma). \end{aligned} \tag{16}$$

Now, suppose that $\varphi = \kappa$ on an interval of nonzero length. Since $u(t)$ is a piecewise continuous function of time, $u(t)$ is continuous on a subinterval of this interval. On such a subinterval, $\dot{\varphi}$ is equal to zero. Consider now two distinct points of this subinterval, call them t_1 and t_2. We have:

$$\begin{aligned}\dot{\varphi}(t_1) &= -\beta I(t_1)S(t_1)(C-\lambda_1(t_1)\gamma) = 0 \\ \dot{\varphi}(t_2) &= -\beta I(t_2)S(t_2)(C-\lambda_1(t_2)\gamma) = 0.\end{aligned}$$

Following lemma 2, we must have: $\lambda_1(t_1) = \lambda_1(t_2)$. However,

$$\dot{\lambda}_1 = -\frac{\varphi}{S}u.$$

Since $\varphi = \kappa > 0$, and $u \geq u_{\min} > 0$, this is a contradiction.

Proof of Step 2. We denote *κ-points* t_κ as epochs at which $\varphi = \kappa$. A κ-crossing point must also be a κ-point, but the reverse is not true. Let the variables with tilde denote their values at t_κ. Next, note that the Hamiltonian is *autonomous*, i.e., does not explicitly depend on the independent variable t ($\frac{\partial H}{\partial t} \equiv 0$). When the final time T is fixed and the Hamiltonian is autonomous then ([34, P.236]):

$$H(S(t), I(t), u(t), \lambda_1(t), \lambda_2(t)) \equiv \text{constant} \equiv H. \tag{17}$$

From (10) and by equating $\varphi(t_\kappa) = \kappa$, we obtain

$$\beta\tilde{I}\tilde{S}(\tilde{\lambda}_2 - \tilde{\lambda}_1) = \kappa. \tag{18}$$

Since u is piecewise continuous, state and co-state functions, and hence φ, are piecewise differentiable. Thus, we can write[5]

$$\begin{aligned}\dot{\varphi}(t_\kappa^-) = \dot{\varphi}(t_\kappa^+) &= -\beta\tilde{I}\tilde{S}(C-\tilde{\lambda}_1\gamma) && \text{[from (16)]} \\ &= -\beta\tilde{I}\tilde{S}(C+\gamma(\frac{\kappa}{\beta\tilde{I}\tilde{S}} - \tilde{\lambda}_2)) && \text{[from (18)]} \\ &= -\beta\tilde{S}(C\tilde{I} - \tilde{\lambda}_2\gamma\tilde{I}) - \gamma\kappa \\ &= -\beta\tilde{S}(H - h(u) - \tilde{\varphi}u) - \gamma\kappa && \text{[from (11)]} \\ &= -\beta\tilde{S}(H-\kappa) - \gamma\kappa. && (19)\end{aligned}$$

Equation (19) follows since according to (13), approaching t_κ, a κ-point, u is either 1 or $u_{\min}$ and for both of these two values, we have $h(u) + \tilde{\varphi}u = \kappa$.

Here, we state a general property of continuous and piecewise differentiable functions which we prove in the appendix.

Property 1. *Let $f(\cdot)$ be a continuous and piecewise-differentiable function. Let t_1, t_2 be its consecutive L-Level points, that is, $f(t_1) = f(t_2) = L$ and $f(t) \neq L$ for all $t_1 < t < t_2$. Also, $\dot{f}(t_1^+) \neq 0$ and $\dot{f}(t_2^-) \neq 0$. Then $\dot{f}(t_1^+)$ and $\dot{f}(t_2^-)$ must have opposite signs.*

We investigate the case of $H - \kappa \geq 0$ first. Then according to (19) and lemma 2, $\dot{\varphi}(t_\kappa^-) = \dot{\varphi}(t_\kappa^+) \leq -\gamma\kappa < 0$, as $\kappa > 0$. Thus, first of all, φ cannot equal κ over an interval of nonzero length, since that would require $\dot{\varphi}$ to be equal to zero over that interval. Now let there be more than one κ-point and call the first two as $t_{\kappa 1}$ and $t_{\kappa 2}$. We have $\dot{\tilde{\varphi}}(t_{\kappa 1}^+), \dot{\tilde{\varphi}}(t_{\kappa 2}^-) \leq -\gamma\kappa < 0$. This contradicts property 1. Thus there is at most one κ-point, and hence at most one $\kappa-$crossing point.

Now, let $H - \kappa < 0$. Since β, H, γ are constants, (19) is linear in $\tilde{S}$. Also, recall from Corollary 1 that S is a strictly monotonic function of time. Thus $\tilde{S}$, as samples of S, is strictly monotonic in t_κ. Therefore, $\dot{\tilde{\varphi}}$ is strictly monotonic in t_κ. This, together with property (1) show that there are at most three distinct κ-points, say $t_{\kappa 1}$ to $t_{\kappa 3}$. Thus, if there are more than two κ-crossing points, then they have to be $t_{\kappa 1}$ to $t_{\kappa 3}$. According to (19) $\dot{\tilde{\varphi}}$ is indeed either negative for all t_κ epochs (case of $H - \kappa \geq 0$), or is strictly decreasing between consecutive samples at t_κ epochs (case of $H - \kappa < 0$), a critical fact that we will use later. Thus, by property 1 and the strict monotonicity of $\dot{\tilde{\varphi}}$ in t_κ, $\dot{\varphi}(t_{\kappa 2}^-) = \dot{\varphi}(t_{\kappa 2}^+) = 0$, and $\dot{\varphi}(t_{\kappa 1}^+)$ and $\dot{\varphi}(t_{\kappa 3}^-)$ have opposite signs. But this contradicts the following property of continuous and piecewise differentiable functions (which we prove in the appendix):

Property 2. *Let $f(\cdot)$ be a continuous and piecewise-differentiable function. Let t_1, t_2, t_3 be three consecutive L-level points that are also L-crossing points, that is, $f(t_1) = f(t_2) = f(t_3) = L$, $f(t) \neq L$ for all $t_1 < t < t_2$ and $t_2 < t < t_3$, and $(f(t) - L)$ changes its sign at these points. Now, if we have $\dot{f}(t_1^+) \neq 0$ and $\dot{f}(t_2^-) = \dot{f}(t_2^+) = 0$ and $\dot{f}(t_3^-) \neq 0$, then $\dot{f}(t_1^+)$ and $\dot{f}(t_3^-)$ must have the same sign.*

Therefore, there cannot be more than two κ-crossing points.

Proof of Step 3. Note that $\varphi(t)$ is a continuous function that following (8), ends at

$$\varphi(T) = \beta u(T)I(T)(\lambda_2(T) - \lambda_1(T)) = \beta u(T)I(T)K. \tag{20}$$

First suppose $\varphi(T) < \kappa$. Hence, from (13), the optimal controller $u(t) = 1$ in a subinterval towards the end of $(0 \ldots T)$. Now if φ has no κ-crossing point then $u(t) = 1$ throughout $(0 \ldots T)$. If φ has one κ-crossing point, say $t_1 \in (0 \ldots T)$, then $u = u_{\min}$ in $(0 \ldots t_1)$ and $u = 1$ in $(t_1 \ldots T)$. Finally, if φ has two κ-crossing points, since $\varphi(T) < \kappa$, $\varphi(t) - \kappa$ must change its sign from negative to positive at some time $0 < t_1 < T$ and then back to negative at some later time t_1 where $0 < t_1 < t_2 < T$. Thus, $u(t) = 1$ in $(0 \ldots t_1)$, then $u(t) = u_{\min}$ in $(t_1, \ldots t_2)$ and $u(t) = 1$ again after t_2.

Now let $\varphi(T) > \kappa$. As we argued in step-2, $\dot{\varphi}$ at κ-crossing points is either always negative, or is decreasing between consecutive κ-crossing points. This shows that the case of φ crossing down κ and then crossing back up κ is not possible since that would require $\dot{\varphi}$ at its κ-crossing points to be strictly increasing. Thus either φ always stays above κ in which case $u = u_{\min}$ throughout, or φ crosses κ up once, which is the case in which u switches from $u = 1$ to $u_{\min}$. Similar arguments apply for the case of $\varphi(T) = \kappa$, depending whether $\varphi(t) > \kappa$ or $\varphi(t) < \kappa$ as t approaches T. This completes step-3 and thus proves the theorem for strictly concave h.

We now consider linear h, i.e., $h(u) = 1 - u$, and use the optimal control characterization in (14). Following similar

[5] $f(t_0^+) \triangleq \lim_{t \downarrow t_0}$ and $f(t_0^-) \triangleq \lim_{t \uparrow t_0}$.

footsteps that lead to eq. (19), and using the fact that here $H = \tilde{I}(C - \gamma\tilde{\lambda}_2) + 1$, we obtain:

$$\tilde{\dot{\varphi}} = -\beta\tilde{S}(H-1) - \gamma.$$

The proof is otherwise similar to that for strictly concave h, with κ replaced with 1. ■

Remark 1. (I): $H \geq -\frac{\gamma\kappa}{\beta(1-I_0)} + \kappa$. Then $\tilde{\dot{\varphi}} < 0$. This follows from (19), and since $0 < S < S_0 = 1 - I_0$ (Corollary 1). The negativity of $\tilde{\dot{\varphi}}$ along with the fact that φ is a continuous function of time, according to property 1, show that there can be at most one switch in the sign of $\varphi - \kappa$, and hence the optimal $u(\cdot)$ has at most one jump. Recall from (20) that $\varphi(T) = 0 < \kappa$. Thus, if $\varphi(0) = \beta I_0 S_0(\lambda_2(0) - \lambda_1(0)) < \kappa$ then $u(t) = 1$ for $t \in [0, T]$. If, on the other hand, $\varphi(0) > \kappa$, then it follows from the Intermediate Value Theorem (IVT) that $u(\cdot)$ jumps from $u_{\min}$ to 1 in $(0, T)$.

(II): $H < -\frac{\gamma\kappa}{\beta(1-I_0)} + \kappa$. This therefore constitutes a necessary condition for the optimal control to have two jumps. According to (8) and (17), $H = H(T) = CI(T) + h(u(T)) + \varphi(T)u(T) - \gamma\lambda_2(T)I(T)$. Also, from (2b) and following the argument in the proof of lemma 2, we have $I(T) \geq I_0 e^{-\gamma T}$. The necessary condition therefore is:

$$I_0 e^{-\gamma T} C < -\frac{\gamma\kappa}{\beta(1 - I_0 - R_0)} + \kappa,$$

which, for instance, requires $\beta(1 - I_0 - R_0) > \gamma$.

B. Strictly Convex $h(u)$:

Theorem 2. *Let Phases 1 and 2 be defined as follows.*

Phase 1:

a. $u(t) = 1$, *on* $0 \leq t < t_1 \leq T$ *for some* $t_1 \geq 0$;
b. $u(t)$ *strictly and continually decreases on* $t_1 \leq t < t_2 \leq T$ *for some* $t_2 \geq t_1$;
c. $u(t) = u_{\min}$ *on* $t_2 \leq t \leq t_3$ *for some* $t_2 \leq t_3 \leq T$.

Phase 2:

a. $u(t)$ *strictly and continually increases on* $t_3 \leq t \leq t_4 \leq T$ *for some* $t_3 \leq t_4 \leq T$;
b. $u(t) = 1$ *on the interval* $t_4 \leq t \leq T$.

For strictly convex h, an optimal $u(t)$ is a continuous function consisting of

- *Only Phase 1, or*
- *Only Phase 2, or*
- *Phase 1 followed by Phase 2.*

Qualitatively, the optimal controller for strictly convex $h(\cdot)$ shows similar pattern of up to two transitions between a maximum and minimum value as that for concave $h(\cdot)$. The transitions are however smooth for strictly convex $h(\cdot)$ as a slight increase in u from $u_{\min}$ decreases the cost due to QoS and hence the overall cost significantly. In contrast, for a concave $h(u)$, the decrease in the overall cost as a result of a slight increase in the value of u is insignificant and if it is at all beneficial to increase u so as to enhance QoS, it is better to increase it to the maximum possible value of 1.

Proof of Theorem 2. We use the optimal control characterization in (15). It follows from the continuity of φ that the optimal u is a continuous function of time. Thus the state and co-state functions and thus any differentiable function of them, e.g. φ, is differentiable throughout $(0 \ldots T)$.

Note that due to strict convexity and decreasing properties and assumptions on h, we have $0 < -h'(1) < -h'(u_{\min})$. The following key lemma can be validated similar to the steps 1 and 2 of the proof of theorem 1:

lemma 3. *Consider any $L > 0$. (i) φ cannot be equal to level L over an interval of nonzero length. (ii) $\varphi = L$ for at most three time epochs. (iii) φ crosses any level L at most at two time epochs in $(0 \ldots T)$. Moreover, (iv) $\dot{\varphi}$ either is negative at these L-crossing points or is decreasing between consecutive L-crossing points.*

Thus, there exists at most one interval of nonzero length on which $\varphi > L$ for any level $L > 0$ (e.g., $L = -h'(1)$). Otherwise φ, as a differentiable function of time, either has to cross L more than twice, or has to be at L for an interval of positive length, or has to cross L down and then above which requires $\dot{\varphi}$ to be non-decreasing between its consecutive L-crossing points. However, all of these cases would contradict the above lemma.

lemma 4. $\dot{\varphi} = 0$ *at at most one time epoch during the (only possible) interval on which* $\varphi > -h'(1)$.

Proof: Suppose $\dot{\varphi}$ is zero at t_1, t_2 in the interval on which $\varphi > -h'(1) > 0$, and $t_1 < t_2$. Since from lemma 2, IS is never zero, from the expression for $\dot{\varphi}$ in (16) we must have:

$$C - \lambda_1(t_1)\gamma = 0 = C - \lambda_1(t_2)\gamma.$$
$$\text{Hence, } \lambda_1(t_1) = \lambda_1(t_2). \tag{21}$$

The relation for $\dot{\lambda_1}$ in (7) can be rewritten as follows:

$$\dot{\lambda}_1 = -\frac{\varphi u}{S}$$

Note that $\varphi u > 0$ over $(t_1 \ldots t_2)$. Thus λ_1 is strictly decreasing during this interval. This contradicts (21). ■

Next, from (15),

$$\frac{du}{dt} = \begin{cases} \frac{-\dot{\varphi}}{h''(h'^{-1}(-\varphi))}, & -h'(1) < \varphi(t) < -h'(u_{\min}) \\ 0, & otherwise. \end{cases} \tag{22}$$

The above relation shows that on the interval over which $-h'(1) < \varphi(t) < -h'(u_{\min})$, $\dot{u}$ has the opposite sign of $\dot{\varphi}$ and over such intervals $\dot{u} = 0$ only if $\dot{\varphi} = 0$.

If $\varphi \leq -h'(1)$ throughout $[0 \ldots T]$, then (15) implies that $u = 1$ throughout and we only have phase 2-b. Otherwise, there exists exactly one interval, denoted as $(\nu_1 \ldots \nu_2)$, $0 \leq \nu_1 < \nu_2 \leq T$, such that $\varphi > -h'(1)$ in $(\nu_1 \ldots \nu_2)$, and $\varphi \leq -h'(1)$ at $t \leq \nu_1$ and $t \geq \nu_2$. Thus, referring to (15), $u = 1$ over the intervals $[0 \ldots \nu_1]$ and $[\nu_2 \ldots T]$, which respectively correspond to phases 1-a and 2-b. Second, Lemmas 3 and 4 imply that on the interval over which $\varphi > -h'(1) > 0$, i.e., $(\nu_1 \ldots \nu_2)$, φ is either (A) always strictly decreasing; (B) always strictly increasing; or (C) strictly

increasing on a sub-interval $(\nu_1 \dots \nu_3)$ and strictly decreasing during $(\nu_3 \dots \nu_2)$. Here, we investigate case (A). Similar arguments can be made about cases (B) and (C). In case (A), $\nu_1 = 0$. Now either (i) $\varphi \leq -h'(u_{\min})$ throughout $(0 \dots \nu_2)$; or (ii) $\varphi > -h'(u_{\min})$ on $(0 \dots \nu_4)$, then $\varphi \leq -h'(u_{\min})$ on $(\nu_4 \dots \nu_2)$. For case (i), u is strictly increasing over $[0 \dots \nu_2]$, and assuming $\nu_2 < T$, then $u = 1$ over $[\nu_2 \dots T]$ (phase 2-a followed by phase 2-b). If $\nu_2 = T$, phase 2-b has length zero. On the other hand, for case (ii), assuming $\nu_2 < T$, we have $u = u_{\min}$, over $[0 \dots \nu_4]$ (phase 1-c), then u strictly increases over $[\nu_4 \dots \nu_2]$ (phase 2-a), then $u = 1$ over $[\nu_2 \dots T]$ (phase 1-c). Again, if $\nu_2 = T$, phase 2-b has length zero. □

VI. Distribution of Security Patches through the Underlying Wireless Network

Security patches may themselves be compromised unless they are obtained directly from trusted resources such as authorized access points, or trained human agents. Nevertheless, we still investigate the alternative (less secure) distribution of the patches through the underlying wireless network. In this case, decreasing the reception gain of the susceptible nodes can increase the delay in delivery of the patches. We therefore replace the recovery rate γ with $\gamma_0 + \gamma_1 u$ where $\gamma_1 \geq 0$, and show that theorem 1 extends. The differential equation for I in (2b) changes to:

$$\dot{I} = \beta u I S - \gamma_0 I - \gamma_1 u I.$$

The Hamiltonian in (6) is updated as follows:

$$H = CI + h(u) + (\lambda_2 - \lambda_1)\beta u I S - \lambda_2 \gamma_0 I - \lambda_2 \gamma_1 u I.$$

If we update the definition of φ in (10) as

$$\varphi \triangleq \beta I S(\lambda_2 - \lambda_1) - \lambda_2 \gamma_1 I,$$

the optimal u may be characterized as in (13) and (14). Rewriting the Hamiltonian using the definition of φ yields:

$$H = CI + h(u) + \varphi u - \lambda_2 \gamma_0 I.$$

Since the system is autonomous, H is a constant. Hence,

$$H = H(t_\kappa^+) = H(t_\kappa^-) = C\tilde{I} + \kappa - \tilde{\lambda}_2 \gamma_0 \tilde{I}. \tag{23}$$

At t_κ we have:

$$\varphi(t_\kappa) = (\tilde{\lambda}_2 - \tilde{\lambda}_1)\beta \tilde{I}\tilde{S} - \tilde{\lambda}_2 \gamma_1 \tilde{I} = \kappa. \tag{24}$$

The co-state equation for $\dot{\lambda}_2$ changes to the following:

$$\dot{\lambda}_2 = -C - (\lambda_2 - \lambda_1)\beta S + \lambda_2(\gamma_0 + \gamma_1 u).$$

The time derivative of φ turns out to be:

$$\dot{\varphi} = -\beta I S C + \beta I S \lambda_1 \gamma_0 + \gamma_1 I C. \tag{25}$$

Hence,

$$\begin{aligned}
\dot{\varphi}(t_\kappa^-) &= \dot{\varphi}(t_\kappa^+) \\
&= -\beta \tilde{I}\tilde{S}C + \gamma_1 \tilde{I}C \\
&\quad + (\tilde{\lambda}_2 - \frac{\kappa + \tilde{\lambda}_2 \gamma_1 \tilde{I}}{\beta \tilde{I}\tilde{S}})\beta \tilde{I}\tilde{S}\gamma_0 \quad \text{[from (24)]} \\
&= -\beta \tilde{I}\tilde{S}C + \tilde{\lambda}_2 \beta \tilde{I}\tilde{S}\gamma_0 + \gamma_1 \tilde{I}C - \gamma_1 \tilde{\lambda}_2 \gamma_0 \tilde{I} - \kappa\gamma_0 \\
&= -\beta(\tilde{I}C - \tilde{\lambda}_2 \gamma_0 \tilde{I})\tilde{S} + \gamma_1(\tilde{I}C - \tilde{\lambda}_2 \gamma_0 \tilde{I}) - \kappa\gamma_0 \\
&= -\beta(H - \kappa)\tilde{S} + \gamma_1(H - \kappa) - \kappa\gamma_0. \quad \text{[from (23)]}
\end{aligned}$$

Therefore, $\dot{\varphi}(t_\kappa^-)$ and $\dot{\varphi}(t_\kappa^+)$ are linear in $\tilde{S}$ and theorem 1 can be established using similar arguments as in subsection V-A.

VII. Implementation and Practical Issues

Dynamic control of the reception gain of the nodes is possible through control of antenna gains, which may be realized through the use of smart antennas and adaptive antenna arrays (see e.g. [35], [36]). A simple example for circuitry and algorithms for achieving controllable gain at the receiver end of adaptive antennas is presented in [**?**]. Such smart antennas have been implemented e.g. by Ericsson and Mannesmann Mobilfunk [**?**], and are expected to be more pervasive in wireless devices in near future. Note that it may not be possible to adjust antenna gains up to arbitrary precision, and in practice, only a few quantized gain levels may be available. This does not lead to any sub-optimality when the $h(.)$ function is concave, since as we proved, the optimal u in this case is either at $u_{\min}$ or 1 during different intervals. For a strictly convex $h(.)$, quantization may however lead to sub-optimality as the optimal u may assume any intermediate value between $u_{\min}$ and 1. Nevertheless, our numerical computations presented in the next section reveal that the above sub-optimality is insignificant.

In absence of adaptive antennas, reduction of reception gain may be achieved by simply rejecting some of the communication requests. In this case u is the fraction of communication requests accepted by each node. In more details, here the rate of contacts of each pair of node is $\frac{2w\alpha E[V^*]}{A}$ where α is the communication range of the nodes which is now fixed. However, only a fraction u of such contacts result in successful communication. Hence the rate of permitted communication between susceptible and infective nodes is $\frac{2w\alpha E[V^*]}{A}u$, and hence the governing system of differential equations is the same as before with $\hat{\beta} = \frac{2w\alpha E[V^*]}{A}$.

Recall that the optimal control for the case of concave h is completely specified by (at most two) jump points, and for a strictly convex h consists of at most two phases, characterized by at most four time epochs. Thus, the reception gain may be optimally controlled by the nodes without any local or global coordination or information exchange once they know these transition epochs. Upon detection of a new malware in the network, a central surveillance can assess the cost coefficients C, K, the rate of recovery γ, and estimate (or may already have an estimate of) the spread rate β of messages from the mobility pattern and the density of the nodes etc. Switching epochs can then be calculated and distributed with small communication overhead at time zero. Alternatively, nodes can receive the estimated parameters from the central surveillance and calculate the epochs themselves.

VIII. Simulations and Numerical Computations

We first develop some intuition about the trends of changes in the structure of the optimum control as a result of changes in values of parameters β, I_0, R_0, K, C. We subsequently demonstrate that overall costs can be substantially lowered by using dynamic optimal reception gain control as compared to

static gain control. Moreover, through simulations, we demonstrate how a heuristic policy which utilizes approximate and temporally evolving state information in a node's neighborhood (hence a node-specific policy) compares to our dynamic optimal policy which requires only one time estimates of the system parameters. Finally, we demonstrate that the dynamic optimal policy is robust to errors in the above estimates, and also to quantization errors in gain control.

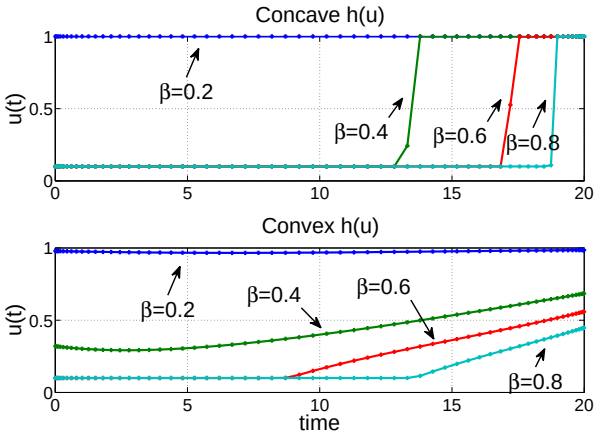


Fig. 3. Optimal u, varying β. Here, $I_0 = 0.1$, $K = 50$, and other parameters are as in fig. 2.

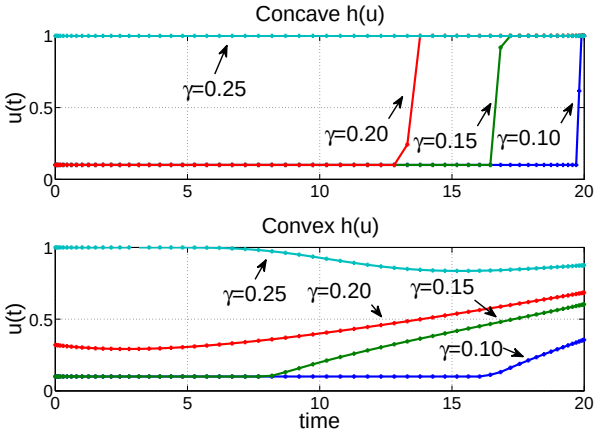


Fig. 4. Optimal u, varying γ. Here, $I_0 = 0.1$, $K = 50$, and other parameters are as in fig. 2.

As fig. 2 reveals, the optimal control becomes more conservative (selects lower values) for higher values of K. However, an interesting phenomenon is that increasing I_0 does not necessarily lead to more conservative defense policy. In fact, the defense policy chooses progressively lower values of u, when I_0 is increased up to a certain value, but once I_0 exceeds this threshold the defense barely deviates u from the normal value of 1. This is because for large I_0 the defense's efficacy is so low that reducing the reception gain does not help the containment but only deteriorates the QoS. The optimal controller becomes more conservative for higher and lower values of β, γ respectively (fig. 3 and fig. 4). Finally, for large C, u is reduced earlier so as to reduce the time-accumulative

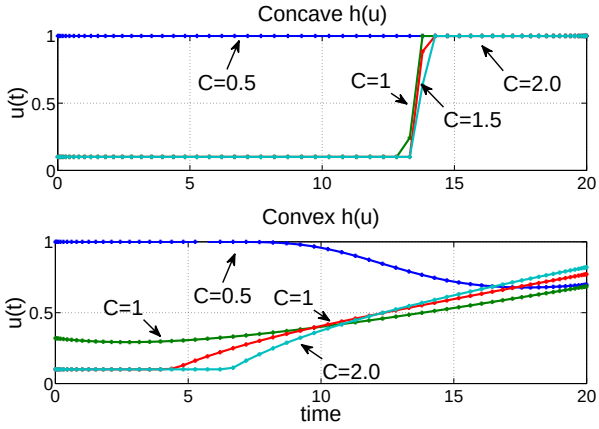


Fig. 5. Optimal u, varying C. Here, $I_0 = 0.1$, $K = 50$, and other parameters are as in fig. 2.

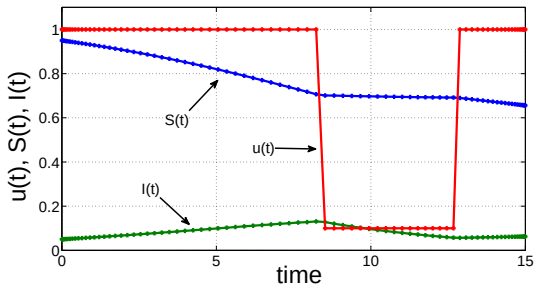


Fig. 6. An optimal u with two jumps. Here, $h(u) = 1-u$, $u_{\min} = 0.1, \gamma = 0.22, \beta = 0.4, I_0 = 0.05, R_0 = 0, C = 0.8$ and $K = 60$.

cost associated with the infectives (and increased earlier too to provide the desired QoS) (fig. 5). Also, as all the above figures reveal, for concave h, usually the optimal u is either at 1 throughout or jumps once from $u_{\min}$ to 1. But, scenarios where it has two jumps does indeed arise (Fig. 6).

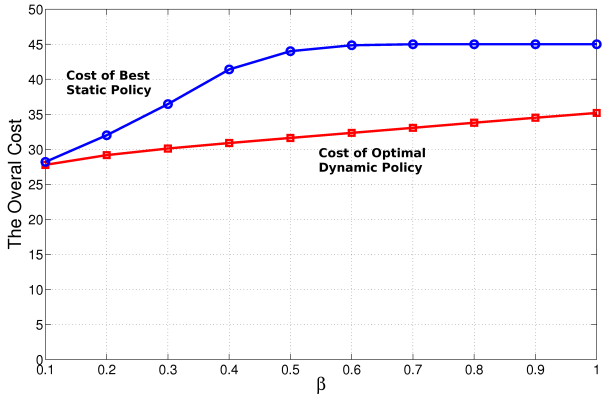


Fig. 7. Cost comparison: optimum dynamic versus the static policies. The parameters are $T = 25$, $u_{\max} = 1$, $u_{\min} = 0.1$ $\gamma = 0.2$, $I_0 = 0.2$, $C = 5$ $K = 50$ and $h(u) = 1 - u$.

Fig. 7 compares the overall costs inflicted by the optimal dynamic policy versus the best static policy, as a function of β. A static policy is one in which the same value of reception

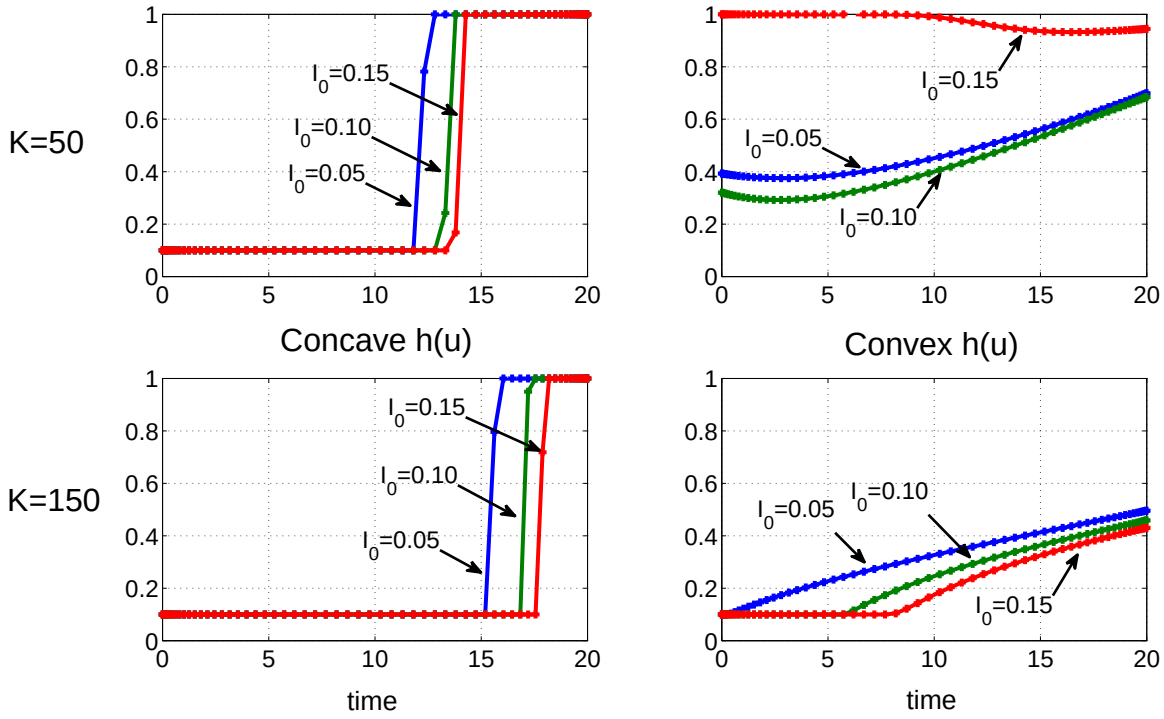


Fig. 2. Optimal u, varying K. The $h(u)$ functions used for concave and convex cases are $0.5(1-u)$ and $(1-u)^{1.2}$, respectively. Other parameters are $u_{\min}=0.1, \gamma=0.2, \beta=0.4, R_0=0$ and $C=1$.

gain is used throughout and we have optimized this fixed value to obtain the best static policy. Our dynamic policy achieves substantially lower costs except when β is small; in the latter case its choice is largely static ($u \approx 1$ most of the time).

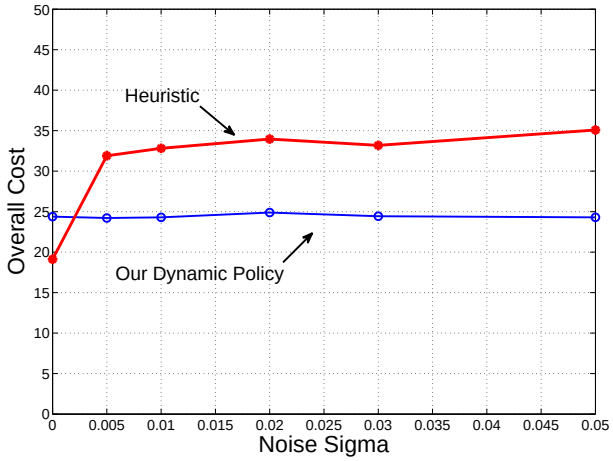


Fig. 8. Comparison of the costs achieved by our dynamic optimal control and a heuristic control that uses (noisy) local state information.

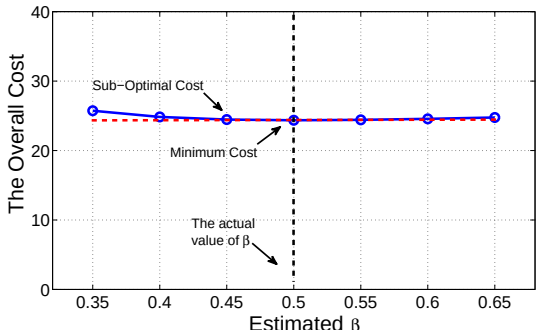
As we discussed before, a node usually does not have information about the states of those that it contacts. However, by monitoring the anomalous increase in the media access activity as a result of attempts of infective nodes to spread the malware, a node may be able to estimate the number of infectives in its neighborhood. This estimate, however, depends on measurements over fading channels in a network whose topology is constantly changing due to mobility. Hence, these estimates have limited accuracy and are fraught with random errors. An important question that remains to be answered then is whether and how nodes can utilize this noisy information about the number of infective nodes in their neighborhood, even at the cost of higher signal processing and computations. In order to assess the usefulness of these noisy estimates, we develop a heuristic node-specific policy that utilizes the available information, and compare its efficacy against our dynamic optimal control through simulation. In the heuristic policy, each node estimates the number of infective nodes in its neighborhood; however, the state of each neighbor is not flawlessly known. In the simulation, we modeled this imprecision in detection by adding a Gaussian noise with mean zero and power σ^2 to the indicator that a node is infective or not. Upon contact by one of its neighbors, the receptive node blocks the communication, by reducing its reception gain to $u_{\min}$, if the estimated fraction of infected nodes in its vicinity is *greater* than a certain threshold. (We consider $u_{\min}$ very close to 0 and hence when $u = u_{\min}$, the communication is effectively blocked). This policy can be optimized over the selected threshold and the size of the sensing area which determines the set of neighbors. Specifically, at any given time t, the neighbors of a node are those who are in contact with it in a time window $(t-\Delta \ldots t+\Delta)$, and Δ depends on the size of the sensing area and node velocity. We choose Δ (as also the decision threshold) so as to minimize the overall cost incurred by the heuristic policy. Our dynamic optimal control

blocks communications at all times at which the optimal u equals $u_{\min}$ (as again $u_{\min} \approx 0$) and accepts communications otherwise (since the optimal u equals 1 otherwise). We ran the simulations for $N = 50$ nodes over a period of $T = 20$, with $\beta = 0.5$, $\gamma = 0.2$, $I_0 = 0.2$ (i.e., $n_I(0) = 0.2 \times 50 = 10$), $C = 10, K = 0, h(u) = 1 - u$, and considering exponentially distributed inter-contact times, with parameter $\tilde{\beta} = \beta/N$ (refer to Section III, 3rd para), as is the case for random waypoint and random direction mobility models ([31], [32]). The overall cost is calculated for both the heuristic policy and our dynamic policy through simulation as follows: the cost of infectives ($\int_0^T CI\ dt$ in (5)) is obtained by integrating (C times) the fraction of infectives over time and the cost due to reduction of u is considered as the fraction of blocked communications. The latter corresponds to $h(u) = 1 - u$, as when $u = u_{\min} \approx 0$ ($u = 1$, respectively) every contact results in a blocked (successful, respectively) communication and incurs unit (0, respectively) cost as per the $h(.)$ function. As fig. 8 reveals, the heuristic policy attains slightly lower costs than our optimal control policy, which does not use any local or global state information, for small estimation errors. This better performance is due to avoiding unnecessary blocking of communication and hence not losing too much of QoS. However, as the estimation noise increases this advantage quickly diminishes and in fact our dynamic policy significantly outperforms the heuristic. Hence, considering the computation overhead that state estimations introduces and since accuracy in such estimates is hard to achieve, our dynamic policy which requires no state information is preferable.

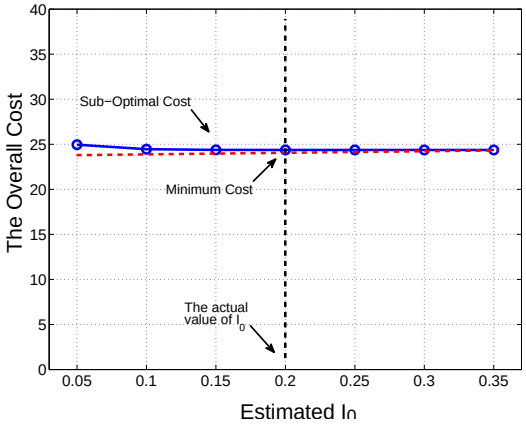
In order to calculate our dynamic policy, one requires a *one time* (as opposed to a continuous estimation of the state) estimate of the parameters of the system, e.g., β, I_0 etc. Here, we demonstrate that the cost achieved by our dynamic policy is robust to errors in estimation of these parameters. Suppose that β equals 0.5 but the optimal control is calculated based on an estimate that is somewhere between 0.35 and 0.65. Fig. 9(a) reveals that the increase in the overall cost as a result of inaccurate estimation of β up to 30% is less than 6%. Similar observation holds about I_0: as fig. 9(b) depicts, up to 75% error in the estimation of I_0 results in less than 2.5% increase in the cost incurred by our dynamic policy. Finally, as we pointed out in the previous section, the reduction of communication rates may only be possible at quantized levels, which leads to sub-optimality only when the $h(.)$ function is strictly convex. The quantization of u however only minimally increases the overall cost: as Fig. 9(c) and 9(d) show that even when the number of levels is only 2 (and thus the controller is bang-bang), the increase in cost is less than 3%.

IX. Conclusion

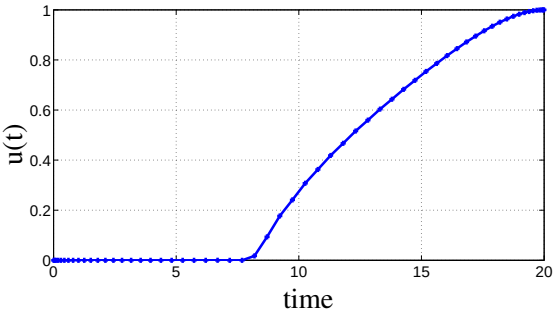
We proposed reduction of reception gains of susceptible nodes for containing malware outbreaks in mobile wireless networks. Using optimal control tools, we identified the optimum policy for dynamically controlling the reception gains so as to minimize the overall network costs. We analytically proved that the optimal policies have simple structures when the cost functions are concave and convex, and can therefore



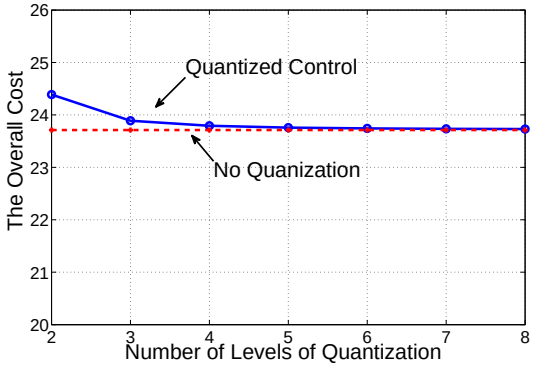
(a) Robustness with respect to β



(b) Robustness with respect to I_0



(c) The un-quantized optimal control



(d) Robustness of the quantized control

Fig. 9. The first two figures respectively demonstrate the robustness with respect to β and I_0 respectively for $h(u) = 1 - u$. The last two figures demonstrate robustness with respect to quantization in the control for $h(u) = (1 - u)^{1.5}$. In the last figure, the x-axis represents the number of levels available for u, and the control is rounded to the level closest to the optimal value, e.g., $x = 2$ means the output is rounded to $u_{\min}$ and 1. The other parameters for all the figures are $\beta = 0.5$, $I_0 = 0.2$, $R_0 = 0$, $\gamma = 0.2$, $u_{\min} \approx 0$, $u_{\max} = 1$, $C = 10$, $T = 20$.

be easily implemented in resource constrained devices without requiring constant coordination and information exchange.

Investigation of dynamic control of infective nodes' transmission gains by the malware (instead of selecting the maximum value throughout) constitutes an interesting direction for future research. Such control may be motivated in scenarios where energy limitations lead to premature battery depletions of infective nodes owing to high transmission range selections, which in turn throttles the spread of the infection. Such control may also be necessary in a highly dense network in which a malware might want to avoid jamming during its spreading period, in order not to self-throttle its propagation, and then initiate a more effective jamming attack. These cases, however, will lead to a dynamic game setting as both the network and an attacker will optimize against each other.

APPENDIX

Proof of Property 1. Without loss of generality, let $\dot{f}(t_1^+) > 0$. Let $\dot{f}(t_2^-) > 0$. The continuity and piecewise differentiability of $f(\cdot)$ implies that there exists $\delta > 0$ such that $f(\cdot)$ is continuous in the closed intervals $[t_1, t_1+\delta]$, $[t_2-\delta, t_2]$ and differentiable in the open intervals $(t_1, t_1+\delta)$, $(t_2-\delta, t_2)$. Thus, since $f(t_1) = f(t_2) = L$ and $\dot{f}(t_1^+) > 0, \dot{f}(t_2^-) > 0$, it follows from the Mean value theorem that

$$\exists\ \delta_1 \in (0 \ldots \frac{1}{2}(t_2 - t_1)) \text{ such that } f(t_1 + \delta_1) > L, \text{ and}$$

$$\exists\ \delta_2 \in (0 \ldots \frac{1}{2}(t_2 - t_1)) \text{ such that } f(t_2 - \delta_2) < L.$$

But, by the Intermediate value theorem (IVT), there exists 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 $t_1 < t < t_2$. Thus, $\dot{f}(t_2^-) < 0$, and Property 1 holds. □

Proof of Property 2. Without loss of generality, let $\dot{f}(t_1^+) > 0$. Arguing as in the proof of Property 1,

$$\exists\ \delta_1 \in (0 \ldots \frac{1}{2}(t_2 - t_1)) \text{ such that } f(t_1 + \delta_1) > L.$$

Also, $(f(t) - L)$ must change its sign from *positive* to *negative* at t_2. This is because otherwise, $\exists\ \delta_2 \in (0 \ldots \frac{1}{2}(t_2 - t_1))$, such that $f(t_2 - \delta_2) < L$. But then, following IVT, $\exists\ \tau_1 \in (t_1 + \delta_1 \ldots t_2 - \delta_2)$ such that $f(\tau_1) = L$. This contradicts the assumption that $f(t) \neq L$, for all $t_1 < t < t_2$. Thus,

$$\exists\ \delta_2 \in (0 \ldots \frac{1}{2}(t_3 - t_2)) \text{ such that } f(t_2 + \delta_2) < L.$$

Now let Property 2 not hold. Then, $\dot{f}(t_3^-) < 0$, and as before,

$$\exists\ \delta_3 \in (0 \ldots \frac{1}{2}(t_3 - t_2)) \text{ such that } f(t_3 - \delta_3) > L.$$

But, by IVT, there exists a time $t_2 + \delta_2 < \tau < t_3 - \delta_3$, such that $f(\tau) = L$. This contradicts the assumption that $f(t) \neq L$ for all $t_2 < t < t_3$. Thus, Property 2 holds. □

REFERENCES

[1] M. Khouzani, E. Altman, and S. Sarkar, "Optimal Quarantining of Wireless Malware Through Power Control," in *Proceedings of the Fourth Symposium on Information Theory and Applications (ITA)*, 2009.

[2] C. Zou, W. Gong, and D. Towsley, "Code red worm propagation modeling and analysis," in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM New York, NY, USA, 2002, pp. 138–147.

[3] J. Kephart and W. SR, "Directed-graph epidemiological models of computer viruses," in *Proceedings of 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, 1991, pp. 343–359.

[4] S. Sellke, N. Shroff, and S. Bagchi, "Modeling and Automated Containment of Worms," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 2, pp. 71–86, 2008.

[5] K. Rohloff and T. Bacşar, "Deterministic and stochastic models for the detection of random constant scanning worms," *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, vol. 18, no. 2, pp. 1–24, 2008.

[6] M. Hypponen, "Malware goes mobile," *Scientific American*, vol. 295, no. 5, pp. 70–77, 2006.

[7] B. Stone-Gross, C. Wilson, K. Almeroth, E. Belding, H. Zheng, and K. Papagiannaki, "Malware in IEEE 802.11 Wireless Networks," *Lecture Notes in Computer Science*, vol. 4979, p. 222, 2008.

[8] N. Ries, "Public health law and ethics: lessons from SARS and quarantine," *Health Law Review*, vol. 13, no. 1, pp. 3–6, 2004.

[9] D. Kienzle and M. Elder, "Recent worms: a survey and trends," in *Proceedings of the 2003 ACM workshop on Rapid malcode*. ACM New York, NY, USA, 2003, pp. 1–10.

[10] J. Kephart and S. White, "Computers and epidemiology," *IEEE Spectrum*, vol. 30, no. 5, pp. 20–26, 1993.

[11] J. Kephart and White, "Measuring and modeling computer virus prevalence," in *Proceedings of 1993 IEEE Computer Society Symposium on Research in Security and Privacy*, 1993, pp. 2–15.

[12] G. Serazzi and S. Zanero, "Computer Virus Propagation Models," *Lecture Notes in Computer Science*, pp. 26–50, 2004.

[13] G. Kesidis, I. Hamadeh, and S. Jiwasurat, "Coupled Kermack-Mckendrick models for randomly scanning and bandwidth saturating Internet worms," in *Proceedings of 3rd International Workshop on QoS in Multiservice IP Networks (QoS-IP)*. Springer, 2005, pp. 101–109.

[14] A. Wagner, T. Dübendorfer, B. Plattner, and R. Hiestand, "Experiences with worm propagation simulations," in *Proceedings of the 2003 ACM workshop on Rapid malcode*. ACM New York, NY, USA, 2003, pp. 34–41.

[15] G. Theodorakopoulos, J. Baras, and J.-Y. Le Boudec, "Dynamic Network Security Deployment Under Partial Information," in *46th Annual Allerton Conference on Communication, Control, and Computing*, 2008, pp. 261–267.

[16] K. Lye and J. Wing, "Game Strategies in Network Security," *International Journal of Information Security*, vol. 4, no. 1, pp. 71–86, 2005.

[17] P. Liu, W. Zang, and M. Yu, "Incentive-based Modeling and Inference of Attacker Intent, Objectives, and Strategies," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 1, pp. 78–118, 2005.

[18] M. Williamson, "Throttling viruses: restricting propagation to defeat malicious mobile code," in *Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC)*, 2002, pp. 61–68.

[19] C. Wong, C. Wang, D. Song, S. Bielski, and G. Ganger, "Dynamic Quarantine of Internet Worms," in *The International Conference on Dependable Systems and Networks (DSN)*, 2004, pp. 62–71.

[20] R. Dantu, J. Cangussu, and A. Yelimeli, "Dynamic Control of Worm Propagation," in *Proceedings of International Conference on Information Technology: Coding and Computing (ITCC).*, vol. 1, 2004.

[21] M. Khouzani, S. Sarkar, and E. Altman, "Maximum Damage Malware Attack in Mobile Wireless Networks," in *Proceedings of IEEE INFOCOM*, vol. 5, 2005.

[22] M. Khouzani and S. Sarkar, "Dynamic Malware Attack in Energy-Constrained Mobile Wireless Networks," in *Proceedings of the Fifth Symposium on Information Theory and Applications (ITA)*, 2010.

[23] M. Bloem, T. Alpcan, and T. Basar, "An optimal control approach to malware filtering," in *Decision and Control, 2007 46th IEEE Conference on*, 2007, pp. 6059–6064.

[24] X. Yan and Y. Zou, "Optimal Internet Worm Treatment Strategy Based on the Two-Factor Model," *ETRI JOURNAL*, vol. 30, no. 1, p. 81, 2008.

[25] S. Lenhart and J. Workman, *Optimal Control Applied to Biological Models*. Chapman & Hall/CRC, 2007.

[26] G. Feichtinger, J. Caulkins, D. Grass, G. Tragler, and D. Behrens, *Optimal Control of Nonlinear Processes: With Applications in Drugs, Corruption and Terror*. Springer, 2008.

[27] R. Morton and K. Wickwire, "On the optimal control of a deterministic epidemic," *Advances in Applied Probability*, vol. 6, no. 4, pp. 622–635, 1974.

[28] S. Sethi and P. Staats, “Optimal control of some simple deterministic epidemic models,” *Journal of the Operational Research Society*, vol. 29, no. 2, pp. 129–36, 1978.
[29] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge Univ Pr, 2005.
[30] C. Balanis, *Antenna theory: analysis and design*. John Wiley & Sons, 1982.
[31] C. Bettstetter, “Mobility Modeling in wireless networks: Categorization, smooth movement, and border effects,” *ACM SIGMOBILE Mobile Computing and Communications Review*, 2001.
[32] G. K. R Groenevelt, P Nain, “The message delay in mobile ad hoc networks,” *Performance Evaluation, Elsevier*, 2005.
[33] T.G.Kurtz, “Solutions of ordinary differential equations as limits of pure jump Markov processes,” *Journal of applied probabilities*, 1970.
[34] D. Kirk, *Optimal Control Theory: An Introduction*. Prentice Hall, 1970.
[35] A. Naguib, A. Paulraj, and T. Kailath, “Capacity improvement with base-station antenna arrays in cellular CDMA,” *IEEE Transactions on Vehicular Technology*, vol. 43, no. 3, pp. 691–698, 2002.
[36] F. Rashid-Farrokhi, L. Tassiulas, and K. Liu, “Joint optimal power control and beamforming in wireless networks using antenna arrays,” *IEEE Transactions on Communications*, vol. 46, no. 10, pp. 1313–1324, 2002.

MHR. Khouzani received the B. Sc degree from Sharif University of Technology, Iran in 2006. He received the M.S.E in Electrical and Systems Engineering, from University of Pennsylvania, Philadelphia, PA in 2008. He is currently a PhD candidate at Multimedia and Networking Laboratory in University of Pennsylvania, Philadelphia, PA. His research interests are in stochastic optimization, resource allocation and dynamic games in wireless networks.

Eitan Altman received the B.Sc. degree in electrical engineering (1984), the B.A. degree in physics (1984) and the Ph.D. degree in electrical engineering (1990), all from the Technion-Israel Institute, Haifa. In (1990) he further received his B.Mus. degree in music composition in Tel-Aviv university. Since 1990, Dr. Altman has been a researcher at INRIA (National research institute in computer science and control) in Sophia-Antipolis, France. He has been in the editorial boards of several scientific journals: Wireless Networks (WINET), Computer Networks (COMNET), Computer Communications (Comcom), J. Discrete Event Dynamic Systems (JDEDS), SIAM J. of Control and Optimisation (SICON), Stochastic Models, and Journal of Economy Dynamic and Control (JEDC). He received the best paper award in the Networking 2006, in Globecom 2007 and in IFIP Wireless Days 2009 conferences, and is a coauthor of two papers that have received the best student paper awards (at QoFis 2000 and at Networking 2002). His areas of interest include networking, stochastic control and game theory. More informaion can be found at www-sop.inria.fr/members/Eitan.Altman/

Saswati Sarkar received ME from the Electrical Communication Engineering Department at the Indian Institute of Science, Bangalore in 1996 and PhD from the Electrical and Computer Engineering Department at the University of Maryland, College Park, in 2000. She joined the Electrical and Systems Engineering Department at the University of Pennsylvania, Philadelphia as an Assistant Professor in 2000 where she is currently an Associate Professor. She received the Motorola gold medal for the best masters 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. She was an associate editor of IEEE Transaction on Wireless Communications from 2001 to 2006, and is currently an associate editor of IEEE/ACM Transactions on Networks. Her research interests are in stochastic control, resource allocation, dynamic games and economics of networks.