Maximum Damage Battery Depletion Attack in Mobile Sensor Networks

M.H.R. Khouzani, Saswati Sarkar

***Abstract*—Developing reliable security measures against outbreaks of malware will facilitate the proliferation of wireless sensing technologies. The first step toward this goal is to investigate potential attack strategies and the extent of damage they can incur. The malware at each infective node may seek to contact more susceptible nodes by amplifying the transmission range and the media scanning rate and thereby accelerate its spread. This may however lead to (a) easier detection of the malware and thus more effective counter-measure by the network, and (b) faster depletion of the battery which may in turn thwart further spread of the infection and/or exploitation of that node. We assume the viewpoint of the malware and cast the problem of dynamically selecting the transmission range and media access rate of the infective nodes as an optimal control problem. We utilize Pontryagin's maximum principle to find an optimum solution, and prove that the maximum damage can be attained using simple three-phase bang-bang strategies.**

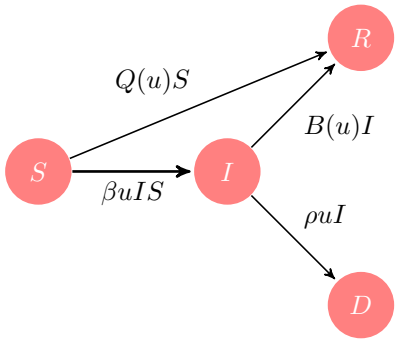


Fig. 1. State transitions: S, I, R, D respectively represent susceptible, infective, recovered, dead states. Here, $u(t)$ is product of the transmission range and media scanning rate of infectives at time t. The parameters β, ρ and functions $B(\cdot), Q(\cdot)$ will be defined in Section II-A.

I. Introduction

A. Motivation and Overture

Wireless sensor networks consisting of mobile nodes are envisioned to facilitate a diverse set of applications ranging from environment monitoring to emergency search-and-rescue operations [1]. Such networks are however prone to the spread of self-replicating malicious codes known as malware. The malware can be used to initiate different forms of attacks ranging from the less intrusive eavesdropping of the sensed data to the more virulent disruption of node functions such as relaying and establishing end-to-end routes (e.g., sinkhole attacks [2]), or even destroying the integrity of the in transit sensed data, as in unauthorized access and session hijacking attacks [3], [4]. Malware can moreover deplete the energy reserves of the sensor nodes and render them dysfunctional either deliberately or as a result of aggressive media access attempts in attempt to infect others. The economic viability of the investments on the sensing infrastructure is therefore contingent on the design of effective security countermeasures.

The first step in devising efficient countermeasures is to anticipate the hazards and understand the threats the attacks pose, before they are launched [5]. Specific attacks such as the wormhole [6], sinkhole [2], and Sybil [7], that utilize vulnerabilities in the routing protocols in a wireless sensor network, and their counter-measures, had been investigated proactively. We pursue the complementary but closely related goals of (i) quantifying fundamental limits on the damages that the attackers can inflict on the network by intelligently choosing their actions, and (ii) identifying the optimal actions that inflict the maximum damage. Such quantification is motivated by the fact that while attackers can pose serious threats by exploiting the fundamental limitations of wireless sensor networks, such as limited energy, unreliable communication, constant changes in topology owing to mobility [8], their capabilities may well be limited by the above as well since they rely on the same network for propagating the malware.

Malware spreads during data or control message transmission from nodes that are infected (*infectives*) to those that are vulnerable, but not yet infected (*susceptibles*). Countermeasures can be launched by installing security patches that either *heal* the infectives or *immunize* the susceptibles by removing the malware and rectifying the underlying vulnerability. Nodes that have been immunized or healed are robust against future attacks and denoted as *recovered*. A node that has lost its battery reserve, is denoted as *dead*, since it can not function any longer. Depending on whether the malware drains an infective's battery before the infective fetches a patch, its state changes to dead or recovered. Susceptibles either become infectives or recovered depending on whether they communicate with infectives before installing the patches. Figure 1 illustrates the state transitions.

The attack seeks to infect and kill as many nodes as possible, use the malware in the infectives to disrupt the hosts as well as the network functions while being cognisant of the countermeasures [9].

B. A decision problem of the attacker

One of the most critical resources in a mobile sensor network is the energy reserves of the nodes. An important

Parts of this work were presented in 2010 Information Theory and Application (ITA) workshop, University of California.

The authors 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. This work has been supported by NSF grants NSF-CNS-0914955, NSF-CNS-0915203 and NSF-CNS-0915697.

decision of the malware 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 malware 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 patches sooner, and (b) depletes the infectives' 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 goal is to render the nodes dysfunctional, early loss of infectives due to their battery depletion may thwart the spread of the malware. The challenge then is to determine the dynamically[1] changing instantaneous transmission gain and/or media access rate of the infectives that maximize the overall damage inflicted by the malware.

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 (sec.II). Specifically, we assume that the damage inflicted by the malware is a cumulative function increasing in the number of infected and dead sensors. 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 malware. The damage maximization problem is cast as an optimal control problem which can be solved numerically by applying Pontryagin's maximum principle [10] (sec.III).

Second, we seek to determine whether the optimal strategies are simple enough to be pursued by the malware while using resource constrained wireless devices. Our results have negative connotations from the counter-measures point of view, as we show that an attacker can inflict the maximum damage by using simple decisions. Specifically, if it seeks to maximize an aggregate over time of the fraction of the infective and the dead nodes but is not concerned about their final tallies, the transmission range and media scanning rate have the following simple structure: until a certain time, the malware uses the maximum power to aggressively spread itself, and subsequently it ceases its media access activities altogether and enters an energy-saving mode while furtively performing its malicious activities like eavesdropping, analyzing sensed data, sabotaging routes, changing data, *etc*. (theorem 1, sec. IV). Thus, the attack consists of an initial *blitz* phase and a subsequent *stealth* phase. If, on the other hand, the malware seeks also to increase the final tally of the dead nodes, then a final *slaughter* phase follows the initial *blitz* and intermediate *stealth* phases. In the final slaughter phase, the malware resumes, at the maximum power, the media access activities of the infected nodes, seeking primarily to kill them by depleting their residual energy reserves. In optimal control terminology [10], 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; also it has at most two jumps between them. Optimality of this simple strategy for this nontrivial problem is surprising. Finally, our numerical computations reveal that the attacker can inflict substantially higher damage by dynamically, rather than statically, choosing the infectives' transmission range and media scanning rates, and the attack is robust to errors in estimation of the network parameters (sec. V).

[1]A dynamic strategy allows the decision variables to vary with time, whereas a static strategy chooses their values at $t = 0$ and does not change them subsequently.

D. Related Works

Energy constraints in attacks on mobile wireless networks have been considered in [11]–[17]. Now, [15]–[17] consider only detection policies based on the anomalous battery consumption behavior due to the activities of a new malware. Next, [13] describes a vulnerability in MMS services in cellular networks that enables an attacker to drain the device batteries, and [14] proposes battery depletion through reduction of sleep cycles of sensors. We focus on managing, rather than merely depleting, the device batteries for maximizing the overall damage inflicted on the network which is fostered both by the spread of the infection and the battery depletion. The closest to our work are [11] and [12] which propose strategies for utilizing the infectives' available energy so as to increase the spread of the malware; [11] proposes heuristics which do not provide any damage guarantee, whereas [12] focuses on the static (as opposed to dynamic) optimum choice of the malware's parameters. Also, [12] considers a S-I-S system where each node is either infected or susceptible and the infection (healing, resp.) rate of a susceptible (infective, resp.) does not change with time. We consider a S-I-R-D system allowing for susceptible, infected, dead and recovered nodes, and the infection (recovery, resp.) rate of a susceptible (infective or susceptible, resp.) dynamically evolves in accordance with the number of infectives (attacker's control, resp.).

Most of the existing work on dynamic control of parameters of the network (e.g., [18]) or the malware (e.g., [19]) propose heuristic dynamic policies in different contexts, and evaluate them using simulations. For example, [19] 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 characterize the damage they inflict.

Interestingly, tools from the optimal control theory such as the Pontryagin's maximum principle have seen limited used in context of network security - [20] and our previous works [21]–[24] constitute notable exceptions. [20] formulates the trade-off for optimal treatment of the infective nodes in wired networks, but does not establish any structural property of the optimal policy. In [21], we propose to slow down the spread of malware by reducing the reception gain of nodes and attain desired tradeoffs between security risks and network quality of service through the dynamic optimal control of the reception gain. In [23], [24], we obtain optimal patching

strategies that attain desired tradeoffs between security risks and bandwidth consumption in patch dissemination. In [22], we have considered the transmission range of the infectives and the rate of killing as two independent parameters of the malware, and have optimized them to inflict the maximum damage. The malware chooses the transmission range subject to a power budget which ensures that every infective's battery lasts the entire duration of interest, and kills an infective by executing a code that damages its hardware. In contrast, here we allow the death rate of the infectives to increase with increase in energy consumed in media access. Also, aggressive media access exposes an anomaly and leads to earlier detection of the malware and therefore faster recovery of the nodes.

II. System Model

A. Dynamics of State Evolution

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 nodes
$I(t)$	fraction of the infective nodes
$R(t)$	fraction of the recovered nodes
$D(t)$	fraction of the dead nodes

TABLE I
List of notations of measures.

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, let $R(0) = D(0) = 0$. Thus, $S(0) = 1 - I_0$.

We now model the dynamics of infection propagation using epidemic models based on the classic Kermack-Mckendrick model [25]. Experiments as well as network simulations have validated that such models provide an acceptable representation for the spread of malware in mobile wireless networks (see e.g. [26]–[28]) - we independently validate them in Section V. Nodes are roaming in a vast 2-D region of area A with an average velocity v. An infective spreads the malware to a susceptible while transmitting data or control messages to it. 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 which depends on the medium access protocol used and also on the node density (N/A). 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 node density (N/A). We assume that the time between consecutive contacts of a specific pair of nodes is *exponentially* distributed with a rate that is linearly dependent on the communication range of the nodes and the proportionality constant η_2 depends only on v and A.[2] Specifically, $\eta_2 \propto \frac{1}{A}$. Let $u(t)$ be the product of the infective's transmission range and its media scanning rate at time t. Then, the malware 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 malware 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 patch, etc. We denote the immunization and healing rates respectively by $Q(u)$ and $B(u)$. A larger transmission range and a higher scanning rate leads to faster detection of the malware [15], [31], and therefore increases the overall recovery rate. Thus, $Q(\cdot)$ and $B(\cdot)$ are non-decreasing functions of u. We assume that $Q(x) > 0$ if $x > 0$. In practice, the advantage of easier detection starts to saturate with increase in u, thus both $B(\cdot)$ and $Q(\cdot)$ are likely to be concave, though we allow them to be convex as well[3]. We assume that $Q(\cdot)$ and $B(\cdot)$ are differentiable functions of u, and also $Q(0) = B(0) = 0$, i.e., no spreading/battery drainage attempts of the malware results in zero recovery rate, though we relax this latter assumption in Remark 2. Finally, we allow $Q(\cdot), B(\cdot)$ to be different functions as different patches may be required for immunization and healing, as the former involves only rectification of the vulnerability that the malware exploits, whereas the latter involves the removal of the malware as well. For instance, while StackGuard programs [32] immunize the susceptibles by removing the buffer overflow vulnerability that the SQL-Slammer malware [33] exploits, specialized patches [34] are required to remove the malware from (and thereby heal) the infectives.

Nodes have random amounts of initial (i.e., at $t = 0$ when the attack starts) energy reserves. The energy consumption during normal operations (i.e., when a node is susceptible or recovered) is negligible as compared to that in media access of the infectives - the former is therefore assumed to be zero.[4] The energy depletion time of an infective's battery will therefore be random with a distribution that depends on its media access activities - we assume this time to be exponentially distributed with rate $\rho u(t)$ at time t. Here, ρ is a positive coefficient. Note that the exponential assumption has been made for convenience of analysis. Also, the depletion rate must be an increasing function of u, we assume it to be a linear function, since u can not be large in order to avoid interference. Since the malware might not know the remaining energy, the selected $u(t)$ at a given node at a given t is not a function of its (or others') residual energies.

[2]Under mobility models such as random waypoint or random direction [29], Groenevelt *et al.* [30] have shown this to be the case when the communication range of the nodes is small compared to A and v is large. Numerical computations [30] reveal that these assumptions can be largely relaxed.

[3]The detection may also be affected by the fraction of infected nodes, which can be incorporated by allowing $Q(\cdot), B(\cdot)$ to be functions of both u and I.

[4]The formulations presented in Sections II and III easily extend when this assumption is relaxed, by allowing a transition from the susceptible state to the dead state (fig. 1).

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 $(S(t), I(t), D(t), R(t))$. Since for all t, $S(t) + I(t) + D(t) + R(t) = 1$, the state of the Markov chain is three dimensional. Let

$$\beta = \lim_{N\to\infty} N\hat{\beta}. \tag{1}$$

Let $\beta > 0$. Now[5], using the results of [35], it can be shown that, as N grows, $S(t)$, $I(t)$ and $D(t)$ converge to the solution of the following system of differential equations:[6]

$$\dot{S}(t) = -\beta u(t) I(t) S(t) - Q(u(t)) S(t), \tag{2a}$$

$$\dot{I}(t) = \beta u(t) I(t) S(t) - B(u(t)) I(t) - \rho u(t) I(t), \tag{2b}$$

$$\dot{D}(t) = \rho u(t) I(t), \tag{2c}$$

$$\text{with} \quad S(0) = 1 - I_0, I(0) = I_0, D(0) = 0, \tag{2d}$$

and also satisfy the following constraints at all t:

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

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 $D(t)$.

Henceforth, wherever not ambiguous we drop the dependence of $S(t), I(t), D(t), u(t)$ on t and make it implicit. Fig. 1 illustrates the transitions between different states of nodes.

B. Maximum Damage Attack

We consider a malware that seeks to inflict the maximum possible damage in a time window $[0, T]$ of its choice. It benefits over time from the dead and the infected hosts. Recall that it can use the infectives to eavesdrop, analyze, alter or destroy data sensed or relayed by the hosts. It also benefits by inflicting a large death-toll by the end of the desired time window. These motivate the following damage function:

$$J = \int_0^T \{\kappa_I I(t) + \kappa_D D(t)\}\, dt + K_I I(T) + K_D D(T). \tag{4}$$

where $\kappa_I > 0$ and $\kappa_D, K_I, K_D \ge 0$.

The malware seeks to maximize the damage function by appropriately regulating $u(t)$, the product of the transmission range and the scanning rate of the infectives.[7] When sensors are moving fast and no sensor has any information about the location of others, each sensor is equally likely to meet any other sensor in future irrespective of the past.[8] Therefore, at any given time the optimal control will be the same for all infectives. The choice of $u(t)$ is subject to:

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

The above bounds arise from the physical constraints of the transmitters and also for ensuring that the interference among simultaneous transmissions remain limited.

Any piecewise continuous function $u : [0, T] \to \mathbb{R}$ such that the left and right hand limits exist and that satisfies (5) belongs to the *control region* denoted by Ω. Now, for any $u(\cdot) \in \Omega$, the state constraints in (3) are satisfied throughout $[0, T]$.

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

Thus, we ignore (3) henceforth. The following proof reveals that $C_1 = \beta u_{\max} + Q(u_{\max})$ and $C_2 = \rho u_{\max} + B(u_{\max})$.

Proof: According to (2), S, I, D are differentiable, and therefore, continuous functions of time. Note that at $t = 0$, by assumption we have $0 < I = I_0 < 1$, and also $0 < S = 1 - I_0 < 1$. Hence, from the continuity of S, I, it follows that $S > 0$ and $I > 0$ in an interval starting from $t = 0$. Since $D(0) = 0$ and $\dot{D} \ge 0$ in this interval, it follows that $D \ge 0$ in this interval. Next, $S + I + D = 1$ at $t = 0$, however, by summing equations (2a), (2b) and (2c) we have $\frac{d}{dt}(S + I + D) \le 0$, and hence $S + I + D \le 1$ throughout this interval. Now, if the lemma is not true, from the continuity of S, I, D, either $S = 0$ or $I = 0$ or $D < 0$ or $S + I + D > 1$ at some $t < T$. Then there exists a time t^* such that $S > 0, I > 0, D \ge 0, S + I + D \le 1$ in $[0, t^*)$ and $S(t^*) = 0$ or $I(t^*) = 0$ or $D(t^*) < 0$ or $S(t^*) + I(t^*) + D(t^*) > 1$. Note that $D(t^*) \ge 0$ and $S(t^*) + I(t^*) + D(t^*) \le 1$ from the continuity of S, I, D. For $0 < t < t^*$, from (2a) we have $\dot{S} \ge -C_1 S$, where $C_1 = (\beta u_{\max} + Q(u_{\max}))$. Thus $S \ge S(0)e^{-C_1 t}$, for all $0 \le t < t^*$ and therefore, due to continuity of S, $S(t^*) > 0$. Similarly, for $0 < t < t^*$ from (2b) we have $\dot{I} \ge -C_2 I$, where $C_2 = \rho u_{\max} + B(u_{\max})$. Thus $I(t^*) > 0$ as well. The result follows from this contradiction. ■

Once the control $u(\cdot)$ is selected, the system state vector $(S(\cdot), I(\cdot), D(\cdot))$ can be obtained as a solution to (2). The state and control functions pair $((S(\cdot), I(\cdot), D(\cdot)), u(\cdot))$ is called an *admissible pair* and $u(\cdot)$ is called an *admissible control* if (i) $u(\cdot)$ is in Ω, and (ii) the pair satisfies (2). If for an admissible pair $((S, I, D), u)$,

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

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 malware, we assume that it computes its optimal control assuming full knowledge of the network parameters, such as β, ρ, initial fraction I_0 of the infectives and the countermeasure functions $(Q(.), B(.))$, which do not change in $[0, T]$. The damage can only be equal or lower otherwise.

[5]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 limiting node density $\lim_{N\to\infty} N/A$ exists.

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

[7]The attacker does not control any other parameter such as the susceptible's reception gain, node mobilities, *etc.*

[8]This assumption can be analytically established when the inter-contact times between sensors are independent and exponentially distributed.

III. Malware's optimal control

We now present a framework using which the malware can determine its *optimal control* function $u(\cdot)$ and also compute the maximum value of the damage function. The main challenge in computing the optimal control is that the differential equations (2) can be solved *provided* the control is known. But, since Ω consists of an uncountably infinite number of such controls, an exhaustive search on Ω is ruled out. This dilemma may however be elegantly resolved using *Pontryagin's maximum principle* which we apply next.

We start with by clarifying a notation: u (and other functions without an underline) represents the optimal control (and functions corresponding to it) whereas $\underline{u}$ represents an admissible control. 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:

$$\begin{aligned} H := \quad & \kappa_I I + \kappa_D D + (\lambda_2 - \lambda_1)\beta u I S - \lambda_1 Q(u) S \\ & -\lambda_2 B(u) I + (\lambda_3 - \lambda_2)\rho u I \end{aligned} \tag{6}$$

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

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 ([10, P.111 theorem 3.14]), there exists continuous and piecewise differentiable co-state functions λ_1, λ_2 and λ_3 that at every point $t \in [0, T]$ where $u(t)$ is continuous, satisfy (7), (8), and we have at each t :

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

Let

$$\begin{aligned} \varphi(x) := \quad & (\lambda_2 - \lambda_1)\beta x I S - \lambda_1 Q(x) S - \lambda_2 B(x) I \\ & +(\lambda_3 - \lambda_2)\rho x I. \end{aligned} \tag{10}$$

Note that for each x $\varphi(x)$ is a continuous function of time. Maximizing the Hamiltonian as per (9), we obtain:

$$\varphi(u(t)) \geq \varphi(\underline{u}(t)) \ \forall \ t, \ \forall \text{ admissible } \underline{u}.$$

Since $\underline{u} = 0$ is admissible, $\varphi(u(t)) \geq 0$ at each t. Following lemma 2, which will come later, $\lambda_1, \lambda_2 \geq 0$. Thus:

- concave $Q, B \Rightarrow \varphi(x)$ is convex in x at each t;
- convex $Q, B \Rightarrow \varphi(x)$ is concave in x at each t.

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). Then, at each t, $\varphi(x)$ is convex in x, and its maxima for $x \in [0, u_{\max}]$ must occur at $x = 0$ or $x = u_{\max}$. Hence:

$$u(t) = \begin{cases} 0, & \text{if } \varphi(u_{\max}) < 0 \text{ at } t \\ u_{\max}, & \text{if } \varphi(u_{\max}) > 0 \text{ at } t. \end{cases} \tag{11}$$

If either $Q(\cdot)$ or $B(\cdot)$ is strictly concave, $\varphi(x)$ is strictly convex in x at each t, and $u(t) \in \{0, u_{\max}\}$ at each t.

If both Q and B are convex, then, at each t, $\varphi(x)$ is concave in x, and its maxima for $x \in [0, u_{\max}]$ must occur either at $x = 0$, or $x = u_{\max}$, or at x such that $\varphi'(x) = 0$. Let

$$\begin{aligned} \psi &:= (\lambda_2 - \lambda_1)\beta I S + (\lambda_3 - \lambda_2)\rho I, \\ C(x) &:= \lambda_1 Q(x) + \lambda_2 B(x). \end{aligned} \tag{12}$$

Then:

$$u(t) = \begin{cases} 0, & \text{if } \ \psi \leq C'(0) & \text{at } t, \\ C'^{-1}(\psi) & \text{if } \ C'(0) < \psi \leq C'(u_{\max}) & \text{at } t, \\ u_{\max}, & \text{if } \ C'(u_{\max}) < \psi & \text{at } t, \end{cases} \tag{13}$$

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

Combining (2), (7), (8) and (11) (or (13), depending on the concavity of Q and B), we obtain a system of (non-linear) differential equations with boundary values that involve only the state S, I, D and co-state $\lambda_1, \lambda_2, \lambda_3$ functions (and not the control u). $S, I, D, \lambda_1, \lambda_2, \lambda_3$ can therefore be obtained using standard numerical procedures that solve differential equations [36]. Now, the optimal control u can be obtained using the above solutions in (11) (or (13), accordingly).

IV. Structural Properties of optimum u

We show that for concave $Q(\cdot), B(\cdot)$, the optimal $u(\cdot)$ is a *bang-bang* function of time, that is, at any given time, it is either at its minimum or maximum possible values, $0, u_{\max}$ respectively (theorem 1). Moreover, the number of jumps it exhibits between the extreme values is at most two.

We first state the lemma that we will use extensively hereafter. We appealed to it in section III (after eq. (10)).

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

Thus, also, $\lambda_2 > 0$. The lemma is consistent with the shadow reward interpretation of co-state functions: shadow rewards associated with susceptible, infective and dead nodes are positive from the malware's point of view. Also, the infectives fetch at least as much shadow reward as the susceptibles.

Proof: Referring to (8), $\lambda_3(T) = K_D \geq 0$, and at any t at which u is continuous, $\dot{\lambda}_3 = -\kappa_D \leq 0$. Also, u and λ_3 are piecewise continuous and continuous functions of time respectively. Hence, (e.g. by integration) $\lambda_3 \geq 0$.

Next, let there exist an interval $[t_1, T)$ over which $(\lambda_2 - \lambda_1) \geq 0$. Then, we show that $\lambda_1 \geq 0$ for $t \in [t_1, T)$. Referring to (7), over this interval, at any t at which u is continuous, we have: $\dot{\lambda}_1 \leq Q(u_{\max})\lambda_1$. Therefore, from the continuity of λ_1, over this interval, $\lambda_1(t) \geq \lambda_1(T) e^{Q(u_{max})(t-T)}$. The result follows since $\lambda_1(T) = 0$. The entire lemma therefore follows if we show that $(\lambda_2 - \lambda_1) > 0$ for $t \in [0, T)$, which we now set to do.

Step-1. We show that for some $\delta > 0$, $\lambda_2(t) - \lambda_1(t) > 0$ for $t \in [T-\delta, T)$. Following (8), $\lambda_2(T) = (\lambda_2(T) - \lambda_1(T)) = K_I \geq 0$. If $K_I > 0$, the above holds due to continuity of $\lambda_2 - \lambda_1$. If $K_I = 0$ and $\kappa_I > 0$, it follows because[9] $(\dot{\lambda}_2(T^-) - \dot{\lambda}_1(T^-)) = -\kappa_I - \rho u(T) K_D < 0$.

Step-2. Let $\lambda_2 - \lambda_1 \leq 0$ at some $t \in [0, T)$. Then there exists t^* such that

$$\text{for } t^* < t < T : \lambda_2(t) > \lambda_1(t), \text{ and } \lambda_2(t^*) = \lambda_1(t^*). \quad (14)$$

Thus, $\lambda_1 \geq 0$ for $t \in [t^*, T)$.

$$(\dot{\lambda}_2(t^{*+}) - \dot{\lambda}_1(t^{*+})) = -\kappa_I - \frac{\varphi(u)}{I} - \lambda_1 \frac{Q(u)S}{I} - \lambda_1 Q(u). \quad (15)$$

Recall that $\varphi(u) \geq 0$. Thus, as $\kappa_I > 0$, it follows from lemma 1 that $\dot{\lambda}_2(t^{*+}) - \dot{\lambda}_1(t^{*+}) < 0$. Since u is piecewise continuous, $\lambda_2(t) - \lambda_1(t)$ is differentiable in $(t^*, t^* + \delta)$ for some $\delta > 0$. Thus, $\dot{\lambda}_2(t) - \dot{\lambda}_1(t) < 0$ for all $t \in (t^*, t^* + \delta)$ for some $\delta > 0$. Referring to (14) and the continuity of $\lambda_2(t) - \lambda_1(t)$, this contradicts the Mean value theorem. Therefore, $\lambda_2 - \lambda_1 > 0$ for all $[0, T)$. ∎

We consider concave Q and B functions in this section. From (11), at any t at which u is continuous,

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

If both Q, B are linear, then

$$Q(u_{\max})u - Q(u)u_{\max} \equiv 0, \text{ and } B(u_{\max})u - B(u)u_{\max} \equiv 0.$$

The above also holds if either Q or B is strictly concave as then $u(t) \in \{0, u_{\max}\}$ at each t. Thus, at any t at which u is continuous,

$$\frac{\dot{\varphi}(u_{\max})}{I} = \kappa_I (B(u_{\max}) + \rho u_{\max} - S\beta u_{\max}) - \kappa_D \rho u_{\max}. \quad (16)$$

From (2), lemma 1 and since S is a continuous function, S is also a non-increasing function of time. Hence, as $\kappa_I > 0$, $\frac{\dot{\varphi}(u_{\max})}{I}$ is a non-decreasing function of time, ignoring its values at the (finite number of) discontinuity points of u. Also, S is constant in any interval in which $\dot{\varphi}(u_{\max}) = 0$. Thus, from (2) and lemma 1 and since $Q(x) \neq 0$ if $x \neq 0$, $u = 0$ in any such interval except at the discontinuity points of u.

Also, from (10),

$$\begin{aligned} \varphi(u_{\max})|_T = \; & K_I \beta u_{\max} I(T) S(T) - B(u_{\max}) K_I I(T) \\ & + (K_D - K_I)\rho u_{\max} I(T). \end{aligned} \quad (17)$$

We are now ready to prove the following theorem:

Theorem 1. *Let Q and B be concave. Then for any optimal u, there exists t_1, t_2 such that $0 \leq t_1 \leq t_2 \leq T$, and*

- *$u(t) = u_{\max}$ for $0 \leq t < t_1$ (*blitz phase*);*
- *$u(t) = 0$ for $t_1 < t < t_2$ (*stealth phase*);*
- *$u(t) = u_{\max}$ for $t_2 < t \leq T$ (*slaughter phase*).*

If $K_I = K_D = 0$, $t_2 = T$, i.e., the slaughter phase does not exist.

Proof: (a) First, in any interval in which $\varphi(u_{\max}) = 0$, $\dot{\varphi}(u_{\max}) = 0$, and hence $u = 0$ except at the discontinuity points of u. (b) Next, consider an interval in which $\varphi(u_{\max}) \leq 0$. Since $\frac{\dot{\varphi}(u_{\max})}{I}$ is non-decreasing (ignoring finite number of points), and since $I > 0$ (from lemma 1) either the interval can be divided in (i) two subintervals such that $\varphi(u_{\max}) = 0$ in one, and $\varphi(u_{\max}) < 0$ in the other, (ii) or three subintervals such that $\varphi(u_{\max}) < 0$ in the intermediate and $\varphi(u_{\max}) = 0$ in the boundary ones. Now, from (a) and (11), $u = 0$ throughout the interval (except at its discontinuity points) in both cases.

Now, first let $\varphi(u_{\max})|_T \leq 0$. From (17), this case, for example, arises when $K_I = K_D = 0$. Again, arguing as in (b), if $\varphi(u_{\max})|_{t'} > 0$, for some $t' \in (0, T)$, then $\varphi(u_{\max})|_t > 0$ for all $t < t'$. The lemma now follows from (b) and (11), with $t_2 = T$ and $t_1 = \inf\{t : \varphi(u_{\max})|_{t'} \leq 0 \; \forall \; t' \geq t\}$. Next, let $\varphi(u_{\max})|_T > 0$. Let $t_2 = \inf\{t : \varphi(u_{\max})|_{t'} > 0 \; \forall \; t' > t\}$. If $t_2 = 0$, the lemma follows from (11), with $t_1 = 0$. Otherwise, $\varphi(u_{\max})|_{t_2} = 0$. The lemma now follows arguing as in the previous case for $[0, t_2]$ rather than $[0, T]$, and with $t_1 = \inf\{t \leq t_2 : \varphi(u_{\max})|_{t'} \leq 0 \; \forall \; t' \in [t, t_2]\}$. ∎

Thus, the malware's activity can be divided into (at most) three distinct phases: an initial *blitz*, an intermediate *stealth* and a final *slaughter* phase. In the blitz phase, infectives use the maximum power to spread the infection as aggressively as possible. During this period, owing to the higher initial number of susceptibles the benefit of using the maximum power for spreading the infection prevails over its harms (higher risk of detection and battery-drainage of the infectives). Subsequently, that is, after a desired number of infectives have been amassed, and the number of susceptibles diminished accordingly, the infectives operate in the stealth mode, altogether ceasing the spreading effort, but instead furtively performing other malicious activities such as eavesdropping, analyzing and altering the sensed data, sabotaging routes, *etc.* The spreading effort is eschewed during this period as it merely results in easier detection and early depletion of the infective nodes' batteries rather than substantially enhancing the infection level owing to the depletion of the susceptibles in the earlier phase. Finally, the media access activities are resumed with the maximum power in the *slaughter* phase, but this time the primary goal is to kill the infectives by depleting their batteries. If however the malware does not gain from enhancing the final tally of the infective and dead nodes, i.e., $K_I = K_D = 0$, then the final slaughter phase is eliminated.

Remark 1. *The simplicity of the optimum attack strategies is conducive to their implementation using resource constrained devices. Before the attack is launched, the attacker estimates the network parameters (e.g., $\beta, \rho, Q(\cdot), B(\cdot)$), the damage coefficients ($\kappa_I, K_I, \kappa_D, K_D$) and the initial fraction of infectives I_0 before the immunization and healing would start. Using the above, it computes the jump points t_1, t_2 by solving a system of differential equations, as described in the last*

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

paragraph of Section III. Note that existing efficient numerical algorithms [36] can solve differential equations very fast, and the computation time is constant in that it does not depend on the number of nodes. The jump points are subsequently incorporated in the code of the malware. The infected devices can execute the attack strategies without any further global coordination or information exchange.

Theorem 2. *For concave Q, B, if $\kappa_D \geq \gamma\kappa_I$ and $K_D \geq \gamma K_I$, where $\gamma = (1 + B(u_{\max})/\rho u_{\max})$, the optimal u is $u_{\max}$ throughout $[0, T]$.*

Proof: Using the conditions in the theorem, it follows from (16) and (17) that $\dot{\varphi} < 0$ at any t at which u is continuous and $\varphi(u_{\max})|_T > 0$. This is because $I, S > 0$ (from lemma 1) and $\beta, \kappa_I > 0$. Since u and $\varphi(u_{\max})$ are respectively piecewise continuous and continuous functions of time, $\varphi(u_{\max}) > 0$ at all t. The theorem follows from (11). ■

When $K_D \gg K_I$ and $\kappa_D \gg \kappa_I$, the malware gains significantly more from dead nodes than from infectives. Nevertheless, choosing $u = u_{\max}$ facilitates detection of the malware leading to faster immunization of the susceptibles and depletes infectives' batteries faster. Both the above may slow down the spread of the infection and thereby reduce the number of dead nodes. The optimality of this extreme choice is therefore somewhat surprising.

Remark 2. *So far, we assumed that $Q(0) = B(0) = 0$. This is the case when detection based on media access activity of the infectives is crucial in the countermeasures. Using similar analysis, we can generalize theorem 1 to allow for $Q(0) > 0$, i.e., when even without any media access activity of the malware, susceptibles are immunized. Theorem 2 can also be generalized to the case in which $Q(0) > 0$ and $B(u) =$ constant $\leq Q(0)$, i.e., the healing is not affected by the media access activity of the malware. The latter assumption ($B \leq Q(0)$) usually holds in practice as fetching more complex, and frequently larger, security patches required for healing incurs larger delays.*

V. Numerical Computations

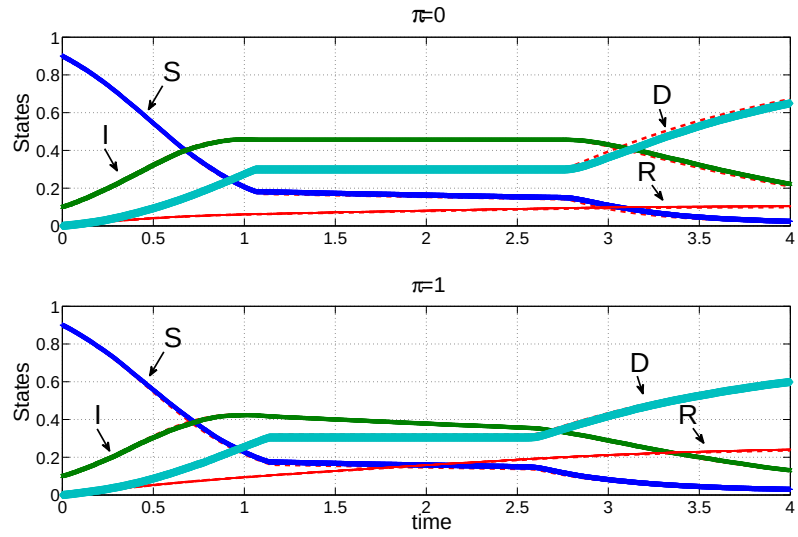
Epidemic models have been validated for mobile wireless networks through experiments as well as network simulations (see e.g. [26], [27]). Nevertheless, we start with by independently validating these models using simulations for a mobile wireless network under two different classes of contact processes: (i) exponential (ii) truncated power-law. The inter-contact times between each pair of nodes have been shown to be exponentially distributed under mobility models such as random waypoint and random direction [30]. On the other hand, the inter-contact times have truncated power-law distributions under the mobility pattern reported in [37] based on measurements on human mobility during INFOCOM 2005. Note that each pair is equally likely to contact in the former, as assumed in Section II-A (this assumption is referred to as homogeneous mixing in the sequel). Power law distributions however arise from mobility patterns under which a pair of nodes that has been in contact in the recent past is more likely to be in contact at present as compared to a pair that has been in contact long ago: the mixing is not therefore homogeneous. The attacker's optimal control function $u(\cdot)$ is calculated using the optimal control framework proposed in the paper[10], and with $T = 4$ hours, $\beta = 4.46, \rho = 0.8920, Q(u) = 0.1115, B(u) = 0.115\pi, \pi \in \{0, 1\}, \kappa_I = 40, K_D = 50, \kappa_D = 0, K_I = 0$. We consider $Q(u), B(u)$ to be constants for simplicity. The value of $\beta = 4.46$ is selected to match the expected value of the inter-contact times reported in [37]. We focus on the two extreme values of $\pi : \pi \in \{0, 1\}$. Note that if $\pi = 0$ security patches can only immunize the susceptibles, but if $\pi = 1$ they heal the infectives as well. Under the simulated contact processes, the damage is obtained by integrating $\kappa_I I(t)$ between 0 and T and adding $K_D D(T)$ to the output of the integration, where $I(t), D(t)$ are the state processes observed in the simulations and $u(t)$ is the optimal control function calculated above.

We first describe the results for the exponential contact process with N nodes. As explained in Section II-A, each pair of infective-susceptible nodes contact as per an exponential process with rate $\hat{\beta}$, where referring to (1), $\hat{\beta} = \beta/N$. Note that homogeneous mixing holds for exponential contact processes, and as discussed in Section II-A, results in [35] predict that as $N \to \infty$, the sample paths under exponential contact process will coincide with the solutions of the epidemiological differential equations ((2)). However, fig. 2(a) reveals that even for a finite N (e.g., $N = 500$) the simulated state fractions $(S(t), I(t), R(t), D(t))$, averaged over 100 runs, closely match the values predicted by the epidemic model. Also, fig. 2(b) shows that the average damages obtained over 100 simulation runs closely match those predicted by the epidemic model for different values of I_0, and the standard deviation decreases with increase in N.

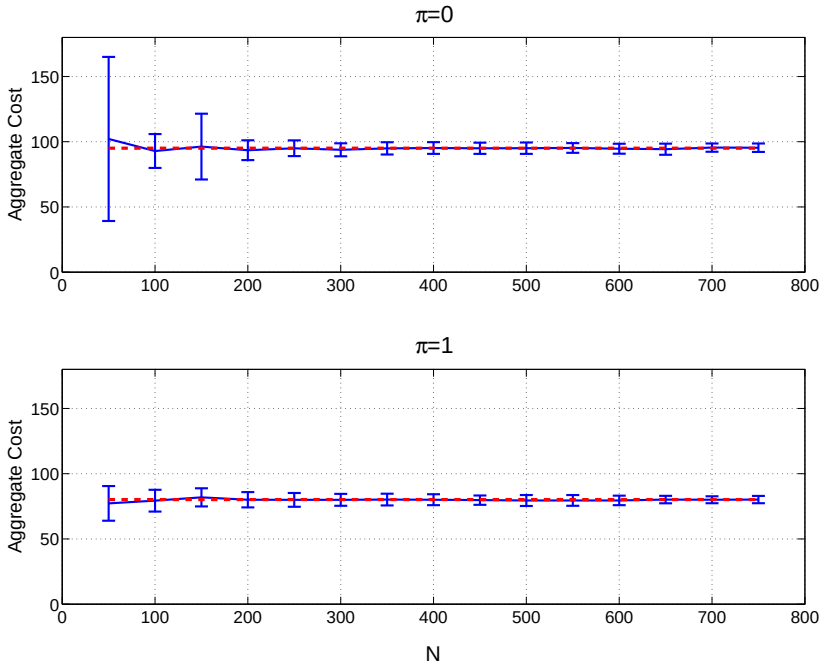
We next describe the results for the truncated power-law contact process (with parameter $\alpha = 0.4$ and truncated between 2 minutes and 24 hours) in a network with $N = 41$ reported in [37] (based on the measurements on human mobility during INFOCOM 2005) that does not satisfy the homogeneous mixing assumption. The epidemiological differential equations use $\beta = 4.46$ so that $1/\beta$ equals the expected value of the inter-contact times between any pair of nodes under the truncated power-law distribution. As fig. 3 shows, the aggregate damage, averaged over 100 runs, follows similar trends as under the epidemic representations, despite the mixing not being homogeneous and N being small.

We next investigate, using the epidemiological differential equations, the nature of the optimal dynamic attack policies and the damage they inflict for different values of network and attack parameters. We also compare the efficacy of the optimal dynamic and static controls. In a static policy, in contrast to a dynamic policy, the value of $u(t)$ is fixed throughout the period of the attack. The optimal static policy is computed by selecting the above fixed value as the one that maximizes the damage among choices in the interval $[0, 1]$. We use $\rho = 0.0892$ and the damage function in (4) with $\kappa_I = 10$, $\kappa_D = 0$, $K_I = 0$ $K_D = 50$ and $T = 40$. We consider concave

[10]We use a commercial software PROPT® launched by Tomlab Optimization Inc, (http://tomopt.com/tomlab/ for MATLAB®) for this purpose.



(a) Comparison of the simulated and calculated state trajectories



(b) Comparison of the simulated and calculated damages

Fig. 2. The top two figures compare the simulated (averaged over 100 runs) and the calculated (from the epidemic model) state trajectories for a network of $N = 500$ nodes, and the bottom two figures compare the simulated and calculated damages for different values of N. The inter-contact times are exponentially distributed. In all the figures the dashed and the solid lines respectively represent the calculated values and the simulation results. The error-bars represent the standard deviations. The dashed and solid lines mostly overlap, and the deviations diminish as N increases.

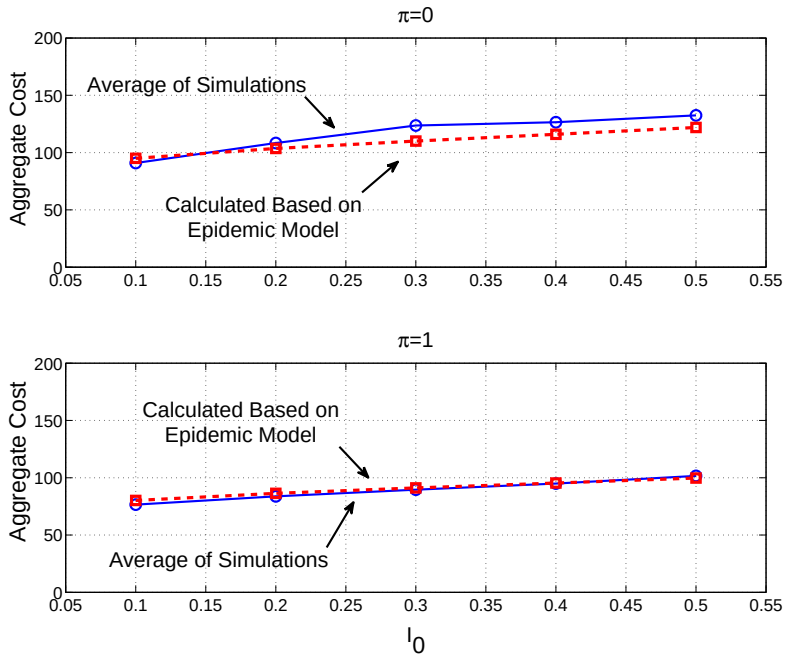


Fig. 3. Comparison of the simulated (averaged over 100 runs) damages and calculated (from the epidemic model) damages under power-law distributed inter-contact times for different value of I_0.

Q, B, i.e., $Q(u) = 0.0446 + 0.0223u$ and $B(u) = 0.0446\pi + 0.0223u$, with $\pi \in \{0, 1\}$, except for fig. 5(a) and 5(b) where Q, B are strictly convex: $Q(u) = 0.0446 + 0.0223u^{3/2}$ and $B(u) = 0.0446\pi + 0.0223u^{3/2}$.

In fig. 4(a) and 4(b), we have depicted both the optimal controls and the fraction of infectives as functions of time for different values of β. In figures 4(c) and 4(d), we have depicted the above for different values of I_0. Note that for $\pi = 1$, unlike for $\pi = 0$, the level of infection drops during the interval of $u = 0$, as $B(0) > 0$ in the former case. Also, for both $\pi \in \{0, 1\}$, the evolution of the level of infection indicate that the initial $u = u_{\max}$ phase is primarily aimed at the spread of the malware and the final $u = u_{\max}$ phase chiefly increases the final tally of the dead. Fig. 4(c) and 4(d) reveal that the initial phase is shorter for higher I_0, however, the final killing phase is less affected by varying I_0. The optimum control have two jumps in all the above, even for $\pi = 1$ and $B(\cdot) \neq$ constant. Recall that the structure of the optimal control in the latter case, as also when B, Q are strictly convex, is not predicted by any of our theorems and their generalizations, namely Remark 2. As fig. 5(a) and 5(b) reveal, the optimal controls for strictly convex B and Q, are similar to those for concave Q and B (fig. 4(a) and 4(b)) except that the transitions between different phases are continuous rather than abrupt.

Fig. 6 and Fig. 7 show that the optimal dynamic attack policy yields higher damages than the optimal static choice of u. The differences are significant for $\pi = 0$.

We have so far assumed that the malware computed the optimum attack strategies assuming full knowledge of the network parameters. However, an attacker may only have a rough estimate of the values of the parameters. Here, we investigate the impact of this inaccuracy on the efficacy of the attack. First, we derive the optimal dynamic and static controls assuming certain values for network parameters. Then we apply the same (dynamic and static, resp.) policies to a network in which the real value of one parameter (e.g., β) is different from the assumed value. Then we plot the amount of reduction in the total damage due to applying these sub-optimal policies as a function of the assumed (i.e., estimated) value of the parameter in question. The reduction is the difference between the damages inflicted by the sub-optimal policy (the dynamic and static optimal control calculated based on the inaccurate estimate of the parameter under consideration) and the optimal (dynamic) policy for the accurate value of that parameter. As fig. 8(a) shows, the damage reduction due to inaccurate estimation of β is insignificant for the dynamic policy. Also, the dynamic policy calculated based on the inaccurate estimate inflicts significantly higher damages than the static policy calculated using the same estimate - thus the dynamic policy retains its advantage over the static even in presence of estimation errors. Similar calculations for varying Q and B suggest the same behavior (figures 8(b) and 8(c) respectively). Optimal dynamic policies are therefore robust to errors in the estimation of the parameters of the network - yet another negative result from the defence point of view.

VI. Conclusion

We showed that attackers can inflict the maximum possible damage by executing simple dynamic media access strategies. These dynamic strategies are robust to the inaccurate estimation of the network parameters and inflict higher damages than the best static policies. The attackers are therefore likely to prefer dynamic choices, and hence countermeasures should be designed to adequately defend against them.

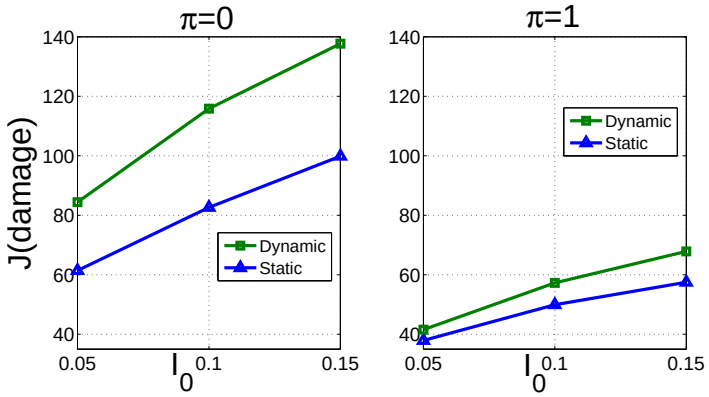


Fig. 7. Comparison of the damages for optimal dynamic and static policies for different I_0, π. Here $\beta = 0.446$.

The deterministic epidemic models considered in the paper are guaranteed to accurately model the spread of the malware only when the network has a large number of nodes and the nodes mix homogeneously. Most current wireless networks have a large number of nodes. Homogeneous mixing does not however hold in some networks: a node may only be in contact with a proper subset of nodes, e.g., when the nodes are moving slowly or moving in clusters, and the locality of infection plays a significant role in such networks since the infection may spread based on the contact list of the infectives. Designing the maximum damage attacks when either of these assumptions is relaxed remains open.

We have so far considered attacks with only one kind of malware and also that patching renders a node immune. Karyotis *et. al.* [38] have analyzed attacks where different kinds of malwares are seeking to simultaneously infect the nodes, and the patching against one kind of malware does not provide immunity against others - nodes may therefore return to susceptible states after recovery. They have however considered only static choice of malwares' parameters and only two networks states: susceptible and infected. Generalization of the framework proposed in the paper so as to characterize the maximum damage attacks under dynamic optimal control of the malwares' parameters in presence of multiple malwares and multiple network states (susceptible, infected, recovered, dead) constitutes an interesting direction for future research.

An interesting direction for future research is to develop attack strategies that are provably robust to errors in estimation of the parameters of the epidemiological differential equation $(\beta, \rho, I_0, B(\cdot), Q(\cdot))$, e.g., a control function that minimizes the maximum damage over a range of values of the parameters and certain classes of functions $B(\cdot), Q(\cdot)$. Formulating stochastic optimal control problems that consider the above parameters as random variables and lend to the maximum damage attack strategies that seamlessly adapt to their dynamic fluctuations also remain open.

We have so far evaluated the efficacy of the attack through simulations and numerical computations; evaluation through implementation in a sensor network testbed in presence of a variety of existing defense schemes remains open.

REFERENCES

[1] D. Estrin, D. Culler, K. Pister, and G. Sukhatme, "Connecting the physical world with pervasive networks," *IEEE pervasive computing*, vol. 1, no. 1, pp. 59–69, 2002.

[2] 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.

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

[4] 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.

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

[6] 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, (San Francisco), April 2003.

[7] 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, 2002.

[8] 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.

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

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

[11] V. Karyotis, S. Papavassiliou, M. Grammatikou, and B. Maglaris, "On the characterization and evaluation of mobile attack strategies in wireless ad hoc networks," in *11th IEEE Symposium on Computers and Communications, 2006. ISCC'06. Proceedings*, pp. 29–34, 2006.

[12] V. Karyotis and S. Papavassiliou, "On the Malware Spreading over Non-Propagative Wireless Ad Hoc Networks: The Attacker's Perspective," in *Proceedings of the 3-rd ACM International Workshop on QoS and Security for Wireless and Mobile Networks*, (Chania, Crete, Greece), ACM New York, NY, USA, October 2007.

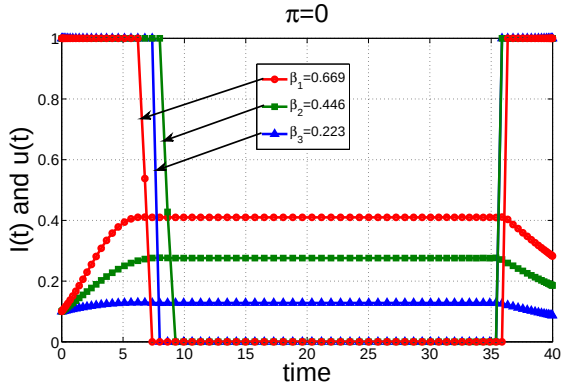
[13] R. Racic, D. Ma, and H. Chen, "Exploiting mms vulnerabilities to stealthily exhaust mobile phone's battery," *IEEE SecureComm*, 2006.

[14] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*, pp. 356–364, 2005.

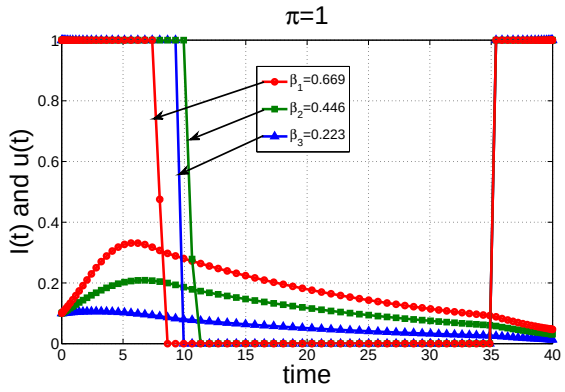
[15] H. Kim, J. Smith, and K. Shin, "Detecting energy-greedy anomalies and mobile malware variants," in *Proceeding of the 6th international conference on Mobile systems, applications, and services*, pp. 239–252, ACM, 2008.

[16] G. Jacoby and N. Davis, "Battery-based intrusion detection," in *IEEE Global Telecommunications Conference, 2004. GLOBECOM'04*, vol. 4, (Dallas, TX), November 2004.

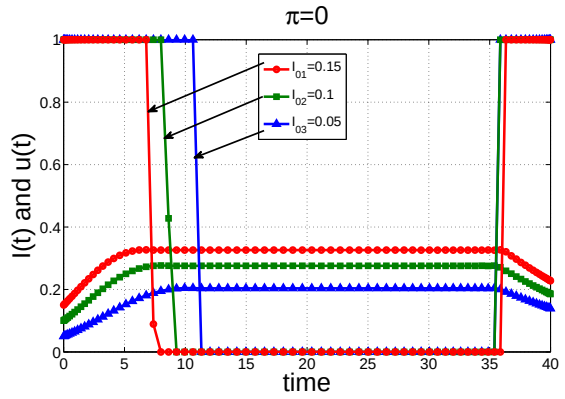
[17] T. Buennemeyer, M. Gora, R. Marchany, and J. Tront, "Battery exhaustion attack detection with small handheld mobile computers," in *IEEE International Conference on Portable Information Devices, 2007. PORTABLE07*, pp. 1–5, 2007.



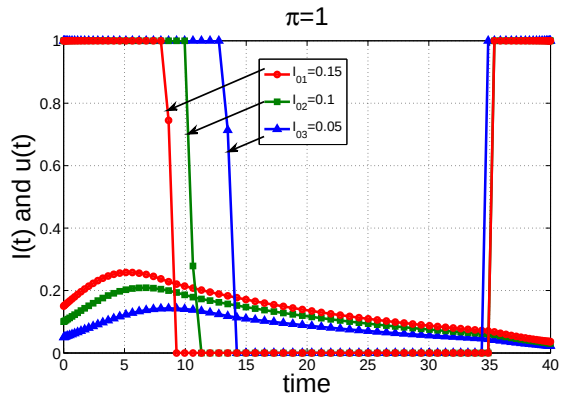
(a)



(b)

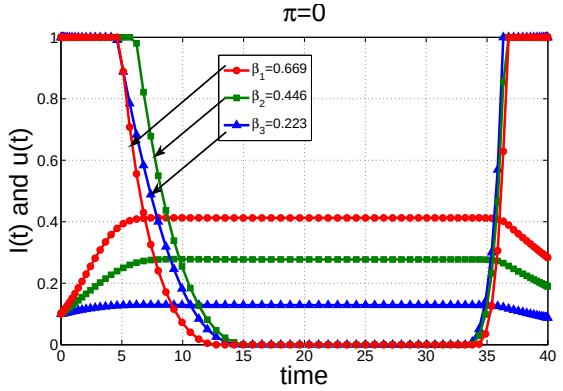


(c)

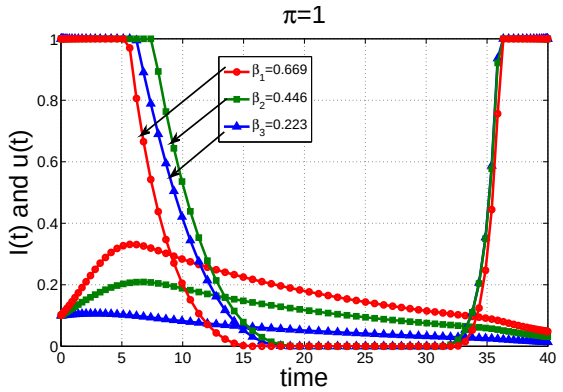


(d)

Fig. 4. Optimal controls and the corresponding levels of infection for different β, I_0, π. In figs (a) and (b), $I_0 = 0.1$, and in figs (b), (c), $\beta = 0.446$. In each, the plots that are always below 0.4 represent $I(\cdot)$. In figs (a), (b) ((c), (d), resp.) the higher infection levels are for the larger β's (I_0's, resp.).



(a) $\pi = 0$



(b) $\pi = 1$

Fig. 5. Optimal controls and the corresponding levels of infection for different β, π for strictly convex Q, B. Here, $I_0 = 0.1$. The plots that are always below 0.4 represent $I(\cdot)$. The higher infection levels are for the larger β's.

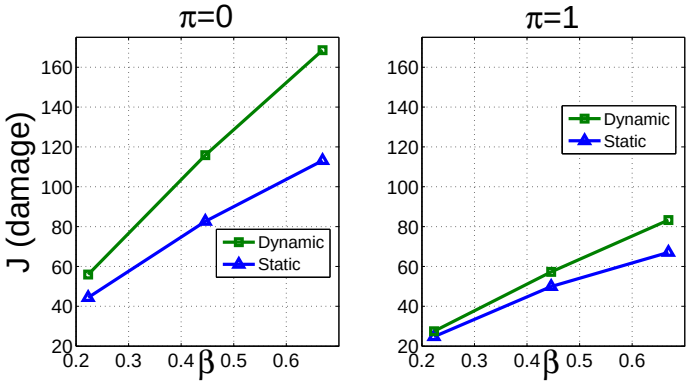


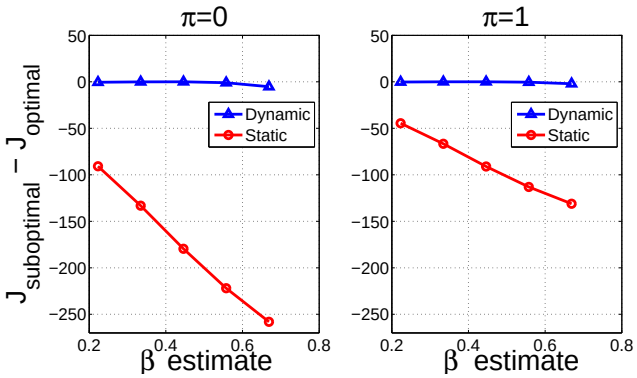
Fig. 6. Comparison of the damages for optimal dynamic and static policies for different β, π. Here $I_0 = 0.1$.

[18] 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.

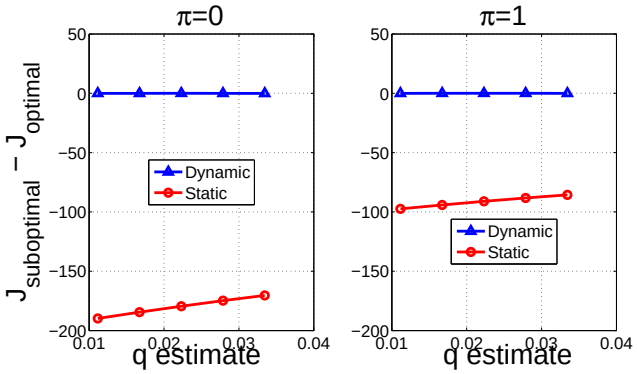
[19] V. Karyotis and S. Papavassiliou, "Risk-based attack strategies for mobile ad hoc networks under probabilistic attack modeling framework," *Computer Networks*, vol. 51, no. 9, pp. 2397–2410, 2007.

[20] 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.

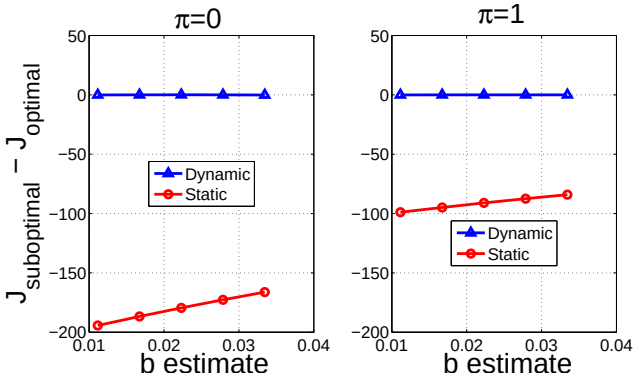
[21] M. Khouzani, E. Altman, and S. Sarkar, "Optimal Quarantining of Wireless Malware Through Power Control," in *Proceedings of the Fourth Symposium on Information Theory and Applications*, University of California at San Diego, 2009. Accepted for publication at IEEE



(a) Reduction in damage due to incorrect estimation of β



(b) Reduction in damage due to incorrect estimation of q



(c) Reduction in damage due to incorrect estimation of b

Fig. 8. The real values of the parameters are $I_0 = 0.1$, $\beta = 0.446$, $Q(u) = 0.0446 + qu$, $B(u) = 0.0446\pi + bu$, $q = b = 0.0223$.

Transaction on Automatic Controls.

[22] M. Khouzani, S. Sarkar, and E. Altman, "Maximum Damage Malware Attack in Mobile Wireless Networks," in *Proceedings of Infocom*, (San Diego), March 2010.

[23] M. Khouzani, S. Sarkar, and E. Altman, "Dispatch then Stop: Optimal Dissemination of Security Patches in Mobile Wireless Networks," in *Proceedings 49th IEEE CDC*, (Atlanta, GA), December 2010.

[24] M. H. R. Khouzani, S. Sarkar, and E. Altman, "Optimal control of epidemic evolution," in *Proceedings of Infocom*, (Shanghai, China), April 2011.

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

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

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

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

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

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

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

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

[37] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot, "Pocket switched networks and human mobility in conference environments," in *2005 ACM SIGCOMM workshop on Delay-tolerant networking*, p. 251, ACM, 2005.

[38] V. Karyotis, M. Grammatikou, and S. Papavassiliou, "On the Asymptotic Behavior of Malware-Propagative Mobile Ad Hoc Networks," in *Proceedings of the the fourth IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, (Pisa, Italy), IEEE, Piscataway, NJ, USA, October 2007.

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.

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.