Security evaluation of cyber networks under advanced persistent threats

Lu-Xing Yang\textsuperscript{a,b}, Pengdeng Li\textsuperscript{c}, Xiaofan Yang\textsuperscript{c,}, Luosheng Wen\textsuperscript{c}, Yingbo Wu\textsuperscript{c}, Yuan Yan Tang\textsuperscript{d}

\textsuperscript{a}School of Mathematics and Statistics, 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}School of Software Engineering, Chongqing University, Chongqing, 400044, China
\textsuperscript{d}Department of Computer and Information Science, The University of Macau, Macau

Abstract

This paper is devoted to measuring the security of cyber networks under advanced persistent threats (APTs). First, an APT-based cyber attack-defense process is modeled as an individual-level dynamical system. Second, the dynamic model is shown to exhibit the global stability. On this basis, a new security metric of cyber networks, which is known as the limit security, is defined as the limit expected fraction of compromised nodes in the networks. Next, the influence of different factors on the limit security is illuminated through theoretical analysis and computer simulation. This work helps understand the security of cyber networks under APTs.

Keywords: cybersecurity, advanced persistent threat, cyber attack-defense, dynamic model, global stability, security metric

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

1. Introduction

Cyberspace has come to be an integral part of our society. Government agencies, schools, hospitals, corporations, financial institutions and other organizations ceaselessly collect, process, and store a great deal of data on computers and transmit these confidential data across networks to other computers [1, 2]. However, cyberspace is vulnerable to a wide range of cyber threats. Sophisticated cyber perpetrators exploit vulnerabilities to steal information and money and develop capabilities to disrupt and destroy essential cyber services. In light of the risk and potential consequences of cyber attacks, strengthening the security and resilience of cyberspace has become an important mission. Cybersecurity is committed to protecting computers, networks, programs and data from unintended or unauthorized access, change, or destruction [3–5]. You cannot manage if you cannot measure. Before working out cyberspace security solutions, the security of cyber networks must be evaluated [6–8].

\textsuperscript{∗}Corresponding author

Email addresses: ylx910920@gmail.com (Lu-Xing Yang), 1414797521@qq.com (Pengdeng Li), xfyang1964@gmail.com (Xiaofan Yang), wls@cqu.edu.cn (Luosheng Wen), yzb@cqu.edu.cn (Yingbo Wu), yytang@umac.mo (Yuan Yan Tang)
Advanced persistent threats (APTs) are a newly emerging class of cyber attacks. With a clear goal, an APT attack is highly targeted, well-organized, well-resourced, covert and long-term [9–11]. APTs pose a severe threat to cyberspace, because they invalidate conventional cyber defense mechanisms. In the last decade, the number of APTs increased rapidly and numerous security incidents were reported all over the world [12]. For the purpose of resisting APTs, it is vital to evaluate the security of cyber networks under APTs. However, due to the persistence of APTs, existing security evaluation methods are not applicable to APTs [13–17]. Recently, Pendleton et al. [18] considered the expected fraction of compromised nodes in a cyber network as a security metric of the network. As the fraction is varying over time, its availability is questionable.

To measure the security of a cyber network under APTs, an APT-based cyber attack-defense process must be modeled as a continuous-time dynamical system. The individual-level dynamical modeling technique, which has been applied to areas such as epidemic spreading [19–21], malware spreading [22–29], rumor spreading [30, 31] and viral marketing [32], is especially suited to the modeling of APT-based cyber attack-defense processes, because the topological structure of the targeted cyber network can be accommodated [33]. Towards this direction, a number of APT-based cyber attack-defense models have been proposed [34–36]. In particular, Zheng et al. [37] found that a special APT-based cyber attack-defense model exhibits a global stability.

This paper focuses on estimating security of cyber networks under APTs. First, an APT-based cyber attack-defense model is modeled as an individual-level dynamical system. Second, the dynamic model is shown to exhibit the global stability. On this basis, a new security metric of cyber networks, which is known as the limit security, is defined as the limit expected fraction of compromised nodes in the networks. Next, the influence of different factors on the limit security is illuminated through theoretical analysis and computer simulation. This work helps understand the security of cyber networks under APTs.

The remaining materials are organized this way. Section 2 derives an APT-based cyber attack-defense model. Section 3 shows the global stability of the model and defines the limit security of cyber networks. The influence of different factors on the limit security is made clear in Sections 4 and 5. Finally, Section 6 closes this work.

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

For the purpose of evaluating the security of a cyber network under APTs, understanding the relevant cyber attack-defense process is requisite. This is the goal of this section.

2.1. The cyber network

Let $G = (V, E)$ denote the network interconnecting computers in a given cyber network, where $V = \{1, \cdots, N\}$, each node represents a computer in the cyber network, and there is an edge from node $i$ to node $j$ if and only if
computer $i$ is allowed to deliver messages directly to computer $j$ through the network. Let $A = (a_{ij})_{N \times N}$ denote the adjacency matrix for $G$. Hereafter, $G$ is assumed to be strongly connected.

In what follows, it is assumed that, at any time, every node in the cyber network is either secure or compromised, where all secure nodes are under the defender’s control, and all compromised nodes are under the attacker’s control. Let $X_i(t) = 0$ and $1$ denote that node $i$ is secure and compromised at time $t$, respectively. Then the state of the cyber network at time $t$ is represented by the vector

$$X(t) = (X_1(t), X_2(t), \cdots, X_N(t)).$$

Let $S_i(t)$ and $C_i(t)$ denote the probability of node $i$ being secure and compromised at time $t$, respectively.

$$S_i(t) = \Pr\{X_i(t) = 0\}, \quad C_i(t) = \Pr\{X_i(t) = 1\}.$$ 

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 $t$.

### 2.2. The attack and defense mechanisms

The threat of an APT attack to the cyber network is twofold.

- **External attack**, which is conducted by the external attacker, with the intent of compromising the secure nodes in the network. The attack strength to secure node $i$ is $\alpha x_i$, where $\alpha$ stands for the technical level of external attack, $x_i$ stands for the resource per unit time used for attacking node $i$, $\sum_{i=1}^{N} x_i > 0$.

- **Internal infection**, which is caused by the compromised nodes in the network, with the intent of compromising the secure nodes in the network. The infection strength of compromised node $i$ to secure node $j$ is $\beta a_{ij}$, where $\beta$ stands for the technical level of internal infection. The combined infection strength to secure node $i$ at time $t$ is

$$f(\beta \sum_{j=1}^{N} a_{ij} 1_{(X_j(t) = 1)})$$

where $1_{A}$ stands for the indicator function of event $A$, $f(0) = 0$, $f(x) \leq x$ for all $x \geq 0$, $f$ is strictly increasing and concave, and $f$ is second continuously differentiable.

We refer to the vector $x = (x_1, \cdots, x_N)$ as an attack scheme. The resource per unit time for the attack scheme $x$ is

$$\|x\|_1 = \sum_{i=1}^{N} x_i,$$

where $\| \cdot \|_1$ stands for the 1-norm of vectors.

The defense of the cyber network against APTs is also twofold.

- **Prevention**, which aims to prevent the secure nodes in the cyber network from being compromised. The prevention strength of secure node $i$ is $\delta y_i$, where $\delta$ stands for the technical level of prevention, $y_i > 0$ stands for the resource per unit time used for preventing node $i$.

- **Recovery**, which is intended to recover the compromised nodes in the cyber network. The recovery strength of compromised $i$ is $\gamma z_i$, where $\gamma$ stands for the technical level of recovery, $z_i > 0$ stands for the resource per unit time for recovering node $i$. 


We refer to the vector \(y = (y_1, \cdots, y_N)\) as a prevention scheme, the vector \(z = (z_1, \cdots, z_N)\) as a recovery scheme, and the vector \((y, z)\) as a defense scheme. The resources per unit time for the prevention scheme \(y\), the recovery scheme \(y\) and the defense scheme \((y, z)\) are \(\|y\|_1, \|z\|_1\) and \(\|y\|_1 + \|z\|_1\), respectively.

Let \(w = (w_1, \cdots, w_N)\) denote an attack scheme or a prevention scheme or a recovery scheme. In the subsequent study, the following two schemes will be used.

- The degree-first scheme: \(w_i\) is linearly proportional to the out-degree of node \(i\). Formally,
  \[
  w = \|w\|_1 \cdot \left(\frac{\sum_{j=1}^{N} a_{ij}}{\sum_{i,j=1}^{N} a_{ij}}, \frac{\sum_{j=1}^{N} a_{ij}}{\sum_{i,j=1}^{N} a_{ij}}, \cdots, \frac{\sum_{j=1}^{N} a_{ij}}{\sum_{i,j=1}^{N} a_{ij}}\right).
  \]

- The degree-last scheme: \(w_i\) is inversely linearly proportional to the out-degree of node \(i\). Formally,
  \[
  w = \|w\|_1 \cdot \left(\frac{1}{\sum_{j=1}^{N} a_{ij}}, \frac{1}{\sum_{i,j=1}^{N} a_{ij}}, \cdots, \frac{1}{\sum_{i,j=1}^{N} a_{ij}}\right).
  \]

- The uniform scheme: all \(w_i\) are identical. Formally,
  \[
  w = \|w\|_1 \cdot \left(\frac{1}{N}, \frac{1}{N}, \cdots, \frac{1}{N}\right).
  \]

2.3. The modeling of APT-based cyber attack-defense processes

For the purpose of modeling APT-based cyber attack-defense processes, the following assumptions are made.

(A1) Due to external attack, at any time secure node \(i\) gets compromised at rate \(\frac{\alpha_i}{\gamma_i}\). This assumption is rational, because the rate is proportional to the attack strength and is inversely proportional to the prevention strength.

(A2) Due to internal infection, at any time secure node \(i\) gets compromised at rate \(\frac{f}{\gamma_i} \frac{\sum_{j=1}^{N} a_{ij} \sum_{j'=1}^{N} a_{jj'}}{\gamma_i}\). This assumption is rational, because the rate is proportional to the combined infection strength and is inversely proportional to the prevention strength.

(A3) Due to recovery, at any time compromised node \(i\) becomes secure at rate \(\gamma z_i\). This assumption is rational, because the rate is proportional to the recovery strength.

Next, let us model the cyber attack-defense process. Let \(\Delta t\) be a very small time interval. Following the above assumptions, we have that, for \(i = 1, \cdots, N, t \geq 0\),

\[
\Pr[X_i(t + \Delta t) = 1 | X_i(t) = 0] = \frac{\Delta t}{\gamma_i} \left[\alpha x_i + f \left(\beta \sum_{j=1}^{N} a_{ij} C_j(t)\right)\right] + o(\Delta t),
\]

\[
\Pr[X_i(t + \Delta t) = 0 | X_i(t) = 1] = \gamma z_i \Delta t + o(\Delta t).
\]
Invoking the total probability formula, rearranging the terms, dividing both sides by $\Delta t$, and letting $\Delta t \to 0$, we get a dynamic model as follows.

$$\frac{dC_i(t)}{dt} = \frac{\alpha x_i}{\delta y_i} - \left( \frac{\alpha x_i}{\delta y_i} + \gamma z_i \right) C_i(t) + \frac{1}{\delta y_i} \left[ 1 - C_i(t) \right] f \left( \beta \sum_{j=1}^{N} a_{ij} C_j(t) \right), \quad t \geq 0, i = 1, \ldots, N. \tag{1}$$

We refer to the model as the generic secure-compromised-secure (GSCS) model, because the function $f$ meets a set of generic conditions. The diagram of state transitions of node $i$ under this model is given in Fig. 1. To a certain extent, the GSCS model accurately captures APT-based cyber attack-defense processes.

![Figure 1: Diagram of state transitions of node $i$ under the GSCS model.](image)

Let

$$\Omega = \{(c_1, c_2, \ldots, c_N)^T \in \mathbb{R}_+^N | c_i \leq 1, i = 1, \ldots, N\}.$$

It is trivial to show that $C(t) \in \Omega$ for $t \geq 0$.

3. Theoretical analysis of the GSCS model

This section is dedicated to studying the dynamical properties of the GSCS model.

3.1. Preliminaries

For fundamental knowledge on differential dynamical systems, see Ref. [38].

**Lemma 1.** (Chaplygin Lemma, see Theorem 31.4 in [39]) Consider a smooth $n$-dimensional system of differential equations

$$\frac{dx(t)}{dt} = f(x(t)), \quad t \geq 0$$

and the corresponding system of differential inequalities

$$\frac{dy(t)}{dt} \geq f(y(t)), \quad t \geq 0$$

with $x(0) = y(0)$. Suppose that for any $a_1, \ldots, a_n \geq 0$, there hold

$$f_i(x_1 + a_1, \ldots, x_{i-1} + a_{i-1}, x_i, x_{i+1} + a_{i+1}, \ldots, x_n + a_n) \geq f_i(x_1, \ldots, x_n), \quad i = 1, \ldots, n.$$

Then $y(t) \geq x(t)$ for $t \geq 0$. 

5
For fundamental knowledge on fixed point theory, see Ref. [40].

**Lemma 2.** *(Brouwer Fixed Point Theorem, see Theorem 4.10 in [40])* Let $D$ be a nonempty, bounded, closed and convex subset of $\mathbb{R}^n$, and let $f : D \to D$ be a continuous function. Then $f$ has a fixed point.

For fundamental knowledge on matrix theory, see Ref. [41]. Let $\text{diag}(a_i)$ denote the diagonal matrix with diagonal entries $a_1, a_2, \cdots, a_N$, and let $\text{col}(a_i)$ denote the column vector of components $a_1, a_2, \cdots, a_N$. This paper considers only real square matrices. For a matrix $A$, let $s(A)$ denote the maximum real part of an eigenvalue of $A$. $A$ is *Metzler* if its off-diagonal entries are all nonnegative.

**Lemma 3.** *(Section 2.1 in [42])* Let $A$ be an irreducible Metzler matrix. Then the following claims hold.

(a) If there is a positive vector $x$ such that $Ax < \lambda x$, then $s(A) < \lambda$.

(b) If there is a positive vector $x$ such that $Ax = \lambda x$, then $s(A) = \lambda$.

(c) If there is a positive vector $x$ such that $Ax > \lambda x$, then $s(A) > \lambda$.

### 3.2. A preliminary result

For the GSCS model, let

$$C_i(t) = \frac{\alpha x_i}{\alpha x_i + \gamma \delta y_i z_i}, \quad \overline{C}_i = \frac{\alpha x_i + f(\beta \sum_{j=1}^N a_{ij})}{\alpha x_i + \gamma \delta y_i z_i + f(\beta \sum_{j=1}^N a_{ij})}, \quad i = 1, \cdots, N.$$

The following lemma will be useful in the subsequent study.

**Lemma 4.** Let $C(t) = (C_1(t), C_2(t), \cdots, C_N(t))^T$ be a solution to the SCS model. Then there are $t_0 > 0$ and $c > 0$ such that

$$\min_{1 \leq i \leq N} C_i(t) \geq c, \quad t \geq t_0.$$

**Proof.** Without loss of generality, assume $x_{i_0} > 0$. It follows from the GSCS model that

$$\frac{dC_{i_0}(t)}{dt} \geq \frac{\alpha x_{i_0}}{\delta y_{i_0}} - \frac{\left(\frac{\alpha x_{i_0}}{\delta y_{i_0}} + \gamma z_{i_0}\right)}{C_{i_0}(t)}, \quad t \geq 0.$$  

Obviously, the comparison system

$$\frac{dU_{i_0}(t)}{dt} = \frac{\alpha x_{i_0}}{\delta y_{i_0}} - \frac{\left(\frac{\alpha x_{i_0}}{\delta y_{i_0}} + \gamma z_{i_0}\right)}{U_{i_0}(t)}, \quad t \geq 0,$$

with $U_{i_0}(0) = C_{i_0}(0)$ admits $U_{i_0} > 0$ as the globally stable equilibrium. By Lemma 1, we have

$$C_{i_0}(t) \geq U_{i_0}(t), \quad t \geq 0.$$

So,

$$\liminf_{t \to \infty} C_{i_0}(t) \geq \lim_{t \to \infty} U_{i_0}(t) = \overline{C}_{i_0}.$$
Thus, for any $0 < \varepsilon < C_h$, there is $t_1 > 0$ such that

$$C_h(t) \geq C_h - \varepsilon, \quad t \geq t_1.$$  

As $G$ is strongly connected, there is $a_{i_0j_0} = 1$. Hence,

$$\frac{dC_{i_0}(t)}{dt} \geq \frac{1}{\delta y_{j_0}} f(\beta(C_h - \varepsilon)) - \frac{1}{\delta y_{j_0}} f(\beta(C_h - \varepsilon) + \gamma z_{j_0}) C_{i_0}(t), \quad t \geq t_1.$$  

Obviously, the comparison system

$$\frac{dv_{j_0}(t)}{dt} \leq \frac{1}{\delta y_{j_0}} f(\beta(C_h - \varepsilon)) - \frac{1}{\delta y_{j_0}} f(\beta(C_h - \varepsilon) + \gamma z_{j_0}) v_{j_0}(t), \quad t \geq t_1$$  

with $v_{j_0}(t_1) = C_{j_0}(t_1)$ admits

$$f(\beta(C_h - \varepsilon)) \over f(\beta(C_h - \varepsilon) + \gamma z_{j_0})$$  

as the globally stable equilibrium. By Lemma 1, we have

$$C_{j_0}(t) \geq v_{j_0}(t), \quad t \geq t_1.$$  

So,

$$\lim_{t \to \infty} C_{j_0}(t) \geq \lim_{t \to \infty} v_{j_0}(t) = \frac{f(\beta(C_h - \varepsilon))}{f(\beta(C_h - \varepsilon) + \gamma z_{j_0})}.$$  

In view of the arbitrariness of $\varepsilon$, we get that

$$\lim_{t \to \infty} C_{j_0}(t) \geq \frac{f(\beta(C_h))}{f(\beta(C_h) + \gamma z_{j_0})} > 0.$$  

The lemma follows by repeating the argument.  

3.3. The equilibrium

**Theorem 1.** The GSCS model admits a unique equilibrium. Denote this equilibrium by $C^* = (C^*_1, \ldots, C^*_N)^T$. Then $C^*_1 > 0, C^*_i \leq C^*_i \leq C^*_i, 1 \leq i \leq N$.  

**Proof.** Let $K = \left[ \prod_{i=1}^N \left[ C^*_i, C^*_i \right] \right]$. Define a continuous mapping $H = (H_1, \ldots, H_N)^T : K \to [0, 1]^N$ as follows.

$$H_i(w) = \frac{a_{x_i} + f(\beta \sum_{j=1}^N a_{jw_j})}{a_{x_i} + \gamma \delta y_{i1} + f(\beta \sum_{j=1}^N a_{jw_j})}, \quad w = (w_1, \ldots, w_N)^T \in K.$$  

It is trivial to show that $C$ is an equilibrium of the GSCS model if and only if $C$ is a fixed point of $H$. Furthermore, it is easy to show that $H$ maps $K$ into itself. It follows from Lemma 2 that $H$ has a fixed point, denoted $C^* = (C^*_1, \ldots, C^*_N)^T$. This implies that $C^*$ is an equilibrium of the GSCS model, where $C^*_1 \leq C^*_i \leq C^*_i, 1 \leq i \leq N$. By Lemma 4, $C^*_i > 0, 1 \leq i \leq N$.  

The remaining thing to do is to show that $C^*$ is the unique fixed point of $H$. On the contrary, suppose $H$ has a fixed point other than $C^*$. Denote this equilibrium by $C^{**} = (C^{**}_1, \ldots, C^{**}_N)^T$. Let

$$\rho = \max_{1 \leq i \leq N} \frac{C^*_i}{C^{**}_i}, \quad i_0 = \arg \max_{1 \leq i \leq N} \frac{C^*_i}{C^{**}_i}.$$  

7
Without loss of generality, assume $\rho > 1$. It follows that
\[ C_{i_0}^* = H_{i_0}(C^*) \leq H_{i_0}(\rho C_{i_0}^{**}) = \frac{\alpha x_{i_0} + f(\rho \beta \sum_{j=1}^{N} a_{j_0} C_j^{**})}{\gamma \delta \mu_{i_0} z_{i_0} + \alpha x_{i_0} + f(\rho \beta \sum_{j=1}^{N} a_{j_0} C_j^{**})} \leq \frac{\alpha x_{i_0} + \rho f(\beta \sum_{j=1}^{N} a_{j_0} C_j^{**})}{\gamma \delta \mu_{i_0} z_{i_0} + \alpha x_{i_0} + \rho f(\beta \sum_{j=1}^{N} a_{j_0} C_j^{**})} \leq \rho H_{i_0}(C^{**}) = \rho C_{i_0}^{**}. \]

This contradicts the assumption that $C_{i_0}^* = \rho C_{i_0}^{**}$. Hence, $C^*$ is the unique fixed point of $H$. The proof is complete. □

3.4. The stability of the equilibrium

**Theorem 2.** The equilibrium $C^*$ of the GSCS model is stable with respect to $\Omega$.

**Proof.** Let $C(t) = (C_1(t), C_2(t), \cdots, C_N(t))^T$ be a solution to the GSCS model. By Lemma 4, there are $t_0 > 0$ and $c > 0$ such that
\[ \min_{i \leq N} C_i(t) \geq c, \quad t \geq t_0. \]

Let
\[ Z(C(t)) = \max_{i \leq N} \frac{C_i(t)}{C_i^*}, \quad z(C(t)) = \min_{i \leq N} \frac{C_i(t)}{C_i^*}, \quad t \geq t_0. \]

Define a function $V$ as
\[ V(C(t)) = \max\{Z(C(t)) - 1, 0\} + \max\{1 - z(C(t)), 0\}. \]

It is easily verified that $V$ is positive definite with respect to $C^*$, i.e., (a) $V(C(t)) \geq 0$, and (b) $V(C(t)) = 0$ if and only if $C(t) = C^*$. Next, let us show that $D^+ V(C(t)) \leq 0$, $t \geq t_0$, where $D^+$ stands for the upper-right Dini derivative of $V$ along $C(t)$. To this end, we need to show the following two claims.

**Claim 1:** $D^+ Z(C(t)) \leq 0$ if $Z(C(t)) \geq 1$. Moreover, $D^+ Z(C(t)) < 0$ if $Z(C(t)) > 1$.

**Claim 2:** $D_+ z(C(t)) \geq 0$ if $z(C(t)) \leq 1$. Moreover, $D_+ z(C(t)) > 0$ if $z(C(t)) < 1$. Here $D_+$ stands for the lower-right Dini derivative.

**Proof of Claim 1:** Choose $k_0$ such that
\[ Z(C(t)) = \frac{C_{k_0}(t)}{C_{k_0}^*}, \quad D^+ Z(C(t)) = \frac{C_{k_0}'(t)}{C_{k_0}^*}. \]
Then,

\[
\frac{C^*_k}{C_k(t)} C'_k(t) = \frac{\alpha x_k}{\delta y_k} (1 - C_k(t)) \frac{C^*_k}{C_k(t)} + \frac{1}{\delta y_k} \left(1 - C_k(t)\right) \frac{C^*_k}{C_k(t)} \beta \sum_{j=1}^N a_{jk} C_j(t) - \gamma z_k C^*_k
\]

\[\leq \frac{\alpha x_k}{\delta y_k} (1 - C_k^*) + \frac{1}{\delta y_k} \left(1 - C_k^*\right) \frac{C^*_k}{C_k(t)} \beta \sum_{j=1}^N a_{jk} C_j(t) - \gamma z_k C^*_k
\]

\[\leq \frac{\alpha x_k}{\delta y_k} (1 - C_k^*) + \frac{1}{\delta y_k} \left(1 - C_k^*\right) f \left(\beta \sum_{j=1}^N a_{jk} C_j(t)\right) - \gamma z_k C^*_k
\]

\[\leq \frac{\alpha x_k}{\delta y_k} (1 - C_k^*) + \frac{1}{\delta y_k} \left(1 - C_k^*\right) f \left(\beta \sum_{j=1}^N a_{jk} C_j^*\right) - \gamma z_k C^*_k = 0,
\]

where the second inequality follows from the concavity of \(f\), and the third inequality follows from the monotonicity of \(f\). This implies \(D^+ Z(C(t)) \leq 0\). As the first inequality is strict if \(Z(C(t)) > 1\), we get that \(D^+ Z(C(t)) < 0\) if \(Z(C(t)) > 1\). Claim 1 is proven.

The argument for Claim 2 is analogous to that for Claim 1 and hence is omitted. Next, consider three possibilities.

Case 1: \(Z(C(t)) < 1\). Then \(z(C(t)) < 1\), \(V(C(t)) = 1 - z(C(t))\). Hence, \(D^+ V(C(t)) = -D_z z(C(t)) < 0\).

Case 2: \(z(C(t)) > 1\). Then \(Z(C(t)) > 1\), \(V(C(t)) = Z(C(t)) - 1\). Hence, \(D^+ V(C(t)) = D^+ Z(C(t)) < 0\).

Case 3: \(Z(C(t)) \geq 1, z(C(t)) \leq 1\). Then \(V(C(t)) = Z(C(t)) = z(C(t))\), \(D^+ V(C(t)) = D^+ Z(C(t)) - D_z z(C(t)) \leq 0\).

Moreover, the equality holds if and only if \(C(t) = C^*\).

The theorem follows from the LaSalle Invariance Principle.

Let \(C(t)\) denote the expected fraction of compromised nodes in the cyber network at time \(t\), \(C^*\) the expected fraction of compromised nodes in the cyber network when the expected network state is \(C^*\).

\[
C(t) = \frac{1}{N} \sum_{i=1}^N C_i(t), \quad C^* = \frac{1}{N} \sum_{i=1}^N C^*_i.
\]

The following result is a corollary of Theorem 2.

**Corollary 1.** Consider the GSCS model (1). Then \(C(t) \to C^*\) as \(t \to \infty\).

Obviously, \(C^*\) is dependent upon the four technical levels, the interconnection network, and the attack and defense schemes. We refer to the four technical levels and the interconnection network as parameters, because they are almost fixed. We refer to the attack and defense schemes as independent variables, because the attack scheme is flexibly choosable by the attacker, and the defense scheme is flexibly choosable by the defender. Formally,

\[C^* = C^*(x, y, z, \alpha, \beta, \delta, \gamma, G).
\]
3.5. The limit security of cyber networks

In practice, $C^*$ can be estimated simply through sampling and averaging. This method for estimating $C^*$ is valuable, because it does not require the defender to know the attack and infection technical levels as well as the attack scheme. Therefore, $C^*$ can be used to evaluate the security of the cyber network. Below let us define a security metric of cyber networks under APTs.

**Definition 1.** Given the four technical levels, the interconnected network, the attack scheme and the defense scheme, the limit security of the cyber network is defined as

$$S_L = 1 - C^*, \quad (3)$$

This security metric of cyber networks is rational, because the higher the limit security, the securer the cyber network would be. The limit security is dependent upon the four technical levels, the interconnection network, the attack scheme and the defense scheme. Formally,

$$C^* = C^*(x, y, z; \alpha, \beta, \delta, \gamma, G).$$

4. The influence of some factors on the limit security of a cyber network

In this section, we theoretically investigate the influence of some factors, including the technical levels, the attack and defense resources per unit time per node, and the addition of new edges to the interconnection network, on the limit security of a cyber network. For this purpose, define an irreducible Metzler matrix as follows.

$$M = \text{diag} \left( \beta (1 - C_i^*) f \left( \beta \sum_{j=1}^{N} a_{ij} C_j^* \right) \right) A^T - \text{diag} \left( \alpha x_i + \gamma \delta y_i z_i + f \left( \beta \sum_{j=1}^{N} a_{ij} C_j^* \right) \right).$$

**Lemma 5.** M is invertible, and $M^{-1}$ is negative.

**Proof.** As $f$ is concave, we have

$$f \left( \beta \sum_{j=1}^{N} a_{ij} C_j^* \right) \leq f \left( \frac{\beta \sum_{j=1}^{N} a_{ij} C_i^*}{\beta \sum_{j=1}^{N} a_{ij} C_j^*} \right).$$

So,

$$MC^* = \text{diag} \left( \beta (1 - C_i^*) f \left( \beta \sum_{j=1}^{N} a_{ij} C_j^* \right) \right) A^T C^* - \text{diag} \left( \alpha x_i + \gamma \delta y_i z_i + f \left( \beta \sum_{j=1}^{N} a_{ij} C_j^* \right) \right) C^* \leq \text{diag} \left( \beta (1 - C_i^*) f \left( \frac{\beta \sum_{j=1}^{N} a_{ij} C_i^*}{\beta \sum_{j=1}^{N} a_{ij} C_j^*} \right) \right) A^T C^* - \text{diag} \left( \alpha x_i + \gamma \delta y_i z_i + f \left( \beta \sum_{j=1}^{N} a_{ij} C_j^* \right) \right) C^*
\leq -\text{col} \left( \alpha x_i + f \left( \beta \sum_{j=1}^{N} a_{ij} C_j^* \right) C_j^* \right) < 0.$$

It follows from Lemma 3(a) that $s(M) < 0$. This implies that $M$ is invertible. As $M$ is Metzler, irreducible and Hurwitz, $M^{-1}$ is negative [43].
4.1. The influence of the four technical levels

**Theorem 3.** For the GSCS model (1), we have \( \frac{\partial C^*}{\partial \alpha} > 0, \frac{\partial C^*}{\partial \beta} > 0, \frac{\partial C^*}{\partial \gamma} < 0, \frac{\partial C^*}{\partial \delta} < 0. \)

**Proof.** We prove only \( \frac{\partial C^*}{\partial \beta} > 0, \) because the arguments for the remaining claims are similar. As \( C^* \) is the equilibrium for the GSCS model, we have

\[ F_i(\beta; C^*_1, C^*_2, \ldots, C^*_N) = \alpha x_i - (ax_i + \gamma \delta y_i z_i) C^*_i + (1 - C^*_i) f \left( \sum_{j=1}^{N} a_{ji} C^*_j \right) = 0, \quad 1 \leq i \leq N. \]

Differentiating on both sides with respect to \( \beta \), we get

\[ \frac{\partial F_i}{\partial \beta} + \frac{\partial C^*}{\partial C^*_1} \cdot \frac{\partial C^*_1}{\partial \beta} + \cdots + \frac{\partial F_i}{\partial C^*_N} \cdot \frac{\partial C^*_N}{\partial \beta} = 0, \quad 1 \leq i \leq N. \]

Calculations show that

\[ M \frac{\partial C^*}{\partial \beta} = -\text{diag} \left( (1 - C^*_i) f' \left( \sum_{j=1}^{N} a_{ji} C^*_j \right) \right) A^T C^*. \]

By Lemma 5, we have

\[ \frac{\partial C^*}{\partial \beta} = -M^{-1} \cdot \text{diag} \left( (1 - C^*_i) f' \left( \sum_{j=1}^{N} a_{ji} C^*_j \right) \right) A^T C^*. \]

where \( M^{-1} \) is negative. As \( G \) is strongly connected, \( A^T C^* \) is positive. Hence, \( \frac{\partial C^*}{\partial \beta} > 0. \)

As a corollary of this theorem, the influence of the four technical levels on the limit security of a cyber network is shown as follows.

**Corollary 2.** For the GSCS model (1), we have \( \frac{\partial S_L}{\partial \alpha} < 0, \frac{\partial S_L}{\partial \beta} < 0, \frac{\partial S_L}{\partial \gamma} > 0, \frac{\partial S_L}{\partial \delta} > 0. \)

This corollary manifests that the limit security of a cyber network goes up with the prevention and recovery technical levels, and comes down with the attack and infection technical levels. These results accord with our intuition. Hence, the defender must try his best to enhance the prevention and recovery technical levels.

4.2. The influence of the attack and defense resources per unit time per node

**Theorem 4.** For the GSCS model (1), we have \( \frac{\partial C^*}{\partial x_i} > 0, \frac{\partial C^*}{\partial y_i} < 0, \frac{\partial C^*}{\partial z_i} < 0, \frac{\partial C^*}{\partial \gamma} < 0, \frac{\partial C^*}{\partial \delta} < 0, \) \( 1 \leq i \leq N. \)

The argument for the theorem is analogous to that for the previous theorem. As a corollary of this theorem, the influence of the attack and defense resources per unit time per node on the limit security of a cyber network is shown as follows.

**Corollary 3.** For the GSCS model (1), we have \( \frac{\partial S_L}{\partial x_i} < 0, \frac{\partial S_L}{\partial y_i} > 0, \frac{\partial S_L}{\partial z_i} > 0, \frac{\partial S_L}{\partial \gamma} > 0, \frac{\partial S_L}{\partial \delta} > 0, \) \( 1 \leq i \leq N. \)

This corollary demonstrates that the limit security of a cyber network rises with the resource per unit time used for preventing or recovering a node, and falls with the resource per unit time used for attacking a node. Again, these results are consistent with our intuition. As a consequence, the defender is suggested to configure more defense resource.
4.3. The influence of the addition of new edges to the interconnection network

**Theorem 5.** For the GSCS model, we have \( \frac{\partial C^*}{\partial a_{ij}} > 0 \), \( 1 \leq i, j \leq N, i \neq j \).

The argument for the theorem is analogous to that for Theorem 3. As a corollary of this theorem, the addition of new edges to the interconnection network on the limit security of a cyber network is shown as follows.

**Corollary 4.** For the GSCS model (1), we have \( \frac{\partial S_{L_i}}{\partial a_{ij}} < 0 \), \( 1 \leq i, j \leq N, i \neq j \).

This corollary manifests that the limit security of a cyber network declines with the addition of new edges to the interconnection network. Hence, a well-connected cyber network is more vulnerable to APTs. Therefore, the defender is suggested to limit the number of connections in the interconnection network.

5. The influence of two other factors on the limit security of a cyber network

In this section, we experimentally examine the influence of two factors, the ratio of the prevention resource to the recovery resource, and the defense resource per unit time with given ratio of the attack resource to the defense resource, on the limit security of a cyber network. In the following experiments, the generic function in the GSCS model is set to be \( f(x) = \frac{1}{1-x} \), and the interconnection network takes value from a set of six non-isomorphic trees shown in Fig. 2.

![Six non-isomorphic trees](image)

**Figure 2:** Six non-isomorphic trees with six nodes and five edges.
5.1. The influence of the ratio of the prevention resource to the recovery resource

For a GSCS model, the ratio of the prevention resource to the recovery resource is

\[ r_{PR} = \frac{|y|_1}{|z|_1}. \]

We examine the influence of \( r_{PR} \) on the limit security of a cyber network through simulation experiments.

**Experiment 1.** Consider 504 GSCS models, where \( \alpha = 0.05, \beta = 0.01, \gamma = 1, \delta = 1, \) \( G \) varies from \( G_1 \) to \( G_6, \)

\[ ||x||_1 = 1, ||y||_1 = \frac{1}{17}, ||z||_1 = \frac{1}{11}, r \in \{ \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, 1, 2, 3, 4 \}, \]

with (a) uniform \( x, y \) and \( z; \) (b) uniform \( x \) and \( y, \) degree-first \( z; \) (c) uniform \( x \) and \( z, \) degree-first \( y; \) (d) uniform \( x, \) degree-first \( y \) and \( z; \) (e) degree-first \( x, \) uniform \( y \) and \( z; \) (f) degree-first \( x \) and \( z, \) uniform \( y; \) (g) degree-first \( x \) and \( y, \) uniform \( z; \) (h) degree-first \( x, y \) and \( z; \) (i) degree-last \( x, \) uniform \( y \) and \( z; \) (j) degree-last \( x, \) uniform \( y, \) degree-first \( z; \) (k) degree-last \( x, \) degree-first \( y, \) uniform \( z; \) (l) degree-last \( x, \) degree-first \( y \) and \( z. \)

For each of the GSCS model, the limit security of the cyber network is shown shown in Fig. 3. It can be seen that, with the increase of \( r_{PR}, \) the limit security of a cyber network goes up first but then it goes down. Moreover, the limit security attains the maximum in the proximity of \( r_{PR} = 1. \)

Many similar experiments exhibit qualitatively similar phenomena. It is concluded that, with the increase of the ratio of the prevention resource to the recovery resource, the limit security of a cyber network goes up first but then it goes down. Moreover, the limit security attains the maximum when the prevention resource is close to the recovery resource. Hence, the defender is suggested to distribute the total defense resource equally to prevention and recovery.
Obviously, the limit security of a cyber network declines with attack resource to the defense resource, how about the impact of the defense resource on the limit security of a cyber network? Then it goes down. Moreover, the limit security attains the maximum in the proximity of $r_{pg} = 1$.

5.2. The influence of defense resource per unit time given the ratio of the attack resource to the defense resource

For a GSCS model, the ratio of the attack resource to the defense resource is

$$r_{AD} = \frac{||x||_1}{||y||_1 + ||z||_1}.$$ 

Obviously, the limit security of a cyber network declines with $r_{AD}$. A question arises naturally: given the ratio of the attack resource to the defense resource, how about the impact of the defense resource on the limit security of a cyber network? Now, let us answer the question through simulation experiments.
Experiment 2. Consider 504 GSCS models, where $\alpha = 0.1$, $\beta = 0.05$, $\gamma = 0.5$, $\delta = 1$, $G$ varies from $G_1$ to $G_6$, $r_{AD} = r$, $||y||_1 = ||z||_1 = s$, $s \in \{2, 3, \cdots, 10\}$, $||y||_1 = s_1$, with (a) $r = \frac{1}{2}$, uniform $x$, $y$ and $z$; (b) $r = 1$, uniform $x$, $y$ and $z$; (c) $r = 2$, uniform $x$, $y$ and $z$; (d) $r = \frac{1}{2}$, uniform $x$, degree-first $y$ and $z$; (e) $r = 1$, uniform $x$, degree-first $y$ and $z$; (f) $r = 2$, uniform $x$, degree-first $y$ and $z$; (g) $r = \frac{1}{2}$, degree-first $x$, uniform $y$ and $z$; (h) $r = 1$, degree-first $x$, uniform $y$ and $z$; (i) $r = 2$, degree-first $x$, uniform $y$ and $z$; (j) $r = \frac{1}{2}$, degree-first $x$, $y$ and $z$; (k) $r = 1$, degree-first $x$, $y$ and $z$; (l) $r = 2$, degree-first $x$, $y$ and $z$. For each of the GSCS models, the limit security of the cyber network is shown in Fig. 4. It can be seen that the limit security of a cyber network ascends with $s$.

Many similar experiments exhibit qualitatively similar phenomena. It is concluded that, given the ratio of the attack resource to the defense resource, the limit security of a cyber network goes up with the defense resource. This result sounds a good news to the defender. Indeed, configuring more defense resource is always an effective means of protecting against APTs.
6. Concluding remarks

This paper is devoted to measuring the security of cyber networks under APTs. An APT-based cyber attack-defense process has been modeled as a dynamical system, which is shown to exhibit the global stability. Thereby, the limit security has been introduced as a new security metric of cyber networks. The influence of different factors on the limit security has been expounded. On this basis, some means of defending against APTs are recommended.

There are lots of open problems about APTs. In the case that the attack scheme is available, the defender must
maximize the limit security over all possible defense schemes, so as to minimize the loss caused by APTs. When the attack scheme is not available, the defender should further minimize this maximized limit security over all possible attack schemes, so as to evaluate the worst-case security of the cyber network. In this work, the attack and defense schemes are both assumed to be unvaried over time. In practice, the attacker may flexibly alter the attack scheme to chase the highest profit, and the defender may flexibly change the defense scheme to maximize the security of the cyber network. In such scenarios, the evaluation of the security of cyber networks would involve optimal control theory [44,46] or/and dynamic game theory [47,48].

Acknowledgments

This work is supported by Natural Science Foundation of China (Grant Nos. 61572006, 71301177), 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] A. Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison-Wesley Professional, 2007.
[7] W. Jensen, Directions in security metrics research, National Institute of Standards and Technology, NISTIR7564, 2009.
[8] Y. Cheng, J. Deng, J. Li, S.A. DeLoach, A. Singhal, X. Ou, Metrics of security, In: A. Kott, C. Wang, R. Erbacher (eds) Cyber Defense and Situational Awareness, Advances in Information Security, vol. 62, Springer, 2014.
[9] C. Tankard, Advanced persistent threats and how to monitor and deter them, Network Security, 2011(8) (2011) 16-19.
[10] P. Chen, L. Desmet, C. Huynens, A study on advanced persistent threats, in: B. De Decker, A. Zuquete (eds.), Communications and Multimedia Security (CMS2014), Lecture Notes in Computer Science, vol. 8735, 2014.
[11] 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.
[12] S. Rass, S. Konig, S. Schauer, Defending against advanced persistent threats using game-theory, PLoS ONE 12(1) (2017) e0168675.
[13] C. Phillips and L. P. Swiler, A graph-based system for network-vulnerability analysis, in: Proceedings of the 1998 Workshop on New Security Paradigms, 1998, pp. 71-79.
[14] I. Kotenko, M. Stepashkin, Attack graph based evaluation of network security, in: Proceedings of the 10th IFIP TC-6 TC-11 international conference on Communications and Multimedia Security, 2006, pp. 216-227.
[15] M. Frigault, L. Wang, Measuring network security using Bayesian network-based attack graphs, in Proceedings of 32nd Annual IEEE International Conference on Computer Software and Applications (COMPSAC’08), 2008.
R.P. Lippmann, J.F. Riordan, T.H. Yu, K.K. Watson, Continuous security metrics for prevalent network threats: introduction and first four metrics, ESC-TR-2010-099, 2012.

S.E. Yusuf, J.B. Hong, M. Ge, D.S. Kim, Composite metrics for network security analysis, Software Networking 2017(1) (2017) 137-160.

M. Pendleton, R. Garcia-Lebron, J.H. Cho, S. Xu, A survey on systems security metrics, ACM Computing Surveys 49(4) (2017) Article No. 62.

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

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

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.

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

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.

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.

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.

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.

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.

Y. Wu, P. Li, L.X. Yang, X. Yang, Y.Y. Tang, A theoretical method for assessing disruptive computer viruses, Physica A: Statistical Mechanics and its Applications 482 (2017) 325-336.

L.X. Yang, P. Li, X. Yang, Y.Y. Tang, Distributed interaction between computer virus and patch: A modeling study, arXiv:1705.04818.

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.

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:1705.10618.

T. Zhang, X. Yang, L.X. Yang, Y.Y Tang, Y Wu, A discount strategy in word-of-mouth marketing and its assessment, arXiv:1704.06910.

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

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.

S. Xu, W. Lu, H. Li, A stochastic model of active cyber defense dynamics, Internet Mathematics 11 (2015) 28-75.

Ren Zheng, W. Lu, S. Xu, Active cyber defense dynamics exhibiting rich phenomena, in: Proceedings of HotSoS’15, 2015, Article No. 2.

Ren Zheng, W. Lu, S. Xu, Preventive and reactive cyber defense dynamics Is globally stable, CoRR abs/1602.06807.

H.K. Khalil, Nonlinear Systems, Third Edition, Pearson Education, Inc., publishing as Prentice Hall, 2002.

J. Szarski, Differential Inequalities, Polish Scientific Publishers, Warszawa, 1965.

R.P. Agarwal, M. Meehan, D. O'Regan, Fixed Point Theory and Applications, Cambridge University, 2001.

R.A. Horn, C.R. Johnson, Matrix Analysis, Second Edition, Cambridge University Press, 2013.

R. Varga, Matrix Iterative Analysis, Springer-Verlag, New York, USA, 2000.
[43] K.S. Narendra, R. Shorten, Hurwitz stability of Metzler matrices, IEEE Transactions on Automatic Control 2010, 55(6): 1484-1487.

[44] E.K. Donald, Optimal Control Theory: An Introduction, 2012.

[45] 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.

[46] 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.

[47] R. Isaacs, Differential Games: A Mathematical Theory with Applications to Warfare and Pursuit, Control and Optimization, Dover Publications, 1999.

[48] A. Bressan, Noncooperative differential games, Milan Journal of Mathematics 79(2) (2011) 357-427.