Defend against advanced persistent threats: An optimal control approach

Pengdeng Li\textsuperscript{a}, Lu-Xing Yang\textsuperscript{b}, Xiaofan Yang\textsuperscript{a*}, Qingyu Xiong\textsuperscript{a}, Junhao Wen\textsuperscript{a}, Yuan Yan Tang\textsuperscript{b}

\textsuperscript{a}School of Software Engineering, Chongqing University, Chongqing, 400044, China
\textsuperscript{b}Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Delft, GA 2600, The Netherlands
\textsuperscript{c}Department of Computer and Information Science, The University of Macau, Macau

Abstract

The new cyber attack pattern of advanced persistent threats (APTs) poses a serious threat to cyberspace. This paper addresses the issue of defending against APTs in a cost-effective way. First, the APT-based cyber attack-defense processes are modeled as a type of differential dynamical systems. Then, the cyber defense problem is modeled as an optimal control problem. The optimal control problem is shown to have an optimal control, and the optimality system for the problem is presented. Therefore, a cost-effective cyber defense strategy can be figured out by solving the optimality system. Finally, the influences of some factors, including the bounds on the admissible controls and the network topology, on the cost-effective defense strategies are examined. To our knowledge, this is the first time the APT-based cyber defense problem is treated this way.

Keywords: cybersecurity, advanced persistent threat, cyber attack-defense, dynamical system, optimal control, optimality system

2000 MSC: 34D05, 34D20, 34D23, 68M99

1. Introduction

Cyberspace has become an integral part of our society. All the time, a great deal of data are collected, processed and stored on computers and are transmitted across networks to other computers \cite{1,2}. However, cyberspace is vulnerable to a wide range of cyber threats. Sophisticated cyber perpetrators exploit vulnerabilities to steal what they want or to disrupt essential cyber services. In light of the consequence of cyber attacks, strengthening the security and resilience of cyber networks has come to be an important mission of the cybersecurity community \cite{3,4,5}.

Advanced persistent threats (APTs) are a new type of cyber attacks. With a clear goal, an APT attack is highly targeted, well-organized, well-resourced, covert and persistent \cite{6,7,8}. APTs pose a severe threat to cyberspace, because they invalidate conventional cyber defense mechanisms. In recent years, the number of APTs has been increasing rapidly \cite{9}. Therefore, it is imperative to develop cost-effective cyber defense strategies against APTs.

\textsuperscript{*}Corresponding author

Email addresses: 1414797521@qq.com (Pengdeng Li), ylx910920@gmail.com (Lu-Xing Yang), xfyang1964@gmail.com (Xiaofan Yang), xiong05@equ.edu.cn (Qingyu Xiong), jhwen@cqu.edu.cn (Junhao Wen), yytang@umac.mo (Yuan Yan Tang)

Preprint submitted to Elsevier September 12, 2017
In order to defend against APT attacks in a cost-effective way, the APT-based cyber attack-defense processes must be modeled properly. The individual-level dynamical modeling technique, which has been successfully applied to areas such as the epidemic spreading [10–14], the malware spreading [15–21], and the rumor spreading [22, 23], is especially suited to the modeling of APT-based cyber attack-defense processes, because the topological structure of the cyber network can be accommodated [24]. Towards this direction, a number of cyber attack-defense models have been proposed [25–28]. On the other hand, the optimal control approach [29, 30] is often employed to minimize an objective functional at a lower cost. In particular, this method has recently been successfully applied to the cost-effective containment of malware [31–33]. In our opinion, this technique also applies to the APT-based cyber defense.

This paper addresses the issue of defending against APTs in a cost-effective way. First, the APT-based cyber attack-defense processes are modeled as a type of differential dynamical systems. Then, the cyber defense problem is modeled as an optimal control problem. The optimal control problem is shown to have an optimal control, and the optimality system for the problem is formulated. Therefore, a cost-effective cyber defense strategy can be figured out by solving the optimality system. Finally, the influences of some factors, including the bounds on the admissible controls and the network topology, on the cost-effective defense strategies are examined. To our knowledge, this is the first time the APT-based cyber defense problem is treated this way.

The remaining materials are organized in this fashion. Section 2 models the APT-based cyber attack-defense processes as dynamical systems. Section 3 models the APT-based cyber defense problem as an optimal control problem, and Section 4 theoretically studies the optimal control problem. The influences of different factors on the cost-effective defense strategy are examined in Section 5. Finally, Section 6 closes this work.

2. The modeling of the APT-based cyber attack/defense processes

The goal of this section is to model the APT-based cyber attack-defense processes as dynamical systems. For the fundamental knowledge on differential dynamical systems, see Ref. [34].

Consider a cyber network $G = (V, E)$ interconnecting a set of $N$ hosts labeled $1, 2, \cdots, N$, where $(i, j) \in E$ if and only if host $i$ can communicate directly with host $j$. Let $A = (a_{ij})_{N \times N}$ denote the adjacency matrix for the network. Suppose there is an attacker to the network and a defender for the network. Suppose that at any time every host in the network is either secure, i.e. under the defender’s control, or compromised, i.e., under the attacker’s control. Let $S_i(t)$ and $C_i(t)$ denote the probability of host $i$ being secure and compromised at time $t$, respectively. As $S_i(t) + C_i(t) \equiv 1$, the vector

$$C(t) = (C_1(t), \cdots, C_N(t))^T$$

represents the expected state of the cyber network at time $t$. 

2
An APT to the cyber network is twofold: external attack and internal infection. The former is conducted by the external attacker, with the intent of compromising the secure hosts in the network. The attack strength to secure host $i$ is $a_i$. We refer to the vector $a = (a_1, \cdots, a_N)$ as a attack strategy. The latter is led by the compromised hosts in the network, with the intent of compromising the secure hosts in the network. The expected infection strength to secure host $i$ at time $t$ is $\beta \sum_{j=1}^{N} a_{ij} C_j(t)$, where $\beta > 0$ is referred to as the infection force.

A defense of the cyber network is also twofold: prevention and recovery. The former is dedicated to preventing the secure nodes in the network from being compromised. The prevention strength of secure node $i$ at time $t$ is $x_i(t)$. We refer to the vector-valued function $x(t) = (x_1(t), \cdots, x_N(t))$ as a prevention strategy. The latter is devoted to recovering the compromised nodes in the network. The recovery strength of compromised host $i$ at time $t$ is $y_i(t)$. We refer to the vector-valued function $y(t) = (y_1(t), \cdots, y_N(t))$ as a recovery strategy. Furthermore, we refer to the vector-valued function

$$u(t) = (x(t), y(t)) = (x_1(t), \cdots, x_N(t), y_1(t), \cdots, y_N(t))$$

as a defense strategy.

Next, let us impose a set of hypotheses as follows.

(H$_1$) Due to external attack, at time $t$ secure node $i$ gets compromised at rate $a_i \frac{x_i}{x(t)}$. This hypothesis is rational, because the rate is proportional to the attack strength and is inversely proportional to the prevention strength.

(H$_2$) Due to internal infection, at time $t$ secure node $i$ gets compromised at the expected rate $\beta \sum_{j=1}^{N} a_{ij} C_j(t) \frac{x_i}{x(t)}$. This assumption is rational, because the expected rate is proportional to the expected infection strength and is inversely proportional to the prevention strength.

(H$_3$) Due to recovery, at time $t$ compromised node $i$ becomes secure at rate $y_i(t)$. This assumption is rational, because the rate is proportional to the recovery strength.

Based on the above hypotheses, an APT-based cyber attack-defense process can be modeled as the following dynamical system.

$$\frac{dC_i(t)}{dt} = \frac{1}{x_i(t)} \left[ a_i + \beta \sum_{j=1}^{N} a_{ij} C_j(t) \right] [1 - C_i(t)] - y_i(t) C_i(t), \quad t \geq 0, i = 1, \cdots, N. \quad (1)$$

We refer to the model as the individual-level secure-compromised-secure (SCS) model. The diagram of state transitions of a host under this model is shown in Fig. 1.
The individual-level SCS model can be rewritten in matrix notation as
\[
\frac{dC(t)}{dt} = F(C(t), u(t)), \quad t \geq 0.
\] (2)

3. The modeling of the cyber defense problem

The defender’s goal is to find a cost-effective cyber defense strategy, i.e., a defense strategy that minimizes the loss caused by the APT at a lower cost. The goal of this section is to model the cyber defense problem.

Suppose the cyber defense starts at time \( t = 0 \) and terminates at time \( t = T \), and the admissible set of the cyber defense strategies is
\[
\mathcal{U} = \left\{ u \in \left(L^2[0, T]\right)^N \mid 0 < x \leq x_i(t) \leq \bar{x}, 0 < y \leq y_i(t) \leq \bar{y}, 0 \leq t \leq T, 1 \leq i \leq N \right\}. \tag{3}
\]

Define the influence of host \( i \) in the cyber network as its degree in the network.
\[
w_i = \sum_{j=1}^{N} a_{ij}. \tag{4}
\]

Intuitively, the more influential a host, the more serious the consequence of compromising it will be [35, 36]. Hence, the expected loss caused by the APT in the time interval \([0, T]\) is estimated as
\[
\text{Loss}(u) = \sum_{i=1}^{N} \int_{0}^{T} w_i C_i(t) dt. \tag{5}
\]

On the other hand, the costs for the prevention strategy \( x \) and the recovery strategy \( y \) in the time interval \([0, T]\) are estimated as
\[
\text{Cost}(x) = \sum_{i=1}^{N} \int_{0}^{T} x_i(t) dt \tag{6}
\]
and
\[
\text{Cost}(y) = \sum_{i=1}^{N} \int_{0}^{T} y_i(t) dt, \tag{7}
\]
respectively. So, the cost for the defense strategy \( u \) in the time interval \([0, T]\) is estimated as
\[
\text{Cost}(u) = \sum_{i=1}^{N} \int_{0}^{T} [x_i(t) + y_i(t)] dt. \tag{8}
\]
Therefore, the expected cost effectiveness of the defense strategy $u$ in the time interval $[0, T]$ can be estimated as

$$J(u) = \text{Loss}(u) + \text{Cost}(u) = \int_0^T L(C(t), u(t)) \, dt,$$

where

$$L(C(t), u(t)) = \sum_{i=1}^N \left[ w_i C_i(t) + x_i(t) + y_i(t) \right].$$

(10)

On this basis, the cyber defense problem can be modeled as the following optimal control problem.

(P) Minimize $u \in U J(u) = \int_0^T L(C(t), u(t)) \, dt,$

subject to $\frac{dC(t)}{dt} = F(C(t), u(t)), \quad 0 \leq t \leq T,$

$C(0) = C_0.$

And an optimal control for the problem (P) represents a cost-effective defense strategy.

4. A theoretical analysis of the optimal control problem

This section is devoted to theoretically studying the optimal control problem (P). For fundamental knowledge on optimal control theory, see Refs. [29, 30].

4.1. The existence of an optimal control

As an optimal control for the problem (P) represents a cost-effective defense strategy, it is critical to show that the problem (P) has an optimal control. The following lemma comes from Ref. [30].

Lemma 1. Problem (P) has an optimal control if the following five conditions hold simultaneously.

(C1) $U$ is closed and convex.

(C2) There is $u \in U$ such that the adjunctive dynamical system is solvable.

(C3) $F(C, u)$ is bounded by a linear function in $C$.

(C4) $L(C, u)$ is convex on $U$.

(C5) $L(C, u) \geq c_1 ||u|| + c_2$ for some vector norm $|| \cdot ||$, $\rho > 1, c_1 > 0$ and $c_2$.

Next, let us show that the five conditions in Lemma 1 indeed hold.

Lemma 2. The admissible set $U$ is closed.

Proof: Let $u = (x_1, \cdots, x_N, y_1, \cdots, y_N)^T$ be a limit point of $U$, $u^{(n)} = \left( x_1^{(n)}, \cdots, x_N^{(n)}, y_1^{(n)}, \cdots, y_N^{(n)} \right)^T$, $n = 1, 2, \cdots$, be a sequence of points in $U$ that approaches $u$. As $\left( L^2[0, T] \right)^{2N}$ is complete, we have $u \in \left( L^2[0, T] \right)^{2N}$. Hence, the claim follows from the observation that

$$\bar{x} \leq x_i(t) = \lim_{n \to \infty} x_i^{(n)}(t) \leq \bar{x}, \quad \bar{y} \leq y_i(t) = \lim_{n \to \infty} y_i^{(n)}(t) \leq \bar{y}, \quad 0 \leq t \leq T, 1 \leq i \leq N.$$
Lemma 3. The admissible set $\mathcal{U}$ is convex.

Proof: Let $u^{(1)} = (x_1^{(1)}, \ldots, x_N^{(1)}, y_1^{(1)}, \ldots, y_N^{(1)})^T$, $u^{(2)} = (x_1^{(2)}, \ldots, x_N^{(2)}, y_1^{(2)}, \ldots, y_N^{(2)})^T \in \mathcal{U}$, $0 < \eta < 1$. As $(L^2[0, T])^{2N}$ is a real vector space, we get $(1 - \eta)u^{(1)}(t) + \eta u^{(2)}(t) \in (L^2[0, T])^{2N}$. So, the claim follows from the observation that

$$\bar{x} \leq (1 - \eta)x_1^{(1)}(t) + \eta x_2^{(1)}(t) \leq \bar{x}, \quad \bar{y} \leq (1 - \eta)y_1^{(1)}(t) + \eta y_2^{(1)}(t) \leq \bar{y}, \quad 0 \leq t \leq T, 1 \leq i \leq N.$$

Lemma 4. There is $u \in \mathcal{U}$ such that the associated adjointive dynamical system is solvable.

Proof: Consider the adjointive dynamical system

$$\frac{dC(t)}{dt} = F(C(t), \bar{u}), \quad 0 \leq t \leq T,$$

where $u(t) \equiv \bar{u} = (\bar{x}, \ldots, \bar{x}, \bar{y}, \ldots, \bar{y})^T$. As $F(C, \bar{u})$ is continuously differentiable, the claim follows from the Continuation Theorem for Differential Systems [34].

Lemma 5. $F(C, u)$ is bounded by a linear function in $C$.

Proof: The claim follows the observation that for $t \geq 0, i = 1, 2, \ldots, N,

$$\frac{1}{x_i(t)} \left[ a_i + \beta \sum_{j=1}^{N} a_j C_j(t) \right] \left[ 1 - C_i(t) \right] - y_i(t)C_i(t) \leq \frac{1}{\bar{x}} \left[ a_i + \beta \sum_{j=1}^{N} a_j C_j(t) \right] \leq \frac{1}{\bar{x}} \left[ a_i + \beta \sum_{j=1}^{N} a_j C_j(t) \right].$$

Lemma 6. $L(C, u)$ is convex on $\mathcal{U}$.

Proof: Let $u^{(1)}, u^{(2)} \in \mathcal{U}$, $0 < \eta < 1$. Then $L \left( C, (1 - \eta)u^{(1)} + \eta u^{(2)} \right) = (1 - \eta)L \left( C, u^{(1)} \right) + \eta L \left( C, u^{(2)} \right)$.

Lemma 7. $L(C, u) \geq \frac{1}{\max \{x, y\}} ||u||_2^2$.

Proof: $L(C, u) = \sum_{i=1}^{N} \left( w_i C_i + x_i + y_i \right) \geq \sum_{i=1}^{N} (x_i + y_i) \geq \sum_{i=1}^{N} \left( \frac{x_i}{\bar{x}} + \frac{y_i}{\bar{y}} \right) \geq \frac{1}{\max \{x, y\}} ||u||_2^2$.

We are ready to present the main result of this subsection.

Theorem 1. The problem (P) has an optimal control.

Proof: The claim follows from Lemmas 2-7.

This theorem guarantees that there is a cost-effective cyber defense strategy against any APT.

4.2. The optimality system

It is known that the optimality system for an optimal control problem offers a method for numerically solving the problem. This subsection is intended to present the optimality system for the problem (P). For this purpose, consider the corresponding Hamiltonian

$$H(C(t), u(t), \lambda(t)) = \sum_{i=1}^{N} \left[ w_i C_i(t) + x_i(t) + y_i(t) \right]$$

$$+ \sum_{i=1}^{N} \lambda_i(t) \left[ a_i + \beta \sum_{j=1}^{N} a_j C_j(t) \right] \left[ 1 - C_i(t) \right] - y_i(t)C_i(t) \right].$$
where \( \lambda = (\lambda_1, \cdots, \lambda_N)^T \) is the adjoint.

**Theorem 2.** Suppose \( u^* \) is an optimal control for the problem \((P)\), \( C^* \) is the solution to the adjunctive dynamical system with \( u = u^* \). Then, there exists \( x^* \) with \( \lambda^*(T) = 0 \) such that for \( 0 \leq t \leq T \), \( 1 \leq i \leq N \),

\[
\frac{d\lambda_i^*(t)}{dt} = -w_i + \gamma_i(t)\lambda_i^*(t) + \frac{\lambda_i^*(t)}{x_i^*(t)} \left[ a_i + \beta \sum_{j=1}^{N} a_jC_j(t) \right] - \beta \sum_{j=1}^{N} \frac{a_j[1 - C_j(t)]\lambda_j^*(t)}{x_j^*(t)},
\]

\[
x_i^*(t) = \max \left\{ \mathcal{A}^*_i(t) \left[ a_i + \beta \sum_{j=1}^{N} a_jC_j(t) \right] [1 - C_i(t)] \right\} \cdot x_i^* \cdot \lambda_i^*(t) C_i^*(t) < 1,
\]

\[
y_i^*(t) = \begin{cases} y_i, & \lambda_i^*(t) C_i^*(t) < 1, \\ \bar{y}, & \lambda_i^*(t) C_i^*(t) > 1. \end{cases}
\]

**Proof:** According to the Pontryagin Minimum Principle \([29]\), there exists \( \lambda^* \) such that

\[
\frac{d\lambda_i^*(t)}{dt} = -\frac{\partial H(C^*(t), u^*(t), \lambda^*(t))}{\partial C_i}, \quad 0 \leq t \leq T, \quad 1 \leq i \leq N
\]

Thus, the first \( N \) equations in the claim follow by direct calculations. As the terminal cost is unspecified and the final state is free, the transversality condition \( \lambda^*(T) = 0 \) holds. By using the optimality condition

\[
u^*(t) = \arg \min_{u \in U} H(C^*(t), u(t), \lambda^*(t)), \quad 0 \leq t \leq T.
\]

we get (a) either

\[
\frac{\partial H(C^*(t), u^*(t), \lambda^*(t))}{\partial x_i(t)} = 1 - \frac{\lambda_i^*(t)}{\left(x_i^*(t)\right)^2} \left[ a_i + \beta \sum_{j=1}^{N} a_jC_j(t) \right] [1 - C_i(t)] = 0
\]

or \( x_i^*(t) = \underline{x} \) or \( x_i^*(t) = \bar{x} \), and (b)

\[
y_i^*(t) = \arg \min_{y \in \mathbb{R}} \left( 1 - \lambda_i^*(t) C_i^*(t) \right) y_i(t) = \begin{cases} y_i, & \lambda_i^*(t) C_i^*(t) < 1, \\ \bar{y}, & \lambda_i^*(t) C_i^*(t) > 1. \end{cases}
\]

Combining the above discussions, we get the optimality system for the problem \((P)\) as follows.

\[
\frac{dC_i(t)}{dt} = \frac{1}{x_i(t)} \left[ a_i + \beta \sum_{j=1}^{N} a_jC_j(t) \right] [1 - C_i(t)] - y_i(t)C_i(t),
\]

\[
\frac{d\lambda_i(t)}{dt} = -w_i + y_i(t)\lambda_i(t) + \frac{\lambda_i(t)}{x_i(t)} \left[ a_i + \beta \sum_{j=1}^{N} a_jC_j(t) \right] - \beta \sum_{j=1}^{N} \frac{a_j[1 - C_j(t)]\lambda_j(t)}{x_j(t)},
\]

\[
x_i(t) = \max \left\{ \mathcal{A}^*_i(t) \left[ a_i + \beta \sum_{j=1}^{N} a_jC_j(t) \right] [1 - C_i(t)] \right\} \cdot x_i^* \cdot \lambda_i^*(t) C_i^*(t) < 1,
\]

\[
y_i(t) = \begin{cases} y_i, & \lambda_i(t) C_i(t) < 1, \\ \bar{y}, & \lambda_i(t) C_i(t) > 1. \end{cases}
\]
where $C(0) = C_0$, $\lambda(T) = 0, 0 \leq t \leq T, 1 \leq i \leq N$.

Applying the forward-backward Euler scheme to the optimality system, we can obtain the optimal control to the problem (P), i.e., a cost-effective cyber defense strategy.

5. A simulation-based study of the optimal control problem

This section is devoted to studying the optimal control problem (P) by solving the optimality system (11).

5.1. Numerical examples of the optimal control

Given an admissible control $u$ to the problem (P), define the overall control (OC) function as

$$OC(t) = \sum_{i=1}^{N} [x_i(t) + y_i(t)], \quad 0 \leq t \leq T,$$

the cumulative loss-cost (CLC) function as

$$CLC(t) = \sum_{i=1}^{N} \int_{0}^{t} w_i C_i(s) ds + \sum_{i=1}^{N} \int_{0}^{t} [x_i(s) + y_i(s)] ds, \quad 0 \leq t \leq T.$$ (13)

This subsection gives three exemplar optimal control for the problem (P).

Example 1. Consider the problem (P) with $T = 20, \beta = 0.001, \bar{x} = \bar{y} = 0.1, \bar{x} = \bar{y} = 0.7, a_i = 0.1, 0 \leq i \leq N,$ and a synthetic scale-free network [37] with $N = 100$ nodes as the cyber network. The initial condition is $C_i(0) = 0.1, 0 \leq i \leq N$. The optimal control for the problem is obtained by solving the optimality system (11). The OC function and the CLC function are shown in Fig. 2(a) and Fig. 2(b), respectively. For comparison purpose, we also present the OC functions and the CLC functions for a few admissible static controls in Fig. 2(a) and Fig. 2(b), respectively.

![Figure 2](image)

**Figure 2.** The OC functions and the CLC functions for the optimal control and a few static controls in Example 1.
Example 2. Consider the problem (P) with $T = 20$, $\beta = 0.001$, $x = y = 0.1$, $\bar{x} = \bar{y} = 0.7$, $a_i = 0.1$, $0 \leq i \leq N$, and a synthetic small-world network [38] with $N = 100$ nodes as the cyber network. The initial condition is $C_i(0) = 0.1$, $0 \leq i \leq N$. The optimal control for the problem is obtained by solving the optimality system (11). The OC function and the CLC function are shown in Fig. 3(a) and Fig. 3(b), respectively. For comparison purpose, we also present the OC functions and the CLC functions for a few admissible static controls in Fig. 3(a) and Fig. 3(b), respectively.

![Figure 3](image1.png)

**Figure 3.** The OC functions and the CLC functions for the optimal control and a few static controls in Example 2.

Example 3. Consider the problem (P) with $T = 20$, $\beta = 0.001$, $x = y = 0.1$, $\bar{x} = \bar{y} = 0.7$, $a_i = 0.1$, $0 \leq i \leq N$, and a realistic email network [39] as the cyber network. The initial condition is $C_i(0) = 0.1$, $0 \leq i \leq N$. The optimal control for the problem is obtained by solving the optimality system (11). The OC function and the CLC function are shown in Fig. 4(a) and Fig. 4(b), respectively. For comparison purpose, we also present the OC functions and the CLC functions for a few admissible static controls in Fig. 4(a) and Fig. 4(b), respectively.

![Figure 4](image2.png)

**Figure 4.** The OC functions and the CLC functions for the optimal control and a few static controls in Example 3.
It is concluded from the above three examples that the cost-effective cyber defense strategy corresponding to the optimal control for the problem (P) is significantly superior to the static cyber defense strategies corresponding to the static controls for the same problem in terms of the cost effectiveness. This justifies the cost-effective cyber defense strategies. Additionally, the OC function corresponding to the optimal control is decreasing rapidly.

5.2. The bounds on the admissible controls

The two upper bounds, $\overline{x}$ and $\overline{y}$, and the two lower bounds, $\underline{x}$ and $\underline{y}$, on the admissible controls have influence on the optimal control for the problem (P). The goal of this subsection is to understand the influence. Suppose $u^*$ is an optimal control for the problem (P). Let $OL^*$ denote the expected overall loss, $OC^*$ the overall cost, $OJ^*$ the sum of the two parts.

$$OL^* = \text{Loss}(u^*), \quad OC^* = \text{Cost}(u^*), \quad OJ^* = OL^* + OC^* = J(u^*).$$

(14)

Example 4. Consider the problem (P) with $T = 20$, $\beta = 0.001$, and $a_i = 0.1$, $0 \leq i \leq N$, and the scale-free network in Example 1 as the cyber network. The initial condition is $C_i(0) = 0.1, 0 \leq i \leq N$. Given $\underline{y} = 0.1$ and $\overline{y} = 0.7$, Fig. 5(a)-(c) display the influences of $\underline{x}$ and $\overline{x}$ on $OL^*$, $OC^*$ and $OJ^*$, respectively. Given $\underline{x} = 0.1$ and $\overline{x} = 0.7$, Fig. 5(d)-(f) display the influences of $\underline{y}$ and $\overline{y}$ on $OL^*$, $OC^*$ and $OJ^*$, respectively.

Example 5. Consider the problem (P) with $T = 20$, $\beta = 0.001$, and $a_i = 0.1$, $0 \leq i \leq N$, and the small-world network in Example 2 as the cyber network. The initial condition is $C_i(0) = 0.1, 0 \leq i \leq N$. Given $\underline{y} = 0.1$ and $\overline{y} = 0.7$, Fig. 6(a)-(c) display the influence of $\underline{x}$ and $\overline{x}$ on $OL^*$, $OC^*$ and $OJ^*$, respectively. Given $\underline{x} = 0.1$ and $\overline{x} = 0.7$, Fig. 6(d)-(f) display the influences of $\underline{y}$ and $\overline{y}$ on $OL^*$, $OC^*$ and $OJ^*$, respectively.

Figure 5. The influences of $\underline{x}$, $\overline{x}$, $\underline{y}$ and $\overline{y}$ on $OL^*$, $OC^*$ and $OJ^*$ in Example 4.

Figure 6. The influences of $\underline{x}$, $\overline{x}$, $\underline{y}$ and $\overline{y}$ on $OL^*$, $OC^*$ and $OJ^*$ in Example 5.
Example 6. Consider the problem (P) with $T = 20$, $\beta = 0.001$, and $a_i = 0.1$, $0 \leq i \leq N$, and the email network in Example 3 as the cyber network. The initial condition is $C_i(0) = 0.1, 0 \leq i \leq N$. Given $\underline{y} = 0.1$ and $\overline{y} = 0.7$. Fig. 7(a)-(c) display the influences of $\underline{x}$ and $\overline{x}$ on $OL^*$, $OC^*$ and $OJ^*$, respectively. Given $\underline{x} = 0.1$ and $\overline{x} = 0.7$, Fig. 7(d)-(f) display the influences of $\underline{y}$ and $\overline{y}$ on $OL^*$, $OC^*$ and $OJ^*$, respectively.
The following conclusions are drawn from the above three examples.

(a) $\mathcal{O}_\star$ goes down rapidly, and $\mathcal{O}_\star$ and $\mathcal{O}_J$ go up rapidly, with the increase of $x$ or $y$. In practice, $x$ and $y$ should be chosen so that a balance between the overall loss and the overall cost is achieved.

(b) The influences of $x$ or $y$ on $\mathcal{O}_\star$, $\mathcal{O}_\star$ and $\mathcal{O}_J$ are almost negligible.

5.3. The structure of the cyber network

This subsection addresses the influence of the structure of the network on the optimal control for the problem (P).

First, it is known that the heterogeneity of a scale-free network increases with the increase of the power-law exponent.

Example 7. Consider the problem (P) with $T = 20$, $\beta = 0.001$, $x = y = 0.1$, $\bar{x} = \bar{y} = 0.7$, $a_i = 0.1$, $0 \leq i \leq N$. The cyber network $G \in \{G_i : 1 \leq i \leq 7\}$, where $G_i$ is a scale-free network with $N = 100$ nodes and a power-law exponent of $\gamma = 2.7 + 0.1 \times i$, respectively. Figure 8(a)-(c) display the influences of the power-law exponent on $\mathcal{O}_\star$, $\mathcal{O}_\star$ and $\mathcal{O}_J$, respectively.

It is concluded that $\mathcal{O}_\star$ and $\mathcal{O}_J$ declines, and $\mathcal{O}_\star$ inclines, with the increase of the heterogeneity of the scale-free cyber network. In practice, cyber networks should be organized in a heterogeneous way.

Second, it is known that the randomness of a small-world network increases with the edge-rewiring probability.

Example 8. Consider the problem (P) with $T = 20$, $\beta = 0.001$, $x = y = 0.1$, $\bar{x} = \bar{y} = 0.7$, $a_i = 0.1$, $0 \leq i \leq N$. The cyber network $G \in \{G_i : 1 \leq i \leq 5\}$, where $G_i$ is a small-world network with $N = 100$ nodes and an edge-rewiring probability of $p = 0.1 \times i$. Figure 9(a)-(c) display the influences of the edge-rewiring probability on $\mathcal{O}_\star$, $\mathcal{O}_\star$ and $\mathcal{O}_J$, respectively.
It is concluded that $OL^*$, $OC^*$ and $OJ^*$ rise rapidly with the increase of the randomness of the small-world cyber network. This shows that a cyber network with less random connections is superior to a cyber network with more random connections in terms of the optimal APT-based cyber defense strategy. In practice, cyber networks should be organized in a less random way.

6. Concluding remarks

This paper has addressed the cost-effective defense of cyber networks under APTs. The cyber defense problem has been modeled as an optimal control problem, which has been studied theoretically. The influences of some factors on the cost-effective defense strategy have been examined.

The weighted balance between the loss and the cost seems a problem. In practice, the execution of the proposed defense strategies needs a great effort. As most realistic networks such as the social networks vary over time, this work should be generalized to the time-varying networks [40–41]. It is of practical importance to study the cyber defense problem in a game-theoretical context, where the APT attack is strategic [42–44].

Acknowledgments

This work is supported by Natural Science Foundation of China (Grant Nos. 61572006, 71301177), National Sci-Tech Support Program of China (Grant No. 2015BAF05B03), Basic and Advanced Research Program of Chongqing (Grant No. cstc2013jcyjA1658), and Fundamental Research Funds for the Central Universities (Grant No. 106112014CD-JZR008823).

References

[1] R. Kitchin, Cyberspace: The World in the Wires, John Wiley & Sons, Inc. 1998.
[2] M. Dodge, R. Kitchin, Mapping Cyberspace, Routledge, 2000.

[3] D. Shoemaker, W.A. Conklin, Cybersecurity: The Essential Body of Knowledge, Cengage Learning, 2011.

[4] G.K. Kostopoulos, Cyberspace and Cybersecurity, Taylor & Francis, 2012.

[5] P.W. Singer, A. Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014.

[6] C. Tankard, Advanced persistent threats and how to monitor and deter them, Network Security, 2011(8) (2011) 16-19.

[7] P. Chen, L. Desmet, C. Huygens, A study on advanced persistent threats, in: B. De Decker, A. Zaquette (eds.), Communications and Multimedia Security (CMS2014), Lecture Notes in Computer Science, vol. 8735, 2014.

[8] P. Hu, H. Li, H. Fu, D. Cansever, P. Mohapatra, Dynamic defense strategy against advanced persistent threat with insiders, in: Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM), 2015, pp. 747-756.

[9] S. Rass, S. Konig, S. Schauer, Defending against advanced persistent threats using game-theory, PLoS ONE 12(1) (2017) e0168675.

[10] P. Van Mieghem, J.S. Omic, R.E. Kooij, Virus spread in networks, IEEE/ACM Transactions on Networking 17(1) (2009) 1-14.

[11] P. Van Mieghem, The N-Interwined SIS epidemic network model, Computing 93(2) (2011) 147-169.

[12] F.D. Sahneh, F.N. Chowdhury, C.M. Scoglio, On the existence of a threshold for preventive behavioral responses to suppress epidemic spreading, Scientific Reports 2 (2012) 623.

[13] F.D. Sahneh, C. Scoglio, P. Van Mieghem, Generalized epidemic mean-field model for spreading processes over multilayer complex networks, IEEE/ACM Transactions on Networking, 2013, 21(5): 1609-1620.

[14] L.X. Yang, X. Yang, Y.Y. Tang, A bi-virus competing spreading model with generic infection rates, IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2017.2734075.

[15] S. Xu, W. Lu, Z. Zhan, A stochastic model of multivirus dynamics, IEEE Transactions on Dependable and Secure Computing 9(1) (2012) 30-45.

[16] S. Xu, W. Lu, L. Xu, Push-and pull-based epidemic spreading in networks: Thresholds and deeper insights, ACM Transactions on Autonomous and Adaptive Systems 7(3) (2012) Article No. 32.

[17] S. Xu, W. Lu, L. Xu, Z. Zhan, Adaptive epidemic dynamics in networks: Thresholds and control, ACM Transactions on Autonomous and Adaptive System 8(4) (2014) Article No. 19.

[18] L.X. Yang, M. Draief, X. Yang, The impact of the network topology on the viral prevalence: a node-based approach, PLoS ONE, 10(7) (2015) e0134507.

[19] L.X. Yang, M. Draief, X. Yang, Heterogeneous virus propagation in networks: A theoretical study, Mathematical Methods in the Applied Sciences 40(5) (2017) 1396-1413.

[20] L.X. Yang, X. Yang, Y. Wu, The impact of patch forwarding on the prevalence of computer virus, Applied Mathematical Modelling, 43 (2017) 110-125.

[21] L.X. Yang, X. Yang, Y.Y. Tang, A bi-virus competing spreading model with generic infection rates, IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2017.2734075.

[22] L.X. Yang, P. Li, X. Yang, Y. Wu, Y.Y. Tang, Analysis of the effectiveness of the truth-spreading strategy for inhibiting rumors, arXiv:1705.06604.

[23] L.X. Yang, T. Zhang, X. Yang, Y. Wu, Y.Y. Tang On the effectiveness of the truth-spreading/rumor-blocking strategy for restraining rumors, arXiv:1705.10610.

[24] S. Xu, Cybersecurity dynamics, in: Proceedings of the 2014 Symposium and Bootcamp on the Science of Security (HotSoS’14), 2014, Article No. 14.

[25] W. Lu, S. Xu, X. Yu, Optimizing active cyber defense, In: S.K. Das, C. Nita-Rotaru, M. Kantarciolu (eds.) Decision and Game Theory for Security, GameSec2013, Lecture Notes in Computer Science, vol. 8252, 2013.

[26] S. Xu, W. Lu, H. Li, A stochastic model of active cyber defense dynamics, Internet Mathematics 11 (2015) 28-75.
[27] R. Zheng, W. Lu, S. Xu, Active cyber defense dynamics exhibiting rich phenomena, in: Proceedings of HotSoS’15, 2015, Article No. 2.
[28] R. Zheng, W. Lu, S. Xu, Preventive and reactive cyber defense dynamics is globally stable, IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2017.2734904.
[29] E.K. Donald, Optimal Control Theory: An Introduction, 2012.
[30] D. Liberzon, Calculus of Variations and Optimal Control Theory: A Concise Introduction, Princeton University Press, 2012.
[31] L.X. Yang, M. Draief, X. Yang, The optimal dynamic immunization under a controlled heterogeneous node-based SIRS model, Physica A, 2016, 450, 403-415.
[32] C. Nowzari, V.M. Preciado, G.J. Pappas, Analysis and control of epidemics: A survey of spreading processes on complex networks, IEEE Control Systems, 2016, 36(1): 26-46.
[33] T. Zhang, L.X. Yang, X. Yang, Y. Wu, Y.Y. Tang, Dynamic malware containment under an epidemic model with alert, Physica A, 470: 249-260.
[34] R.C. Robinson, An Introduction to Dynamical Systems: Continuous and Discrete, Pearson Education, Inc., 2004.
[35] D. Kempe, J. Kleinberg, E. Tardos, Influential nodes in a diffusion model for social networks, Proceedings of the 32nd International Conference on Automata, Languages and Programming, 2005, 1127-1138.
[36] W. Chen, Y. Wang, S. Yang, Efficient influence maximization in social networks, Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2009, pp. 199-208.
[37] A.L. Barabasi, R. Albert, Emergence of scaling in random networks, Science, 286 (1999) 509-512.
[38] D.J. Watts, S.H. Strogatz, Collective dynamics of 'small-world' networks, Nature, 393 (1998) 440-442.
[39] J. Kunegis, U. Rovira i Virgili. [Online] 27 April 2017 http://konect.uni-koblenz.de/networks/arenas-email
[40] Y. Schwarzkopf, Rakos A, D. Mukamel, Epidemic spreading in evolving networks, Physical Review E, 82 (2010) 036112.
[41] M. Karsai, N. Perra, A. Vespignani, Time varying networks and the weakness of strong ties, Scientific Reports, 4 (2014) 4001.
[42] R. Isaacs, Differential Games: A Mathematical Theory with Applications to Warfare and Pursuit, Control and Optimization, Dover Publications, 1999.
[43] A. Bressan, Noncooperative differential games, Milan Journal of Mathematics 79(2) (2011) 357-427.
[44] M. Tambe, Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned, Cambridge University Press, 2012.