Physica A 470 (2017) 249–260

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Dynamic malware containment under an epidemic model with alert

Tianrui Zhang [a], Lu-Xing Yang [b], Xiaofan Yang [a,*], Yingbo Wu [a], Yuan Yan Tang [c]

[a] College of Software Engineering, Chongqing University, Chongqing, 400044, China
[b] Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Delft, GA 2600, The Netherlands
[c] Department of Computer and Information Science, The University of Macau, Macau

HIGHLIGHTS

- An optimal control problem based on an epidemic model with alert is formulated.
- The optimality system for the optimal control problem is derived.
- The structure of an optimal control is characterized under some conditions.
- The optimal control can be improved by adjusting bounds on admissible controls.

ARTICLE INFO

Article history:
Received 29 September 2016
Received in revised form 28 November 2016
Available online 10 December 2016

Keywords:
Malware
Node-level epidemic model
Dynamic malware containment
Optimal control

ABSTRACT

Alerting at the early stage of malware invasion turns out to be an important complement to malware detection and elimination. This paper addresses the issue of how to dynamically contain the prevalence of malware at a lower cost, provided alerting is feasible. A controlled epidemic model with alert is established, and an optimal control problem based on the epidemic model is formulated. The optimality system for the optimal control problem is derived. The structure of an optimal control for the proposed optimal control problem is characterized under some conditions. Numerical examples show that the cost-efficiency of an optimal control strategy can be enhanced by adjusting the upper and lower bounds on admissible controls.

1. Introduction

Nowadays, communication networks of all forms, ranging from technological networks such as the Internet and wireless networks, to online social networks such as Facebook and Twitter, have become an indispensable part of the human society, because they have greatly enhanced the efficiency of our work and learning and improved our quality of life. As a double-edged sword, these networks also provide a shortcut for the rapid propagation of malware, posing a great threat to the human society [1]. How to effectively contain the prevalence of malware on networks has come to be an urgent task we are faced with. Detecting and eliminating electronic viruses in infected nodes using antivirus software is recognized as the main measure of suppressing malware. For the purpose of assessing the losses caused by infections as well as the effectiveness of different malware-defending strategies, a multitude of epidemic models, ranging from the coarsest population-level

* Corresponding author.
E-mail addresses: 363726657@qq.com (T. Zhang), ylx910920@gmail.com (L.-X. Yang), xfyang1964@gmail.com (X. Yang), wyb@cqu.edu.cn (Y. Wu), yytang@umac.mo (Y.Y. Tang).

http://dx.doi.org/10.1016/j.physa.2016.11.143
0378-4371/

epidemic models [2–6] and the mesoscale epidemic models [7–12] to the finest individual-level epidemic models [13–19], have been proposed.

Alerting at the early stage of malware invasion turns out to be an important complement to malware detection and elimination; before an efficacious program against a new virus is available, the dissemination of a news about the virus through networks helps reduce the possibility of susceptible nodes being infected. In real-world applications, the active alerting should be integrated with the passive treatment so that the losses caused by computer viruses are minimized at a lower cost. For the purpose of assessing the effectiveness of different alerting strategies, a number of node-level epidemic models with alert, which are known as the SAIS (Susceptible-Alert-Infected-Susceptible) models, have been suggested [20–23].

One of the central tasks in network security is to minimize the losses caused by malware within a limited budget. Towards this direction, there are two different classes of malware-containing problems: the static malware-containing problems and the dynamic malware-containing problems; for the former the state of the network is assumed to be unvaried, whereas for the latter the network state is assumed to be varying over time [24]. A static malware-containing problem can be modeled as an optimization problem subject to a limited budget [25–27]. Recently, some static malware-containing problems under SAIS models have been investigated [28,29]. Unfortunately, the static malware containment only applies to the small-timescale situations. A dynamic malware-containing problem can be modeled as an optimal control problem subject to an epidemic model [30–37]. The dynamic malware containment outperforms its static counterpart in the sense that it not only enhances the cost-efficiency but applies to the more realistic large-timescale situations. To our knowledge, the dynamic malware-containing problem with alert has yet to be resolved.

This paper addresses the dynamic malware-containing problem, provided alerting is feasible. A controlled SAIS model is established, and an optimal control problem based on the SAIS model is formulated. The optimality system for this optimal control problem is derived, and the structure of an optimal control for the optimal control problem is characterized under some conditions. Numerical examples show that the cost-efficiency of an optimal control strategy can be enhanced by adjusting the upper and lower bounds on admissible controls.

The subsequent materials of this work are organized as follows. Sections 2 and 3 formulate and study the optimal control problem, respectively. Numerical examples are provided in Section 4. Finally, Section 5 closes this work.

2. Formation of the optimal control problem

Consider a network connecting a set of N computers (nodes) labeled $1, 2, \ldots, N$. As with the traditional SAIS model, at any time every node in the network is assumed to be either *susceptible* or *alert* or *infected*, where susceptible nodes are uninfected but not alert to new malware, and alert nodes are uninfected and alert to new malware. Let $S_i(t)$, $A_i(t)$, and $I_i(t)$ denote the probability of node i being susceptible, alert, and infected at time t, respectively. The vector

$$(S_1(t), \ldots, S_N(t), A_1(t), \ldots, A_N(t), I_1(t), \ldots, I_N(t))^T$$

probabilistically captures the state of the network at time t. As $S_i(t) + A_i(t) + I_i(t) \equiv 1$, $1 \le i \le N$, the shorter vector

$$\mathbf{x}(t) = (A_1(t), \ldots, A_N(t), I_1(t), \ldots, I_N(t))^T$$

also probabilistically captures the state of the network at time t.

Now, let us impose a set of probabilistic assumptions on the state transition of a node.

- (H_1) At time t, a susceptible node i is alerted by an alert node j at a controllable rate $\alpha_{ij}(t)$, where (a) $\alpha_{ij}(t) \in L^2[0, T]$, and (b) $\underline{\alpha} \le \alpha_{ij}(t) \le \overline{\alpha}$, $0 \le t \le T$. So, at time t an susceptible node i becomes alert roughly at rate $\sum_{j=1}^{N} \alpha_{ij}(t)A_j(t)$.
- (H_2) At any time, a susceptible node i is infected by an infected node j at a constant rate $\beta_{1ij} \ge 0$. Hence, at time t a susceptible node i becomes infected roughly at rate $\sum_{j=1}^{N} \beta_{1ij}I_j(t)$.
- (H_3) At any time, an alert node i is infected by an infected node j at a constant rate $0 \le \beta_{2ij} \le \beta_{1ij}$. As a result, at time t a susceptible node i becomes infected roughly at rate $\sum_{j=1}^{N} \beta_{2ij}I_j(t)$.
- (H_4) At time t, an infected node i gets cured and hence becomes susceptible at a controllable rate $\gamma_i(t)$, where (a) $\gamma_i(t) \in L^2[0, T]$, and (b) $\underline{\gamma} \le \gamma_i(t) \le \overline{\gamma}$, $0 \le t \le T$.
- (H_5) At any time, the loss incurred by an infected node i is $c_i > 0$.
- (H_6) At time t, the cost for alerting a susceptible node i by node j is $g(\alpha_{ij}(t))$, where function g is differentiable.
- (H_7) At time t, the cost for healing an infected node i is $h(\gamma_i(t))$, where function h is differentiable.

Fig. 1 shows assumptions (H_1)–(H_4) schematically.

Let Δt be a very small time interval. Assumptions (H_1)–(H_4) imply that the probabilities of state transition of node i satisfies the following relations.

$$\Pr(i \text{ is alerted at time } t + \Delta t \mid i \text{ is susceptible at time } t) = \Delta t \sum_{j=1}^{N} \alpha_{ij}(t)A_j(t) + o(\Delta t),$$