Dynamic Malware Attack in Energy-Constrained Mobile Wireless Networks

M.H.R. Khouzani, Saswati Sarkar

Abstract

Large scale proliferation of wireless technologies are dependent on developing reliable security measures against outbreaks of malware. The first step toward this goal is investigating the possible attack strategies of wireless malware and the extent of damage they can incur. A malware in a mobile wireless network relies on the infrastructure of the network and the constrained resources to spread itself. In this paper, we consider a battery-constrained mobile wireless network. The worm at each infective node at any given time may choose to amplify the transmission range and elevate the media scanning rate and thus increase the chance of contacting susceptible nodes and accelerate its spread. However, a larger transmission range and an elevated media scanning rate results in (a) easier detection of the malware and thus more effective counter-measure by the network, and (b) faster depletion of the battery and thus losing the node. Even if depleting the battery is an objective of the malware, early loss of infective nodes may thwart the spread of the malware. We assume the viewpoint of the malware and cast the problem of dynamically selecting the transmission range and media accessing rate in the infective nodes as an optimal control problem. We utilize Pontryagin's Maximum Principle to find an optimum solution. Moreover, we investigate the structural properties of an optimal solution to develop intuition about the nature of optimum attacks.

I. Introduction

A. Motivation and Overture

Wireless computing infrastructure is prone to the spread of self-replicating malicious codes known as malware. The malware can be used to initiate different forms of attacks on the wireless network. The attacks can vary from the less intrusive forms such as violation of confidentiality or privacy, as in traffic analysis and eavesdropping, to the more intrusive methods that either disrupt the normal functions of the nodes such as relaying data and establishing end-to-end routes (e.g., sinkhole attacks [1]), or even alter the network traffic and hence destroy the integrity of the information, as in unauthorized access and session hijacking attacks [2], [3]. Worms can moreover deplete the energy reserves of the nodes and render them dysfunctional, e.g., by aggressive media access attempts. 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 the design of effective security countermeasures. Experiences of malware outbreaks like those of Slammer [4] and Code Red [5] worms in wired Internet have demonstrated how expenses of the scales of billions of dollars can be inflicted in repair after viruses rapidly infected thousands of hosts within few hours.

The first step in devising efficient countermeasures is to envisage malware hazards, and understand the threats they pose, before they emerge in the hands of the attackers [6]. Specific attacks such as the wormhole [7], sinkhole [1], and Sybil [8], that utilize vulnerabilities in the routing protocols in a wireless sensor network, and their counter-measures, had been investigated before they were actually launched. We pursue the complementary but closely related goals of (i) quantifying fundamental limits on the damages that the attackers can inflict by intelligently choosing their actions, and (ii) identifying the optimal actions that inflict the maximum damage on the network. Such 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, constant changes in topology owing to mobility [9], their capabilities may well be limited by the above as well since they rely on the same network for propagating the malware.

Worms spread during data or control message transmission from nodes that are infected (*infectives*) and those that are vulnerable, but not yet infected (*susceptibles*). Counter-measures 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 future attacks. For instance, for SQL-Slammer worms [10], while StackGuard programs [11] immunize the susceptibles by removing the buffer overflow vulnerability that the worms exploit, specialized security patches [12] are required to remove the worm from (and thereby heal) the infectives. Nodes that have been immunized or healed are denoted as *recovered*. An infective node that has lost its energy reserve, as a result of aggressive and energy-intensive activities of the malware, is called a *dead* node. Depending on whether an infective node is drained of its battery by the malware 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.

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 [13].

B. A decision problem of the attacker

One of the most critical underlying resources in a mobile wireless network is the energy reserves of the nodes, i.e., the battery. An important decision of the worm pertains to its optimal use of the available energy of the infective nodes. The infectives, at any given time, can accelerate the rate of spread of the worm by increasing their contact rates with susceptibles by selecting higher transmission gains and media scanning rates. Such a choice, however, (a) can lead to easier detection of the malware, prompting the nodes to fetch appropriate security patches sooner, and (b) depletes the infective nodes' energy reserves faster which in turn limits the spread of the infection and also their other malicious activities such as eavesdropping, traffic destruction, *etc*. Even if the malware's objective is to render the nodes dysfunctional, early loss of infective nodes due to their battery depletion may thwart the spread of the malware. Due to these trade-offs, it is not trivial to determine the dynamically changing instantaneous transmission gain and/or media access rate of the infective nodes that maximizes the overall damage inflicted by the worm.

C. Contributions

First, we construct a mathematical framework which cogently models the effect of the decisions of the attackers on the state dynamics and their resulting trade-offs 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 infected and dead hosts, which are both changing with time. We assume the viewpoint of the malware, which seeks to maximize the damage by dynamically selecting the energy usages of its hosts while assuming full knowledge of the network parameters and the counter-measures. The maximum value of the 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 problem is cast as an optimal control problem which can be solved numerically by applying Pontryagin's Maximum Principle [14]–[16] (section III).

Second, we seek to develop insight about the nature of the optimum policies of the worm, also whether they are simple enough to be pursued by the malware. Towards this end, we investigate structures of the optimum solutions of the optimal control problem. Our results are significant and have negative connotations from the counter-measures point of view, as we show that an attacker can inflict the maximum damage by using very simple decisions. Specifically, if the malware seeks to maximize an aggregate over time of the fraction of the infective and the dead nodes but is not particularly interested in the final tally of them, the transmission range and media scanning rate has the following simple structure: until a certain time, the worm uses maximum power to spread itself, and right after that, the malware ceases its spreading effort (theorem 1). In other words, the malware's activity can be divided into (at most) two distinct phases: an initial *blitz* phase and a subsequent *stealth mode* phase. During the initial phase, the malware in each infective node uses the maximum power to aggressively spread the malware (blitz phase), until a threshold time at which, infective nodes cease their media access activities and enter an energy-saving mode. During the stealth mode phase, infective nodes furtively perform their malicious activities: eavesdropping, traffic analysis, sabotaging routes, changing data, *etc*. In optimal control terminology [14]–[16], we have proved that the optimal strategy has a *bang-bang* structure, that is, at any given time, the optimum power usage is either at its minimum or maximum possible values; in addition it has at most one jump which necessarily terminates at the minimum possible value. Optimality of this simple strategy for this nontrivial problem is in fact quite surprising.

If, on the other hand, the malware is interested in increasing the final tally of the dead nodes in addition, then our next result (corollary 1) states that there are up to three distinct phases: the initial *blitz* phase during which infective nodes use maximum power to spread the infection as aggressively as possible, the intermediate energy-saving *stealth mode* phase during which malware ceases the power-intensive media access activities in the infective nodes, and finally the *slaughter* phase when the media access activities are turned back on with maximum power, but this time with the primary goal of depleting the remaining batteries of the infectives and *killing* them.

D. Related Works

Malware outbreaks in wireless networks constitute an emerging research topic (e.g., [17]–[24]), though, the research on spread of malware has traditionally focused on wired networks. Epidemic modeling based on the classic Kermack-Mckendrick model [25] has extensively been used to analyze the spread of malware in wired networks [5], [26]–[34], *etc*, and more recently in wireless networks [35]. 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 represent 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 these however do not identify the optimal policies nor provide provable performance guarantees, but instead propose heuristic dynamic policies in different contexts, and evaluate through simulations the efficacies and various trade-offs of the policies they propose. For example, [36] proposes heuristics for dynamic quarantining of nodes in wired networks that appear suspicious through traffic analysis, and [37] introduces heuristic strategies for dynamically adjusting the transmission power of attacker nodes in wireless

networks. We instead obtain attack policies that provably attain the maximum possible damage and consider a general model that incorporates healing, immunization and mortality of nodes.

Interestingly, tools from the optimal control theory such as the effective theorem of Pontryagin maximum Principle has rarely been used for analyzing network security - [38] and our previous work [39] constitute notable exceptions. The first formulates the trade-off for optimal treatment of the infective nodes in wired networks. However, in contrast to our work, the solution is based on numerical evaluations only and no structural property of the optimal policy is established. One of our earlier works [39] proposes reduction of reception gain of wireless nodes as a counter-measure for slowing down the spread of malware in wireless networks. Another one of our papers [40] focuses on the attack viewpoint and considers the transmission range of the infective nodes and the rate of killing as two independent dynamic parameters of the worm to inflict the maximum damage. In particular, killing a node is achieved by executing a malicious code damaging a vital part of the hardware. Moreover, [40] considers a worm with a power budget which specifically ensures that every infective node lasts the entire duration of interest. In contrast, we consider the case in which the killing process of the infective nodes is not independent of the energy-greedy media access activities. Furthermore, we consider another side-effects of an aggressive media access activity, which is exposing an anomaly and hence, easier detection of the malware.

II. System Model

A. Dynamics of State Evolution

A **susceptible** node is a mobile wireless device which 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 to it. A node that has lost its battery reserve is denoted as a **dead** node, that is, it cannot function any longer. A functional node that is immune to the worm is referred to as **recovered**. Installation of appropriate security patches, by the respective users or the network operator, can *immunize* susceptibles to the recovered states, also *heal* infectives to the recovered states.

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 $D(t) = n_D(t)/N$ (Table I) respectively. Then, $S(t) + I(t) + R(t) + D(t) = 1$.

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

TABLE I
List of notations of measures.

We assume that at the time of the outbreak of the infection, that is at time zero, some but not all nodes are infected: $0 < I(0) = I_0 < 1$. For simplicity, we assume $R(0) = D(0) = 0$. Thus, $S(0) = 1 - I_0$.

We now model the dynamics of infection propagation. Nodes are assumed to roam in a vast 2-D region of area A with an average velocity v. An infective transmits a message to a susceptible with a given probability whenever the two are in *contact*, that is, the susceptible is in the transmission range of the infective. This probability is a linear function of the rate at which the infective scans the media in search of susceptibles nearby, and the proportionality constant is determined by the message collision probability η_1. When the communication range of the nodes is small compared to A (which is usually the case in multihop networks), η_1 is essentially determined by the overall node density (N/A). Next, under mobility models such as random waypoint or random direction model [41], Groenevelt *et al*. [42] have shown that the time between consecutive contacts of a specific pair of nodes is nearly *exponentially* distributed, and the rate of this exponential process is linearly dependent[1] on the communication range of the nodes with a proportionality constant η_2 that depends only on v and A. Specifically, $\eta_2 \propto \frac{1}{A}$. Let $u(t)$ be the product of the infective's transmission range and its media scanning rate. Then, the worm is transmitted between a given infective-susceptible pair as per an exponential random process whose rate at any given time t is $\hat{\beta}u(t)$, where $\hat{\beta} = \eta_1\eta_2$. The worm regulates the spread of the infection by controlling $u(t)$ through appropriate choice of its transmission gain and media scanning rate.

The security patches are installed at an infective (susceptible, respectively) after exponentially distributed random times starting from when it is infected ($t = 0$, respectively). The delays account for the time required in detection of infection, and fetching the appropriate security patch, etc. We denote the immunization and healing rates respectively by $q + Q(u)$ and $\pi q + B(u)$, which we next explain explicitly. First, consider the part of the countermeasure rates which does not depend on

[1]The result has been proved when the communication range of the nodes is small compared to the total area of the region and v is sufficiently high. Numerical computations reveal that the result holds even otherwise.

u, i.e., q and πq. Typically, the rate of immunization is no less than the rate of healing, as the security patch required for immunization involves only rectification of the vulnerability that rendered the susceptibles accessible to the attack, whereas the second involves both the removal of the worm and the vulnerability that the worm exploits. This makes it harder to obtain a healing security patch than an immunizing one. Moreover, the malware in an infective node may sabotage the effectiveness of the security patch. π can also represent the case in which a single type of security patch immunizes the susceptibles, however successfully removes the infection and heals an infective node with probability π and with probability $1-\pi$ it fails to do so. Next, we investigate the part of the countermeasure rates which is a function of u. The rates of immunization and healing are affected by u, the product of the transmission range and media scanning rate of the infective nodes: a larger transmission range and a higher rate of scanning the media facilitates detection of the malware [43], [44]. This in turn increases the overall recovery rate since it reduces the delay associated with detection of the malware. This effect is modeled by allowing the overall rates of immunization and of healing to be increasing functions of u. The effect of u can potentially be different for healing and immunization since detection of the malware is likely more critical for healing than the immunization. We have introduced increasing and differentiable functions $B(u)$ and $Q(u)$ to capture the correlation between a higher u and easier detection and, consequently, a larger healing and immunization rate, respectively. That is, the instantaneous rates of healing and immunization are $\pi q + B(u)$ and $q + Q(u)$.[2] In practice, the advantage of easier detection starts to saturate after large enough u, thus it makes sense to assume that both $B(u)$ and $Q(u)$ functions are concave. We will however address both cases of concave and convex B and Q functions.

Each node has a limited battery capacity. We allow the nodes to have different amounts of initial energy reserves, i.e., energy reserve at $t=0$ when the attack starts. We allow the initial remaining battery to be random, and for conventicle of the analysis, exponentially distributed. When the media access rate is u, the battery depletes proportionally. and the rate of depletion of the battery can be approximated to be linear when u is not too large. In wireless networks, especially multi-hop wireless networks, u is constrained to be less than a designated value $u_{\max}$. Thus u cannot be too large and the rate of battery depletion can be represented by ρu, where ρ is a positive coefficient. Since the worm might not know the remaining energy reserves, the selected $u(t)$ at a given node at a given time is not a function of the remaining battery at that (and any other) node(s).

Following the conditions assumed for the model, the number of nodes of each type evolves according to a pure jump Markov chain with state vector $(n_S(t), n_I(t), n_D(t))$. Since for all t, $n_S(t)+n_I(t)+n_R(t)+n_D(t)=N$, the state of the Markov chain is three dimensional. Let $\beta = \lim_{N\to\infty} N\hat{\beta}$.

Now[3] according to the results of [45], as N grows, $S(t)$, $I(t)$ and $D(t)$ converge to the solution of the following system of differential equations[4]:

$$\dot{S}(t) = -\beta u(t) I(t) S(t) - qS(t) - Q(u(t))S(t) \qquad S(0) = 1 - I_0 \tag{1a}$$

$$\dot{I}(t) = \beta u(t) I(t) S(t) - \pi q I(t) - B(u(t)) I(t) - \rho u(t) I(t) \qquad I(0) = I_0 \tag{1b}$$

$$\dot{D}(t) = \rho u(t) I(t) \qquad D(0) = 0. \tag{1c}$$

and also satisfy the following constraints at all t:

$$0 \le S(t), I(t), D(t) \tag{2a}$$

$$S(t) + I(t) + D(t) \le 1. \tag{2b}$$

The convergence is in the following sense:

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

and likewise for $I(t)$ and $D(t)$.

Similar epidemic models have been validated through experiments as well as network simulations which indicate that such epidemic models provide an acceptable representation of the spread of malware in mobile wireless networks (see e.g. [46], [47]).

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

[2]Note that we did not assume that the detection is affected by the fraction of infected nodes. An alternative model could incorporate that effect too.

[3]Note that since $\hat{\beta} = \eta_1 \eta_2$, and η_1 depends only on the node density, and $\eta_2 \propto \frac{1}{A}$, the limit β exists as long as the node density $\lim_{N\to\infty} N/A$ exists for large N.

[4]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).

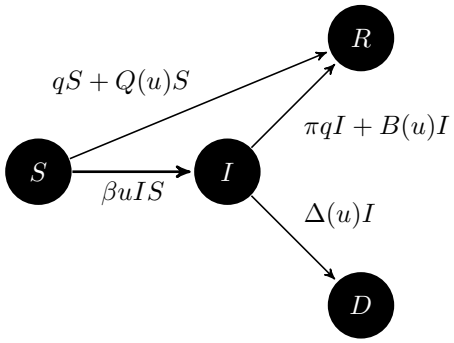

Fig. 1. $u(t)$ is product of the transmission range$\times$media scanning rate of infectives at time t.

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 dead and the infected hosts. Recall that the malware can use the infective nodes to (i) eavesdrop and analyze traffic generated or relayed by the infected hosts, or the traffic that traverses in the hosts' vicinity, and (ii) alter or destroy the traffic 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:

$$J = \int_0^T \{\kappa_I I(t) + \kappa_D D(t)\}\, dt + K_I I(T) + K_D D(T). \tag{3}$$

where $\kappa_I, \kappa_D, K_I, K_D \geq 0$. Note that this reward function includes the case where a malware cares only about the infective (by $\kappa_D = K_D = 0$) or the case in which it only seeks after killing the nodes (by assuming $\kappa_I = K_I = 0$). We make the following technical assumption:

$$\text{If} \quad \kappa_I = \kappa_D = q = 0 \quad \text{then} (K_D - K_I)\rho u_{\max} - B(u_{\max})K_I s > 0 \tag{4}$$

The attacker seeks to maximize the damage function by appropriately regulating $u(t)$, the product of the transmission range and the scanning rate of the infective nodes[5] subject to:

$$0 \leq u(t) \leq u_{\max} \tag{5}$$

The bounds on $u(t)$ are dictated by the physical constraints of the transmitters and also for ensuring that the interference and hence collisions between simultaneous transmissions remain limited.

Any continuous function $u : [0, T] \to \mathbb{R}$ such that the left and right hand limits exist and that satisfy the constraint in (5) belongs to the *control region* denoted by Ω.

We first show that for any $u(t) \in \Omega$, the state constraints in (2) are automatically satisfied throughout $(0 \ldots T]$. Thus, we safely ignore (2) henceforth.

Lemma 1: For any $u \in \Omega$, the state functions $(S, I, D) : [0, T] \to \mathbb{R}^3$ that satisfy (1), also satisfy (2). Moreover, $S(t) \geq (1 - I_0)e^{-C_1 t} > 0$, $I(t) \geq I_0 e^{-C_2 t} > 0$ for $t \in [0, T]$ and some finite C_1, C_2.

The constants turn out to be $C_1 = \beta u_{\max} + q + Q(u_{\max}), C_2 = \pi q + B(u_{\max})$. The proof is similar to that of lemma 1 in [39], and is omitted for brevity.

Once the control u is selected, the system state vector (S, I, D) is specified at all t as a solution to (1). The state and control functions pair $((S, I, D), u)$ is called an *admissible pair* if (i) u is in Ω, i.e. satisfies (5), (ii) u is piecewise continuous such that the left and right hand limits exist at the points of discontinuity, and (iii) eq.'s in (1) hold. The function u is then called an admissible control. Let $((S, I, D), u)$ be an admissible pair. Now, if

$$J(u) \geq J(\underline{u}) \quad \text{for any admissible control } (\underline{u})$$

then $((S, I, D), u)$ is called an *optimal solution* and 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 parameters of the system, such as the mobility pattern, the reception gain of the susceptibles and the healing and immunization rate functions $(q, \pi, Q(.), B(.))$. 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 counter-measures are adaptive or the attacker does not know the above parameters.

[5]The attacker does not control any other parameter such as the susceptible's reception gain, server's transmission gains, mobility patterns, *etc.*

III. WORM'S OPTIMAL CONTROL

We now present a framework using which the worm can determine its *optimal control* functions u and also compute the maximum value of the damage function. Throughout this section, variables without an underline correspond to their value according to an optimal solution, whereas underlined variables are according to any feasible solution.

The main challenge in computing the optimal control is that the differential equations (1) can be solved provided the functions $\underline{u}$ are known. Thus, the only approach seems to be that of an exhaustive search on all functions $\underline{u}$ in Ω. This will require the evaluation of the damage function $J(\underline{u})$ for each one of such functions where the corresponding $(\underline{I}, \underline{D})$ functions required in evaluating $J(\underline{u})$ are obtained by solving (1) for each such function. But, 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.

Let $((S, I, D), u)$ be an optimal solution. Consider the *Hamiltonian* H, and the *co-state* or *adjoint* functions $\lambda_1(t)$ to $\lambda_3(t)$ defined as follows:

$$H := \kappa_I I + \kappa_D D + (\lambda_2 - \lambda_1)\beta u I S - \lambda_1(q + Q(u))S - \lambda_2(\pi q + B(u))I + (\lambda_3 - \lambda_2)\rho u I \tag{6}$$

$$\begin{aligned} \dot{\lambda}_1 &= -\frac{\partial H}{\partial S} = -(\lambda_2 - \lambda_1)\beta u I + \lambda_1(q + Q(u)) \\ \dot{\lambda}_2 &= -\frac{\partial H}{\partial I} = -\kappa_I - (\lambda_2 - \lambda_1)\beta u S + \lambda_2(\pi q + B(u)) - (\lambda_3 - \lambda_2)\rho u \\ \dot{\lambda}_3 &= -\frac{\partial H}{\partial D} = -\kappa_D \end{aligned} \tag{7}$$

along with the final (or *transversality*) conditions:

$$\lambda_1(T) = 0, \quad \lambda_2(T) = K_I, \quad \lambda_3(T) = K_D \tag{8}$$

Then according to Pontryagin's Maximum Principle With Terminal Constraints ([14, P.111 theorem 3.14]), there exists continuous and piecewise continuously differentiable co-state functions λ_1, λ_2 and λ_3 that at every point $t \in [0 \dots T]$ where $u(t)$ is continuous satisfy (7), and the transversality conditions (8), and we have at each t :

$$u(t) \in \arg\max_{\underline{u}(t) \in \Omega} H(\vec{\lambda}(t), (S(t), I(t), D(t)), \underline{u}(t)) \tag{9}$$

Maximizing the Hamiltonian as per (9), we obtain:

$$\begin{aligned} &(\lambda_2 - \lambda_1)\beta u I S - \lambda_1 Q(u) S - \lambda_2 B(u) I + (\lambda_3 - \lambda_2)\rho u I \\ &\quad \geq (\lambda_2 - \lambda_1)\beta \underline{u} I S - \lambda_1 Q(\underline{u}) S - \lambda_2 B(\underline{u}) I + (\lambda_3 - \lambda_2)\rho \underline{u} I. \end{aligned} \tag{10}$$

for all admissible $\underline{u}$. Let

$$\varphi(u) := (\lambda_2 - \lambda_1)\beta u I S - \lambda_1 Q(u) S - \lambda_2 B(u) I + (\lambda_3 - \lambda_2)\rho u I \tag{11}$$

Thus we ought to maximize $\varphi(\underline{u})$ over the admissible $\underline{u}$. A very important observation is that $\varphi(u) \geq 0$. This is simply because $u = 0$ is a feasible candidate for maximization of $\varphi(u)$ and it makes it zero. Following lemma 2, which will come later, $\lambda_1, \lambda_2 \geq 0$. Thus the concavity of φ with respect to $\underline{u}$ is opposite of that of Q and B, that is, if Q and B are concave in $\underline{u}$ then $\varphi(\underline{u})$ is convex, and vice versa. Note that we assumed that Q and B are either both concave, or both convex. We thus differentiate the following two cases:

- concave $Q \Rightarrow$ convex φ;
- convex $Q \Rightarrow$ concave φ.

We start from the first case, i.e., concave Q and B, which is when the sensitivity of the detection, which is equal to the (partial) derivative of Q and B with u, reduces with more intense media access activity of the malware (more aggressive scanning rates, larger transmission powers). Since for concave Q and B, φ would be convex and is continuous in u, we face a convex maximization. Thus the maxima occur necessarily at the extrema of the range of the control, which are determined by comparison. Hence:

$$u = \begin{cases} 0, & \varphi(u_{\max}) < 0 \\ u_{\max}, & \varphi(u_{\max}) > 0, \end{cases} \tag{12}$$

Note that $\varphi(u_{\max})$ is a continuous and differentiable function of time.

Now we consider the second case, where Q and B are convex. Since for convex Q and B, φ is concave, we thus are dealing with a concave maximization. Hence, the maxima of $\varphi(u)$ occur necessarily at the points where the partial derivative w.r.t u is zero or the extrema of the ranges of the control, which are then determined by comparison. Let

$$\psi := (\lambda_2 - \lambda_1)\beta I S + (\lambda_3 - \lambda_2)\rho I \tag{13}$$

and

$$C(u) = \lambda_1 Q(u) + \lambda_2 B(u)$$

Then:

$$u = \begin{cases} 0, & \psi \le C'(0), \\ C'^{-1}(\psi) & C'(0) < \psi \le C'(u_{\max}), \\ u_{\max}, & C'(u_{\max}) < \psi \end{cases} \tag{14}$$

where $C'(u) := \frac{\partial}{\partial u} C(u) = \lambda_1 Q'(u) + \lambda_2 B'(u)$.

Combining (1), (7), (12) (or (14), depending on the concavity of Q and B and (8), we obtain a system of (non-linear) differential equations with boundary values that involve only the state and co-state functions (and not the control u). Functions S, I, D and λ_1 to λ_3 that satisfy these differential equations and final values, can therefore be obtained using standard numerical procedures that solve differential equations [48]. Now, the optimal control u can be explicitly obtained using the above solutions in (12) (or (14), accordingly).

IV. Structural Properties of optimum u

In this section, we investigate the structural properties of an optimal energy usage of the malware that inflicts the maximum damage. It is difficult (or perhaps impossible) to obtain a closed-form solution to the differential equations leading to the optimal solution. However, as we will see, it is possible to examine and establish structural properties of the optimal solution without access to the close form solution. Our objective is to develop insight about the nature of the optimum policies of the malware, and to examine whether they are simple enough to be pursued by the malware. Our results are significant and have negative connotations from the counter-measures point of view, as we show that an attacker can inflict the maximum damage by using very simple decisions. Our major results are that for concave Q and B, the transmission range and media scanning rate has the following simple structure: until a certain time, the worm uses maximum power to spread itself, and right after that, the malware ceases its spreading effort (theorem 1). In optimal control terminology [14]–[16], we have proved that the optimal strategy has a *bang-bang* structure, that is, at any given time, the optimum power usage is either at its minimum or maximum possible values; in addition it has at most one jump which necessarily terminates at the minimum possible value. Optimality of this simple strategy for this nontrivial problem is in fact quite surprising.

Before we delve into the properties of u, we will need an important lemma, which we appealed to in the previous section (after eq. (11)), and that we will use extensively hereafter.

Lemma 2: For $t \in [0 \dots T)$ we have $\lambda_1 > 0, \lambda_3 \ge 0$ and $(\lambda_2 - \lambda_1) > 0$.

Note that the lemma also implies that $\lambda_2 > 0$. The shadow price interpretation of co-state functions provides an intuition about this lemma: shadow rewards associated with susceptible and infective and dead nodes are positive from the viewpoint of the malware. Moreover, the shadow reward of an infective node is at least as much as the shadow reward of a susceptible one.

Proof: The proof for $\lambda_3 \ge 0$ is straightforward: referring to (8), $\lambda_3(T) = K_D \ge 0$ and $\dot{\lambda}_3 = -\kappa_D \le 0$. Hence (e.g. by integration) $\lambda_3 \ge 0$.

Step-1. We show that $\lambda_2(t) - \lambda_1(t)$ is strictly positive over an interval of nonzero length towards the end of interval $(0 \dots T)$. Following (8), $\lambda_2(T) = (\lambda_2(T) - \lambda_1(T)) = K_I \ge 0$. If $K_I > 0$, this is due to continuity of $\lambda_2 - \lambda_1$, and if $K_I = 0$ but $\kappa_I > 0$ it follows because $(\dot{\lambda}_2(T) - \dot{\lambda}_1(T)) = -\kappa_I(T) - \rho u(T) K_D < 0$. If $K_I = \kappa_I = 0$ but $K_D > 0$, then $u(T) > 0$[6] and $(\dot{\lambda}_2(T) - \dot{\lambda}_1(T)) = -\rho u(T) K_D < 0$, hence the claim. For the case in which $K_I = K_D = \kappa_I = 0$ and only $\kappa_D > 0$, we have $(\ddot{\lambda}_2(T^-) - \ddot{\lambda}_1(T^-)) = \rho u(T)^6 \kappa_D > 0$ which yields the claim. A similar argument applies to λ_1 and we can show that $\lambda_1(t) > 0$ over an interval of nonzero length toward the end of $(0 \dots T)$. We have $\dot{\lambda}_1(T) = -K_I \beta u(T) I(T) \le 0$. Now if this value is strictly negative then the claim follows. If $K_I = 0$, then we have $\ddot{\lambda}_1(T) = (\kappa_I + \rho u(T) K_D) \beta u(T) I(T) \ge 0$. If this value is strictly positive then the claim is established. If, however, $K_I = \kappa_I = K_D = 0$ and only $\kappa_D > 0$ then $u(T) > 0$[6] and $\dddot{\lambda}_1(T^-) = -(\rho u(T) \kappa_D) \beta u(T) I(T) < 0$, settling the validity of the claim.

Step-2. Let t^* be the last time at which (at least) one of these two strict positivity constraints is violated, i.e., for $t^* < t < T$, we have:

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

[6]because following (10) u needs to maximize φ and in this case $\varphi(u_{\max})|_T = K_D \rho u_{\max} I(T) > 0$. However $\varphi(0)|_T = 0$ hence $0 < u(T) \le u_{\max}$.

- Case 1: $\lambda_2(t^*) - \lambda_1(t^*) = 0$ and $\lambda_1(t^*) \geq 0$. Now:

$$\begin{aligned}
&(\dot{\lambda}_2(t^{*+}) - \dot{\lambda}_1(t^{*+})) \\
&= -\kappa_I - \frac{\varphi(u)}{I} + \lambda_2 \pi q - \lambda_1 q - \lambda_1 \frac{Q(u)S}{I} - \lambda_1 Q(u) && [\because (7)] \\
&= -\kappa_I - \frac{\varphi(u)}{I} - (1-\pi)\lambda_2 q - \lambda_1 \frac{Q(u)S}{I} - \lambda_1 Q(u) && (15)
\end{aligned}$$

  Recall that $\varphi(u) \geq 0$. Also, from the definition of t^*, $\lambda_2(t^{*+}) \geq 0$. Thus, we observe that $[\frac{d}{dt}(\lambda_2 - \lambda_1)]|_{t^{*+}} \leq 0$. Thus, by integration, case 1 could not occur.
- Case 2: $\lambda_1(t^*) = 0$, and $\lambda_2(t^*) - \lambda(t^*) > 0$, Then, from (7), $\dot{\lambda}_1(t^{*+}) = -(\lambda_2 - \lambda_1)\beta u_0 I$. Since in this case $(\lambda_2(t^*) - \lambda_1(t^*)) > 0$, we have $\dot{\lambda}_1(t^{*+}) < 0$ which is impossible. Hence case 2 is also ruled out.

Therefore, none of the two cases could occur, which is a contradiction with existence of t^*. Hence follows the lemma. ■

We consider concave (or linear) Q and B functions in this section. So far, we know from (12) that for concave Q and B, an optimum u is at zero or $u_{\max}$, depending on the sign on $\varphi(u_{\max})$. First of all, note that

$$\varphi(u_{\max})|_T = K_I \beta u_{\max} I(T) S(T) - B(u_{\max}) K_I I(T) + (K_D - K_I)\rho u_{\max} I(T). \tag{16}$$

Based on the given parameters, (16) can be either positive or negative, if $K_D \gg K_I$ then $\varphi(u_{\max})|_T > 0$. In this case, we are sure that u ends up at $u_{\max}$. For the number of jumps we investigate the sign of time derivative of $\varphi(u_{\max})$:

$$\begin{aligned}
\dot{\varphi}(u_{\max}) = \frac{d}{dt}\{&(\lambda_2 - \lambda_1)\beta u_{\max} IS - Q(u_{\max})\lambda_1 S - B(u_{\max})\lambda_2 I + (\lambda_3 - \lambda_2)\rho u_{\max} I\} \\
&= (\dot{\lambda}_2 - \dot{\lambda}_1)\beta u_{\max} IS + (\lambda_2 - \lambda_1)\beta u_{\max} \dot{I} S + (\lambda_2 - \lambda_1)\beta u_{\max} I \dot{S} \\
&\quad - Q(u_{\max})(\dot{\lambda}_1 S + \lambda_1 \dot{S}) - B(u_{\max})(\dot{\lambda}_2 I + \lambda_2 \dot{I}) \\
&\quad + (\dot{\lambda}_3 - \dot{\lambda}_2)\rho u_{\max} I + (\lambda_3 - \lambda_2)\rho u_{\max} \dot{I}
\end{aligned}$$

which after replacing and simplification, we obtain:

$$\begin{aligned}
\frac{\dot{\varphi}(u_{\max})}{I} &= B(u_{\max})\kappa_I + \kappa_I \rho u_{\max} - \kappa_D \rho u_{\max} \\
&\quad - \pi q \lambda_3 \rho u_{\max} - S\beta\kappa_I u_{\max} + S\pi q \beta \lambda_1 u_{\max} - S\beta\lambda_2 q u_{\max} \\
&\quad - Q(u) S\beta\lambda_2 u_{\max} + Q(u_{\max}) S\beta\lambda_2 u - B(u)\lambda_3 \rho u_{\max} + B(u_{\max})\lambda_3 \rho u + B(u) S\beta\lambda_1 u_{\max} - B(u_{\max}) S\beta\lambda_1 u
\end{aligned}$$

Notice that following (12),

$$\begin{aligned}
Q(u_{\max})u - Q(u)u_{\max} &\equiv 0 \\
B(u_{\max})u - B(u)u_{\max} &\equiv 0.
\end{aligned}$$

Thus we can further simplify as follows:

$$\begin{aligned}
\frac{\dot{\varphi}(u_{\max})}{I} &= \kappa_I(B(u_{\max}) + \rho u_{\max} - S\beta u_{\max}) - \kappa_D \rho u_{\max} \\
&\quad - \pi q \lambda_3 \rho u_{\max} - Sq\beta u_{\max}(\lambda_2 - \pi\lambda_1)
\end{aligned} \tag{17}$$

In the light of eq. (17), we present two types of results for two ranges of parameters. Here are the two cases:

Case 1. $\pi = 0$, that is, the healing process relies on the activity of the malware. This assumption pertains to the case where recognition of an infective node is essential in removing it.

Case 2. $B \equiv 0$, i.e., healing is not affected by increasing u. A trivial case is where there is no healing involved and the only counter-measure is immunization. Moreover, $\kappa_D \geq \kappa_I$, and $K_D \geq K_I$: the dead nodes are at least as interesting as the infective (i.e. achieve no less utility per node for the dead than the infective.) The first case becomes especially interesting when infective nodes are more attractive to the malware than the dead.

In the first case, we perform the following re-arrangement of the remaining terms of $\frac{\dot{\varphi}(u_{\max})}{I}$ in (17) as the following:

$$\begin{aligned}
\frac{\dot{\varphi}(u_{\max})}{I} &= \kappa_I(B(u_{\max}) + \rho u_{\max}) - \kappa_D \rho u_{\max} && (18a) \\
&\quad - \kappa_I \beta u_{\max} S && (18b) \\
&\quad - \lambda_2 S q \beta u_{\max} && (18c)
\end{aligned}$$

We now show that, wherever u is continuous, expressions in 18a, 18b and 18c all have positive time derivatives (i.e., they are all non-decreasing in time). Note that the expression in (18a) is constant, thus its time derivative is zero. The time derivative of the term in (18b) is as follows:

$$\frac{d}{dt}(-\kappa_I \beta u_{\max} S) = -\kappa_I \beta u_{\max} \dot{S}$$

Referring to (1) and lemma 1, $\dot{S}$ is (strictly) negative and hence, the time derivative of (18b) is positive. For the expression in (18c) we have:

$$\frac{d}{dt}(-\lambda_2 S q \beta u_{\max}) = -\dot{\lambda}_2 S q \beta u_{\max} - \lambda_2 \dot{S} q \beta u_{\max} \tag{19}$$

The second term in the above equation is positive due to lemma 2 and negativity of $\dot{S}$ which we just discussed. In order to prove that the first term is positive we need to show that $\dot{\lambda}_2$ is negative. We start from rewriting $\dot{\lambda}_2$ in (7) as follows (noting that $\pi = 0$ for the case we are investigating):

$$\dot{\lambda}_2 = -\kappa_I - \frac{\varphi(u)}{I} - \lambda_1 \frac{QS}{I} \tag{20}$$

Recalling that $\varphi(u) \geq 0$ and referring to lemmas 1 and 2, all terms in (20) are negative. Thus, all of the terms in (19) are positive. Therefore, (18) is positive. A closer scrutiny also reveals that at least one of the terms in (18) has a strictly positive time-derivative at any given time: if either $\kappa_D > 0$ or $\kappa_I > 0$, then this follows respectively from expressions in (18a) and (18b). If $q > 0$, then the claim follows from expression in (18c)[7]. This leads to the following theorem:

Theorem 1: For concave Q and B, if $\pi = 0$ (the first case) and moreover $K_D = K_I = 0$, then an optimal u has at most one jump from $u_{\max}$ to 0. It can be always at $u_{\max}$ or can be always at zero.

Proof: Since we showed that $\frac{\dot{\varphi}(u_{\max})}{I}$ is always strictly increasing, and since $I > 0$, then (a) $\varphi(u_{\max})$ cannot be equal to zero on an interval of non-zero length; (b) $\varphi(u_{\max})$ cannot change its sign more than twice and they are from positive to negative and then back to positive throughout $[0 \dots T]$. However, $\varphi(u_{\max})|_T = 0$ and thus, at most one change in the sign of $\varphi(u_{\max})$ is possible, and that is from positive to negative. Cases in which $\varphi(u_{\max})$ is always negative or always positive are not negated. Referring to (12), the proof is complete. ∎

Let us develop some intuition about theorem 1. If the final tally of the infective and dead nodes are not matters of interest for the malware, i.e., $K_I = K_D = 0$, then the malware's activity can be divided into (at most) two distinct phases: a *blitz* phase and a subsequent *stealth mode* phase. During the initial phase, the malware in each infective node aggressively uses the maximum power to spread the malware (blitz phase), until a threshold time at which infective nodes cease their media access activities, and enter an energy-saving mode. For the malware, the benefits of using the maximum power for spreading the infection prevail over its harms (higher risk of detection and battery-drainage of the infectives) before the switching time. During the stealth mode phase, malware furtively performs its malicious activities in infective nodes: eavesdropping, traffic analysis, sabotaging routes, changing data, *etc*. During the stealth mode phase, due to the drop in the number of susceptibles from the initial phase, it is not worth trying to spread the malware which just results in easier detection and early depletion of the infective nodes' batteries.

Corollary 1: If on the other hand, we did NOT have that $K_I = K_D = 0$, then according to the sign of $\varphi(u_{\max})|_T$ in (16), we can have up to two jumps which terminates in $u_{\max}$ (the case in which $\varphi(u_{\max})|_T > 0$); or up to one jump which terminates in 0 (the case in which $\varphi(u_{\max})|_T < 0$).

Proof: The proof is identical to the proof of theorem 1. ∎

Referring to (16), the first case occurs, e.g., when $K_D \gg K_I$, that is, the malware is interested in increasing the final tally of dead nodes as well. Then corollary 1 can be interpreted as follows. There are up to three distinct phases: the initial *amassing* phase during which infective nodes use maximum power to as aggressively as possible spread the infection, the intermediate energy-saving *stealth mode* phase during which malware ceases the power-intensive media access activities in the infective nodes, and finally the *slaughter* phase when the media access activities are turned back on with maximum power, but this time with the primary goal of depleting the batteries of the infectives and killing them.

Now turning our focus to the second case, i.e. $B \equiv 0, \kappa_D \geq \kappa_I, K_D \gg K_I$, we rearrange the terms in (17) as in the following:

$$\frac{\dot{\varphi}(u_{\max})}{I} = (\kappa_I - \kappa_D)\rho u_{\max} \tag{21a}$$

$$-\pi q \lambda_3 \rho u_{\max} \tag{21b}$$

$$-S\beta\kappa_I u_{\max} \tag{21c}$$

$$-\beta u_{\max} S q (\lambda_2 - \pi\lambda_1) \tag{21d}$$

[7]In case where $\kappa_I = \kappa_D = q = 0$, then we have $\dot{\varphi}(u_{\max}) = 0$ which means $\varphi(u_{\max})|_t = \varphi(u_{\max})|_T$. Referring to (16) and the technical assumption in (4), $\varphi(u_{\max})|_t = \varphi(u_{\max})|_T \neq 0$.

Each term in each line of the above expression is negative. Moreover, at least one of them is strictly negative at any given time[8]. Hence we have the following theorem:

Theorem 2: For concave Q and B, for the case where $B \equiv 0, \kappa_D \geq \kappa_I$ and $K_D \gg K_I$, the optimal u is $u_{\max}$ throughout $[0 \dots T]$.

Proof: Based on the above calculations and since $I > 0$ for all times, then $\dot{\varphi} < 0$ and since $\varphi(u_{\max})|_T \geq 0$ (a) $\varphi(u_{\max})$ is not constant on any subinterval and (b) has no zero crossing points inside the interval $[0 \dots T)$ and the theorem follows from (12). ■

Remark 1: From the expressions in (17) and the above proof, it should be clear that the condition $(\kappa_D - \kappa_I)\rho u_{\max} \geq \kappa_I B(u_{\max})$ and $(K_D - K_I)\rho u_{\max} \geq K_I B(u_{\max})$ suffices for the validity of the same result.

Remark 2: A moment of reflection indicates that this result was not trivial, and its simplicity is indeed significant: using $u_{\max}$ has both the harmful effects of easier detection and thus faster recovery of nodes (losing them) and early battery depletion of infective nodes (potentially resulting in self-throttling of the epidemic). But theorem 2 states that for a malware that primarily cares about the final tally of dead nodes and the effect of high activity on detection of infective nodes is not dominant then regardless of the negative effects, it is optimal to use maximum power for media access throughout.

REFERENCES

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

[2] D. Welch and S. Lathrop, "Wireless security threat taxonomy," in *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, pp. 76–83, 2003.

[3] A. Herzog, N. Shahmehri, and C. Duma, "An ontology of information security," *International Journal of Information Security and Privacy*, vol. 1, no. 4, pp. 1–23, 2007.

[4] 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, 2003.

[5] 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*, pp. 138–147, ACM New York, NY, USA, 2002.

[6] E. Filiol, M. Helenius, and S. Zanero, "Open problems in computer virology," *Journal in Computer Virology*, vol. 1, no. 3, pp. 55–66, 2006.

[7] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *IEEE INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3.

[8] J. Douceur, "The sybil attack," in *Peer-to-Peer Systems, First International Workshop, IPTPS 2002, Cambridge, MA, USA, March 7-8, 2002, Revised Papers*, pp. 251–260.

[9] J. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," *Security in Distributed, Grid, Mobile, and Pervasive Computing*, p. 367, 2007.

[10] 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, 2003.

[11] C. Cowan, C. Pu, D. Maier, H. Hinton, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, and Q. Zhang, "StackGuard: Automatic adaptive detection and prevention of buffer-overflow attacks," in *Proceedings of the 7th USENIX Security Conference*, vol. 78, San Antonio: USENIX Press, 1998.

[12] Symantec, "W32.sqlexp.worm," (02.13.2007).

[13] N. Weaver and V. Paxson, "A worst-case worm," in *Proc. Third Annual Workshop on Economics and Information Security (WEIS'04)*, 2004.

[14] D. Grass, A. Vienna, J. Caulkins, and P. RAND, *Optimal Control of Nonlinear Processes*. Springer-Verlag Berlin Heidelberg, 2008.

[15] D. Kirk, *Optimal Control Theory: An Introduction*. Prentice Hall, 1970.

[16] A. Seierstad and K. Sydsaeter, *Optimal control theory with economic applications*. 1986.

[17] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, "A social network based patching scheme for worm containment in cellular networks," *IEEE INFOCOM, Rio de Janeiro, Brazil*, 2009.

[18] Y. Yang, S. Zhu, and G. Cao, "Improving sensor network immunity under worm attacks: a software diversity approach," in *Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing*, pp. 149–158, ACM New York, NY, USA, 2008.

[19] B. Sun, G. Yan, Y. Xiao, and T. Andrew Yang, "Self-propagating mal-packets in wireless sensor networks: Dynamics and defense implications," *Ad Hoc Networks*, 2009.

[20] C. Fleizach, M. Liljenstam, P. Johansson, G. Voelker, and A. Mehes, "Can you infect me now?: malware propagation in mobile phone networks," in *Proceedings of the 2007 ACM workshop on Recurring malcode*, pp. 61–68, ACM New York, NY, USA, 2007.

[21] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38–47, 2004.

[22] A. Bose and K. Shin, "Proactive security for mobile messaging networks," in *Proceedings of the 5th ACM workshop on Wireless security*, pp. 95–104, ACM New York, NY, USA, 2006.

[23] A. Bose, *Propagation, Detection and Containment of Mobile Malware*. PhD thesis, The University of Michigan, 2008.

[24] A. El Fawal, J. Le Boudec, and K. Salamatian, "Vulnerabilities in epidemic forwarding," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007*, pp. 1–6, 2007.

[25] D. Daley and J. Gani, *Epidemic modelling: an introduction*. Cambridge Univ Pr, 2001.

[26] J. Kephart, S. White, I. Center, and Y. Heights, "Directed-graph epidemiological models of computer viruses," in *Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on*, pp. 343–359, 1991.

[27] J. Kephart, S. White, I. Center, and Y. Heights, "Measuring and modeling computer virus prevalence," in *Research in Security and Privacy, 1993. Proceedings., 1993 IEEE Computer Society Symposium on*, pp. 2–15, 1993.

[28] J. Kephart, S. White, D. Chess, I. Center, and N. Hawthorne, "Computers and epidemiology," *Spectrum, IEEE*, vol. 30, no. 5, pp. 20–26, 1993.

[29] C. Staniford, V. Paxson, and N. Weaver, "How to 0wn the Internet in Your Spare Time," in *Proceedings of the 11th USENIX Security Symposium, San Francisco, CA*, 2002.

[8]It is because either $\kappa_D > 0$, or if $\kappa_D = 0$ then it has to be that $K_D > 0$ to have realized this case. The latter and the facts that $\lambda_3(T) = K_D$ and $\dot{\lambda}_3 = -\kappa D = 0$ will lead to $\lambda_3 = \kappa > 0$.

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

[31] Z. Chen, L. Gao, and K. Kwiat, "Modeling the spread of active worms," in *IEEE INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3.

[32] C. Zou, W. Gong, and D. Towsley, "Worm propagation modeling and analysis under dynamic quarantine defense," in *Proceedings of the 2003 ACM workshop on rapid malcode*, pp. 51–60, ACM New York, NY, USA, 2003.

[33] G. Serazzi and S. Zanero, "Computer Virus Propagation Models," *LECTURE NOTES IN COMPUTER SCIENCE*, pp. 26–50, 2004.

[34] 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*, pp. 101–109, Springer, 2005.

[35] S. Tanachaiwiwat and H. A., "Encounter-based worms: Analysis and defense," *Ad Hoc Networks, Elsevier JOURNAL*, 2009.

[36] C. Zou, W. Gong, and D. Towsley, "Worm propagation modeling and analysis under dynamic quarantine defense," in *Proceedings of the 2003 ACM workshop on Rapid Malcode*, pp. 51–60, ACM New York, NY, USA, 2003.

[37] V. Karyotis and S. Papavassiliou, "Risk-based attack strategies for mobile ad hoc networks under probabilistic attack modeling framework," *Computer Networks*, vol. 51, no. 9, pp. 2397–2410, 2007.

[38] 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.

[39] 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*, University of California at San Diego, 2009.

[40] M. Khouzani, S. Sarkar, and E. Altman, "Maximum Damage Malware Attack in Mobile Wireless Networks," *To appear in Infocom 2010*.

[41] C. Bettstetter, "Mobility modeling in wireless networks: categorization, smooth movement, and border effects," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 3, pp. 55–66, 2001.

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

[43] H. Kim, J. Smith, and K. Shin, "Detecting energy-greedy anomalies and mobile malware variants," in *Proceeding of the 6th international conference on Mobile systems, applications, and services*, pp. 239–252, ACM, 2008.

[44] A. Bose, X. Hu, K. Shin, and T. Park, "Behavioral detection of malware on mobile handsets," in *Proceeding of the 6th international conference on Mobile systems, applications, and services*, pp. 225–238, ACM, 2008.

[45] T. Kurtz, "Solutions of ordinary differential equations as limits of pure jump Markov processes," *Journal of Applied Probability*, pp. 49–58, 1970.

[46] R. Cole, "Initial Studies on Worm Propagation in MANETS for Future Army Combat Systems," 2004.

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

[48] M. Hirsch and S. Smale, *Differential equations, dynamical systems, and linear algebra*. Academic Press Inc, 1974.