Hindawi
Discrete Dynamics in Nature and Society
Volume 2019, Article ID 2051489, 12 pages
https://doi.org/10.1155/2019/2051489

Research Article

An Advanced Persistent Distributed Denial-of-Service Attacked Dynamical Model on Networks

Chunming Zhang, Junbiao Peng, and Jingwei Xiao

School of Information Engineering, Guangdong Medical University, Dongguan 523808, China

Correspondence should be addressed to Chunming Zhang; chunfei2002@163.com

Received 18 October 2018; Revised 7 December 2018; Accepted 8 January 2019; Published 3 February 2019

Academic Editor: Chuanxi Qian

The advanced persistent distributed denial-of-service (APDDoS) attack does a serious harm to cyber security. Establishing a mathematical model to accurately predict APDDoS attack on networks is still an important problem that needs to be solved. Therefore, to help us understand the attack mechanisms of APDDoS on networks, this paper first puts forward a novel dynamical model of APDDoS attack on networks. A systematic analysis of this new model shows that the maximum eigenvalue of the networks is a vital factor that determines the success or failure of the attack. What is more, a new sufficient condition for the global stability of attack-free equilibrium is obtained. The global attractivity of attacked equilibrium has also been proved. Eventually, this paper gives some numerical simulations to show the main results.

1. Introduction

Cyber-attack overwhelmingly invades every aspect of our life, which causes huge threats and enormous damage to thousands of industries. According to the report [1], the percentage of cyber-attack motivated by Cyber Crime has risen to 72.1% in 2017. And nowadays, there are a lot of attack ways, such as DDoS attack, DoS attack, and so on. Here, let us discuss some attacked means to achieve a better understanding of the cyber-attack. DoS attack, which is known as the denial-of-service attack, is an important means of attack. It always launches attacks of blocking the buffer of the host of service providers so as to make legal guests can not access the server. And among the cyber-attacks in 2016, about 11.3% attacks were DoS attacks. Different from the DoS attack, in a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources [2]. In addition, APT (Advanced Persistent Threat), which is a stealthy and continuous computer hacking process, usually has the characteristics of strong concealment, sophisticated techniques, and continuous monitoring [3]. Most importantly, this paper mainly talks about APDDoS (advanced persistent distributed denial-of-service) attack which is DDoS attack equipped with the advance of APT. With the characters of advanced reconnaissance, clear motive, tactical execution, outstanding computing power, and long-term durability [4], it has caused great losses to the world. During the opening ceremonies of the PyeongChang Winter Olympics in February 2018, TV and web services were affected by an APDDoS attack for about 12 hours [5]. In February 2018, GitHub (the world's largest code hosting website) suffered a serious APDDoS attack; the peak flow rate reached 1.35Tbps [6]. It is easy to know that the APDDoS attack is being more and more harmful and it has a profound impact on the world.

To fully understand the APDDoS attack, its steps must be introduced. First, attacker will invade as many infected computers as possible by inserting or injecting computer malware into phishing websites or phishing texts. So, if the visitor opens it, his/her computer would be infected. And then, the infected computers will be composed into a botnet that is controlled by the attacker. When there are enough infected computers, the attacker can launch flood attack to targeted IPs (services of host) which will be blocked or broken down soon after the attack.

The cyber-attack process on the network can be accurately expressed as a continuous-time Markov chain which is proposed by Van Mieghem [7, 8]. However, this method is

difficult in mathematical analysis. In order to overcome these difficulties, some approximation methods are proposed, such as individual-based mean-field theory (*IBMF*) and degree-based mean-field theory (*DBMF*) [9, 10]. For *IBMF*, any node can be regarded as a computer or local network in the network is statistically independent from its neighboring nodes [11–14]. For *DBMF,* any vertex classified by degree is connected to the set of nodes with different degree with the special probability [15–17].

To better understand the impact of network topology on APDDoS attack, in this paper we propose a novel APDDoS attack model on networks with *IBMF*. Then we found that the global stability of attack-free equilibrium and the global attractivity of attacked equilibrium depend on the value of the maximum eigenvalue of the attack network.

In Section 2, the paper proposes the APDDoS attack model. Its threshold and the equilibriums are calculated in Section 3. Further Discussions are given in Section 4. Next, the paper shows some numerical simulations in Section 5. Finally, a brief summary of the full paper is given.

2. Model Descriptions

According to the ability of computers to defend against malicious software on the network, the paper divides the computers into two groups: Weak-Protected group and Strong-Protected group. Here, we can divide computers into two groups by checking whether the computer has firewall.

The Weak-Protected group (WP), which lacks firewall protection, is vulnerable to malware attacks, such as computer worm, Trojan, and so on. The Weak-Protected group consists of two kinds of computers, which includes susceptible computers (*S*-node) and infected computers (*I*-node). The susceptible computers (*S*-node) are weak in preventing malware attacks but have not been infected yet, while the infected computers (*I*-node) refers to the computers which has been infected by malwares and controlled by hackers.

However, because the existence of the firewall, the Strong-Protected group (SP) can defend against many kinds of attacks, but it also can be attacked by APDDoS attack. The Strong-Protected group also consists of two kinds of computers, tolerant computers (*T*-node), and missed computers (*M*-node). Tolerant computers (*T*-node) represent computers with a firewall (which usually means servers) and works normally, while missed computers (*M*-node) denote the computers with a firewall but cannot respond to the request and become missed for the visitors due to the APDDoS attacks (see Figure 1).

Based on the above facts, some constants can be defined as follows:

(i) $G=(V, E)$: the network structure of the computers on network, and G can be represented as an undirected, connected, and nonlooped graph.

(ii) N: the scale of network G, which is also the whole number of the computer in the G.

(iii) A: the matrix of the network connection situation. A is a symmetric matrix with zero diagonal. $A = (a_{ij})$, $1 \le i, j \le N$.

(iv) λ_k: the spectrum of A, $1 \le k \le N$. As A is real and symmetric, we may assume $\lambda_{\max} \ge \lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_N$.

(v) $S_i(t)$: the i^{th} node, which is susceptible(S-node) at time t.

(vi) $I_i(t)$: the i^{th} node, which is infected(I-node) at time t.

(vii) $T_i(t)$: the i^{th} node, which is tolerant(T-node) at time t.

(viii) $L_i(t)$: the i^{th} node, which is missed(M-node) at time t.

Next, some reasonable assumptions are proposed as follows [18–21].

($H1$) As executing some operations that do harm to the computer security, like browsing the phishing websites or opening the phishing email, etc., any S_i infected by the neighboring I-nodes with probability β, the average probability of each S_i gets infected per unit time, is $\beta \sum_j a_{ij} I_j$.

($H2$) By installing some antivirus soft-wares, any $I_i(t)$ recovers to the state of susceptible, which also means becoming $S_i(t)$ with the probability γ.

($H3$) As occurring APDDoS attacks, any $T_i(t)$ can be attacked by neighboring I-nodes with the probability α. By calculating, the average probability of each $T_i(t)$ turns into the $M_i(t)$ per unit time is $\alpha \sum_j a_{ij} I_j$.

($H4$) As changing the hardware of computers and strengthen the firewall, any $M_i(t)$ restarts or recovers with the probability η.

($H5$) As the two groups of the computer are separated, the paper uses ϕ to denote the proportion of the Weak-Protected group and then $1-\phi$ is the proportion of the Strong-Protected group; also there are $S_i(t)+I_i(t)=\phi$ and $T_i(t)+M_i(t)=1-\phi$.

Let

$$\begin{aligned} S_i(t) &= \Pr\left(X_i(t) = 0\right), \\ I_i(t) &= \Pr\left(X_i(t) = 1\right), \\ T_i(t) &= \Pr\left(X_i(t) = 2\right), \\ M_i(t) &= \Pr\left(X_i(t) = 3\right). \end{aligned} \tag{1}$$

Also, the following equations can be obtained:

$$\begin{aligned} &S_i(t+\Delta t) \\ &\quad = S_i(t) \Pr\left(X_i(t+\Delta t) = 0 \mid X_i(t) = 0\right) \\ &\qquad + I_i(t) \Pr\left(X_i(t+\Delta t) = 0 \mid X_i(t) = 1\right) \\ &\qquad + T_i(t) \Pr\left(X_i(t+\Delta t) = 0 \mid X_i(t) = 2\right) \\ &\qquad + M_i(t) \Pr\left(X_i(t+\Delta t) = 0 \mid X_i(t) = 3\right), \\ &I_i(t+\Delta t) \\ &\quad = S_i(t) \Pr\left(X_i(t+\Delta t) = 1 \mid X_i(t) = 0\right) \\ &\qquad + I_i(t) \Pr\left(X_i(t+\Delta t) = 1 \mid X_i(t) = 1\right) \\ &\qquad + T_i(t) \Pr\left(X_i(t+\Delta t) = 1 \mid X_i(t) = 2\right) \\ &\qquad + M_i(t) \Pr\left(X_i(t+\Delta t) = 1 \mid X_i(t) = 3\right), \end{aligned}$$

$$
\begin{aligned}
&T_i(t+\Delta t)\\
&\quad = S_i(t)\Pr\left(X_i(t+\Delta t)=2 \mid X_i(t)=0\right)\\
&\qquad + I_i(t)\Pr\left(X_i(t+\Delta t)=2 \mid X_i(t)=1\right)\\
&\qquad + T_i(t)\Pr\left(X_i(t+\Delta t)=2 \mid X_i(t)=2\right)\\
&\qquad + M_i(t)\Pr\left(X_i(t+\Delta t)=2 \mid X_i(t)=3\right),\\
&M_i(t+\Delta t)\\
&\quad = S_i(t)\Pr\left(X_i(t+\Delta t)=3 \mid X_i(t)=0\right)\\
&\qquad + I_i(t)\Pr\left(X_i(t+\Delta t)=3 \mid X_i(t)=1\right)\\
&\qquad + T_i(t)\Pr\left(X_i(t+\Delta t)=3 \mid X_i(t)=2\right)\\
&\qquad + M_i(t)\Pr\left(X_i(t+\Delta t)=3 \mid X_i(t)=3\right).
\end{aligned}
\tag{2}
$$

In order to satisfy these above equations, β and α should be far less than 1. Let Δt be a very small interval. According to the assumptions given above, the following equations can be got:

$$
\begin{aligned}
&\Pr\left(X_i(t+\Delta t)=0 \mid X_i(t)=1\right)=\gamma\Delta t+o(\Delta t),\\
&\Pr\left(X_i(t+\Delta t)=2 \mid X_i(t)=3\right)=\eta\Delta t+o(\Delta t),\\
&\Pr\left(X_i(t+\Delta t)=1 \mid X_i(t)=1\right)=1-\gamma\Delta t+o(\Delta t),\\
&\Pr\left(X_i(t+\Delta t)=3 \mid X_i(t)=3\right)=1-\eta\Delta t+o(\Delta t).\\
&\Pr\left(X_i(t+\Delta t)=1 \mid X_i(t)=0\right)\\
&\quad =\beta\sum_j a_{ij}I_j\Delta t+o(\Delta t),\\
&\Pr\left(X_i(t+\Delta t)=3 \mid X_i(t)=2\right)\\
&\quad =\alpha\sum_j a_{ij}I_j\Delta t+o(\Delta t),\\
&\Pr\left(X_i(t+\Delta t)=2 \mid X_i(t)=2\right)\\
&\quad =1-\alpha\sum_j a_{ij}I_j\Delta t+o(\Delta t),\\
&\Pr\left(X_i(t+\Delta t)=0 \mid X_i(t)=0\right)\\
&\quad =1-\beta\sum_j a_{ij}I_j\Delta t+o(\Delta t),\\
&\Pr\left(X_i(t+\Delta t)=0 \mid X_i(t)=2\right)\\
&\quad =\Pr\left(X_i(t+\Delta t)=0 \mid X_i(t)=3\right)=o(\Delta t),\\
&\Pr\left(X_i(t+\Delta t)=1 \mid X_i(t)=2\right)\\
&\quad =\Pr\left(X_i(t+\Delta t)=1 \mid X_i(t)=3\right)=o(\Delta t),\\
&\Pr\left(X_i(t+\Delta t)=2 \mid X_i(t)=0\right)\\
&\quad =\Pr\left(X_i(t+\Delta t)=2 \mid X_i(t)=1\right)=o(\Delta t),\\
&\Pr\left(X_i(t+\Delta t)=3 \mid X_i(t)=0\right)\\
&\quad =\Pr\left(X_i(t+\Delta t)=3 \mid X_i(t)=1\right)=o(\Delta t).
\end{aligned}
\tag{3}
$$

Substituting these equations into the above relations and letting $\Delta t>0$, the following $4N$-dimensional dynamic system has been proposed:

$$
\begin{aligned}
&\frac{dS_i(t)}{dt}=-\beta\sum_j a_{ij}I_j(t)\cdot S_i(t)+\gamma I_i(t),\\
&\frac{dI_i(t)}{dt}=\beta\sum_j a_{ij}I_j(t)\cdot S_i(t)-\gamma I_i(t),\\
&\frac{dT_i(t)}{dt}=-\alpha\sum_j a_{ij}I_j(t)\cdot T_i(t)+\eta M_i(t),\\
&\frac{dM_i(t)}{dt}=\alpha\sum_j a_{ij}I_j(t)\cdot T_i(t)-\eta M_i(t).\\
&\qquad\qquad 1\le i\le N,
\end{aligned}
\tag{4}
$$

with the initial conditions that $0\le S_i(t), I_i(t)\le\phi$, $0\le T_i(t)$, $M_i(t)\le 1-\phi$.

According to Assumption ($H5$) that $S_i(t)+I_i(t)=\phi, T_i(t)+M_i(t)=1-\phi$, system (4) can be rewritten into the following $2N$-dimensional dynamic system:

$$
\begin{aligned}
&\frac{dI_i(t)}{dt}=\beta\sum_j a_{ij}I_j(t)\cdot\left(\phi-I_i(t)\right)-\gamma I_i(t),\\
&\frac{dM_i(t)}{dt}=\alpha\sum_j a_{ij}I_j(t)\cdot\left(1-\phi-M_i(t)\right)-\eta M_i(t),\\
&\qquad\qquad 1\le i\le N,
\end{aligned}
\tag{5}
$$

with the initial conditions $0\le I_i(t)\le\phi$, $0\le M_i(t)\le 1-\phi$.

Since the first N equations of system (5) are independent of M, so system (5) can be simplified into the following form:

$$
\begin{aligned}
&\frac{dI_i(t)}{dt}=\beta\sum_j a_{ij}I_j(t)\cdot\left(\phi-I_i(t)\right)-\gamma I_i(t),\\
&\qquad\qquad 1\le i\le N,
\end{aligned}
\tag{6}
$$

with the initial conditions $0\le I_i(t)\le\phi$.

3. Model Analysis

This section aims to understand the dynamical behavior of system (5) and system (6) which was proposed in the previous section.

Clearly, there is a unique attack-free equilibrium $P_0=(0,\cdots,0)^T_{2N\times 1}$ in system (5). First, consider properties of the attack -free equilibrium of system (5).

To achieve that, let

$$
\begin{aligned}
\Omega=\Big\{&x=\left(x_1,\ldots,x_{2N}\right)^{\mathrm{T}}\in R_+^{2N}\mid x_i\le\phi,\ x_{i+N}\le 1\\
&-\phi,\ i=1,\ldots,N\Big\}.
\end{aligned}
\tag{7}
$$

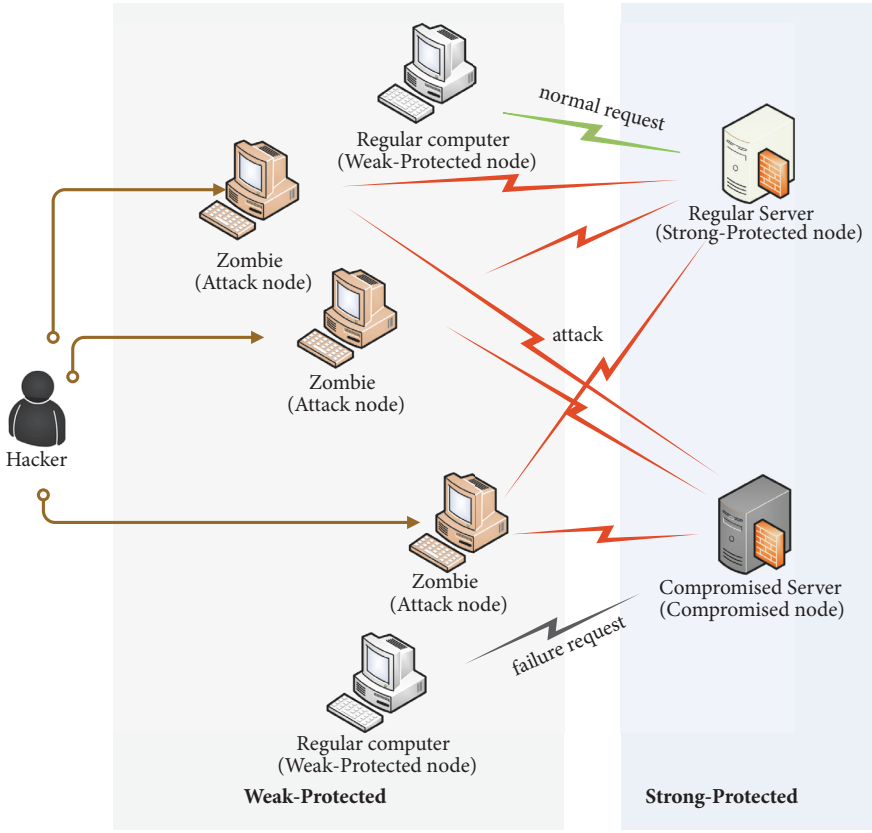

Figure 1: Schematic diagram of APDDoS attack.

Let $x(t)=(I_1(t),\ldots,I_N(t),M_1(t),\ldots,M_N(t))^{\mathrm{T}}$, and rewrite system (5) as the following notation:

$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = \mathbf{B}x(t) + \mathbf{G}(x(t)), \tag{8}$$

with the initial condition $x(0) \in \Omega$, where

$$\mathbf{B} = \begin{pmatrix} \beta\phi\mathbf{A} - \gamma\mathbf{E}_N & O_{N\times N} \\ \alpha(1-\phi)\mathbf{A} & -\eta\mathbf{E}_N \end{pmatrix},$$

$$\mathbf{G}(x(t)) = \Bigg(-\beta I_1(t)\sum_j a_{ij}I_j(t), \ldots, -\beta I_N(t)\sum_j a_{ij}I_j(t), -\alpha M_1(t)\sum_j a_{ij}I_j(t), \ldots, -\alpha M_N(t)\sum_j a_{ij}I_j(t) \Bigg). \tag{9}$$

Let

$$R_0 = \frac{\gamma}{\beta\phi}. \tag{10}$$

Theorem 1. *Consider system (5) that*

(a) *the attack-free equilibrium P_0 is locally asymptotically stable if $\lambda_{\max} < R_0$;*

(b) *the attack-free equilibrium P_0 is a saddle point.*

Proof. The characteristic equation with respect to P_0 is

$$\begin{aligned} &\det(\rho\mathbf{E}_{2N} - \mathbf{B}) \\ &= \det\begin{pmatrix} (\rho+\gamma)\mathbf{E}_N - \beta\phi\mathbf{A} & \mathbf{O}_{N\times N} \\ -\alpha(1-\phi)\mathbf{A} & (\rho+\eta)\mathbf{E}_N \end{pmatrix} \\ &= \det\left((\rho+\gamma)(\rho+\eta)\mathbf{E}_N - \beta\phi(\rho+\eta)\mathbf{A}\right) \\ &= (\rho+\eta)^N \det\left((\rho+\gamma)\mathbf{E}_N - \beta\phi\mathbf{A}\right) = 0. \end{aligned} \tag{11}$$

Equation (11) has negative roots $-\eta$ with multiplicity N and has $\beta\phi\lambda_k - \gamma, 1 \le k \le N$ as the remaining N roots. When $\lambda_{\max} < \gamma/\beta\phi = R_0$, then $\lambda_k - \gamma/\beta\phi \le \lambda_{\max} - \gamma/\beta\phi < 0$ for all k. So, all the roots of (11) are negative, implying that the attacked-free equilibrium of system (5) is locally asymptotically stable. Otherwise, if $\lambda_{\max} > \gamma/\beta\phi = R_0$, then the attack-free equilibrium is a saddle point.

Remark 2. This theorem can also be formulated as (a) $\lambda_{\max} < R_0 \Longrightarrow s(\mathbf{B}) < 0$, and (b) $\lambda_{\max} > R_0 \Longrightarrow s(\mathbf{B}) > 0$.

Next, study the global stability of the attack-free equilibrium of system (6).

Let

$$\Psi = \left\{ y = (y_1, \ldots, y_N)^{\mathrm{T}} \in R_+^N \mid y_i \le \phi,\ i = 1, \ldots, N \right\}. \tag{12}$$

Let $y(t)=(I_1(t), \ldots, I_N(t))^{\mathrm{T}}$, and rewrite system (6) as the following notation:

$$\frac{\mathrm{d}y(t)}{\mathrm{d}t} = \mathbf{C}y(t) + \mathbf{H}(x(t)), \tag{13}$$

with the initial condition $y(0) \in \Psi$, where

$$\mathbf{C} = \beta\phi\mathbf{A} - \gamma\mathbf{E}_N,$$

$$\mathbf{H}(y(t)) = \left(-\beta I_1(t) \sum_j a_{ij} I_j(t), \ldots, -\beta I_N(t) \sum_j a_{ij} I_j(t) \right). \tag{14}$$

Lemma 3 (see [22]). *Consider a smooth dynamical system $dy(t)/dt = g(y(t))$ that is defined at least in a compact set U. Then, U is positively invariant if for any smooth point $\boldsymbol{w}$ on ∂U, the vector $g(\boldsymbol{w})$ is tangent to or pointing into U.*

Lemma 4 (see [23, 24]). *Consider an n-dimensional autonomous system*

$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = \mathbf{D}x(t) + \mathbf{Y}(x(t)), \quad x \in D, \tag{15}$$

where Γ is a region that contains the origin, $\boldsymbol{Y}(x) \in C^1(\Gamma)$, $\lim_{x \to 0} \|\boldsymbol{Y}(x)\|/\|x\| = 0$. Suppose there is a positively invariant compact convex set $C \subset \Gamma$ that contains the origin, and a real eigenvector ω of $\boldsymbol{D}^{\mathrm{T}}$, a positive number r such that

(C1) $(x, \omega) \ge r\|x\|$ for all $x \in \Gamma$,

(C2) $(Y(x), \omega) \le 0$ for all $x \in \Gamma$,

(C3) the origin forms the largest positively invariant set that is included in the set $\{x \in C \mid (Y(x), \omega) = 0\}$.

Then we have

(1) $s(D^T) < 0$ implies that the origin is globally asymptotically stable in C,

(2) $s(D^T) > 0$ implies there exists $m > 0$ such that $x(0) \in C - \{0\}$ implies $\liminf_{t \to \infty} \|x(t)\| \ge m$.

Lemma 5. *The set of Ψ is positively invariant for system (6). That is, $y(0) \in \Psi$ implies $y(t) \in \Psi$ for all $t > 0$.*

$$T_i = \{ y \in \Psi \mid y_i = \phi,\ i = 1, \ldots, N \},$$
$$W_i = \{ y \in \Psi \mid y_i = 0,\ i = 1, \ldots, N \}, \tag{16}$$

and for i=1,...,N, T_i, W_i. We have

$$\xi_i = \left(0, \ldots, 0, \overset{i}{-1}, 0, \ldots, 0\right),$$
$$\zeta_i = \left(0, \ldots, 0, \overset{i}{1}, 0, \ldots, 0\right), \tag{17}$$

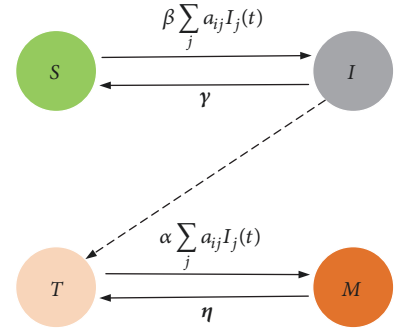

FIGURE 2: Status transition graph of the basic model (the dashed line on the graph means the attack from I-node to T-node).

as their respective outer normal vectors. Let y be a smooth point of $\partial\Psi$. The paper distinguishes among two possibilities.

$$\left(\frac{\mathrm{d}y}{\mathrm{d}t} \mid y \in T_i, \zeta_i \right) = -\gamma\phi \le 0,$$
$$\left(\frac{\mathrm{d}y}{\mathrm{d}t} \mid y \in W_i, \xi_i \right) = -\beta\phi \sum_j a_{ij} I_j(t) \le 0. \tag{18}$$

Combining the above discussions, we get that $g(\boldsymbol{w})$ is pointing into $\partial\Psi$. The claimed result then follows from Lemma 3. The proof is completed. □

Theorem 6. *The attacked-free equilibrium of system (6) is globally and asymptotically stable if $\lambda_{\max} < R_0$.*

Proof. Look at system (13). As matrix $\boldsymbol{C}^{\mathrm{T}}$ is irreducible and its off-diagonal entries are all nonnegative, it follows from [23] that $\boldsymbol{C}^{\mathrm{T}}$ has a positive eigenvector $z=(z_1, \ldots, z_N)$ belonging to its eigenvalue $s(\boldsymbol{C}^{\mathrm{T}})$. Let $r=\min_i z_i (r>0)$. Then, for all $y \in \Psi$, we have

$$\langle y, z \rangle \ge r \sum_i y_i = r \|y\|_1,$$
$$\langle H(y), z \rangle = -\beta \sum_{i=1}^{N} z_i I_i(t) \sum_j a_{ij} I_j(t) \le 0. \tag{19}$$

Moreover, $<H(y), z> = 0$ implies that y=0. In view of Theorem 1 and Lemma 5, the claimed result follows from Lemma 4. The proof is complete. □

Theorem 7. *The attacked-free equilibrium of system (5) is globally and asymptotically stable if $\lambda_{\max} < R_0$ (see Figures 2, 4, 6, and 8).*

Proof. It follows from Theorem 6, which implies that

$$\lim_{t \to \infty} I_i(t) = 0, \quad 1 \le i \le N. \tag{20}$$

for any $\varepsilon > 0$ there exists time T_1 such that, for all $t \geqslant T_1$, we have

$$I_i(t) < \varepsilon, \quad 1 \le i \le N. \tag{21}$$

From the last N equations of system (5), we get that for $1 \le i \le N$. And for $t \ge T_1$,

$$\frac{\mathrm{d}M_i(t)}{\mathrm{d}t} \le \alpha \sum_j a_{ij}\varepsilon(1-\phi) - \left(\alpha \sum_j a_{ij}\varepsilon + \eta\right) M_i(t), \quad (22)$$

As the comparison system

$$\frac{\mathrm{d}y_i(t)}{\mathrm{d}t} = \alpha \sum_j a_{ij}\varepsilon(1-\phi) - \left(\alpha \sum_j a_{ij}\varepsilon + \eta\right) y_i(t), \quad (23)$$

has a globally asymptotically stable equilibrium $\alpha \sum_j a_{ij}\varepsilon(1-\phi)/(\alpha \sum_j a_{ij}\varepsilon + \eta)$, we get that, for any $\varepsilon > 0$, there exists $T_2 > 0$ such that, for all $t \ge T_2$,

$$M_i(t) \le \frac{\alpha \sum_j a_{ij}\varepsilon(1-\phi)}{\alpha \sum_j a_{ij}\varepsilon + \eta}. \quad (24)$$

This implies that

$$\lim_{t\longrightarrow\infty} M_i(t) = 0, \quad 1 \le i \le N. \quad (25)$$

The proof is complete. □

The following corollary can be obtained easily based on Lemma 4 and Theorem 7.

Corollary 8. *System (5) is uniformly persistent if* $\lambda_{\max} > R_0$.

Second, consider properties of the attacked equilibrium of system (5).

Theorem 9. *System (5) has an attacked equilibrium* $P^* = (P_1^*, P_2^* \cdots, P_{2N}^*)^T$ *if* $\lambda_{\max} > R_0$.

Proof. Note that any solution of system (5) is bounded. Hence, the claimed result follows easily from Corollary 8 [25]. □

Theorem 10. *The attacked equilibrium* $P^* = (P_1^*, P_2^*, \ldots, P_{2N}^*)^T$ *is globally attractive if* $\lambda_{\max} > R_0$.

Proof. For any solution P(t) to system (5), let

$$F(P(t)) = \max\left\{\frac{P_k(t)}{P_k^*} : 1 \le k \le 2N\right\},$$
$$f(P(t)) = \min\left\{\frac{P_k(t)}{P_k^*} : 1 \le k \le 2N\right\}. \quad (26)$$

Clearly, $F(P(t))$, $f(P(t))$ are continuous and have right-hand derivatives. For some t_0 and $\varepsilon > 0$, we may assume $P_{k_0}(t)/{P_{k_0}}^* \ge P_k(t)/{P_k}^*, 1 \le k \le 2N, t \in [t_0, t_0+\varepsilon]$, then

$$F'(P(t)) \coloneqq \lim_{h\longrightarrow 0^+} \sup \frac{F(P(t+h)) - F(P(t))}{h} = \frac{{P'}_{k_0}}{P_{k_0}^*}, \quad t \in [t_0, t_0+\varepsilon]. \quad (27)$$

If $F(P(t_0)) > 1$, then $P_{k_0}(t) > P_{k_0}^*$.
When $1 < k < N$,

$$\begin{aligned} &P_{k_0}^* \frac{{P'}_{k_0}(t_0)}{P_{k_0}(t_0)} \\ &= \frac{P_{k_0}^*}{P_{k_0}(t_0)} \left\{\beta \sum_{j=1}^{N} \alpha_{k_0 j} P_k(t_0)\left(\phi - P_{k_0}(t)\right) - \gamma P_{k_0}(t_0)\right\} \le \frac{P_{k_0}^*}{P_{k_0}(t_0)} \beta \sum_{j=1}^{N} \alpha_{k_0 j} P_j^* \frac{P_k(t_0)}{P_{k_0}^*}\left(\phi - P_{k_0}(t)\right) - \gamma P_k^*(t_0) \le \frac{P_{k_0}^*}{P_{k_0}(t_0)} \beta \sum_{j=1}^{N} \alpha_{k_0 j} P_j^* \\ &\cdot \frac{P_k(t_0)}{P_{k_0}^*}\left(\phi - {P_{k_0}}^*\right) - \gamma P_k^*(t_0) \le \beta \sum_{j=1}^{N} \alpha_{k_0 j} P_j^*\left(\phi - {P_{k_0}}^*\right) - \gamma P_k^*(t_0) = 0. \end{aligned} \quad (28)$$

When $N < k < 2N$,

$$\begin{aligned} &P_{k_0}^* \frac{{P'}_{k_0}(t_0)}{P_{k_0}(t_0)} \\ &= \frac{P_{k_0}^*}{P_{k_0}(t_0)} \left\{\alpha \sum_{j=1}^{N} \alpha_{k_0 j} P_{k-N}(t_0)\left(1 - \phi - P_{k_0}(t)\right) - \eta P_{k_0}(t_0)\right\} \le \frac{P_{k_0}^*}{P_{k-N}(t_0)} \alpha \sum_{j=1}^{N} \alpha_{k_0 j} P_k^* \frac{P_{k-N}(t_0)}{P_{k_0}^*}\left(1 - \phi - P_{k_0}(t)\right) - \eta P_k^*(t_0) \le \frac{P_{k_0}^*}{P_{k-N}(t_0)} \alpha \sum_{j=1}^{N} \alpha_{k_0 j} P_k^* \\ &\cdot \frac{P_{k-N}(t_0)}{P_{k_0}^*}\left(1 - \phi - {P_{k_0}}^*\right) - \eta P_k^*(t_0) \le \alpha \sum_{j=1}^{N} \alpha_{k_0 j} P_k^*\left(1 - \phi - P_{k_0}(t)\right) - \eta P_k^*(t_0) = 0. \end{aligned} \quad (29)$$

As $P_{j_0}^*$, $P_{j_0}(t) > 0$, we know that $P'(t) < 0$, implying $F'(P(t_0)) < 0$. Likewise, $F(P(t_0)) = 1$ implies $F'(P(t_0)) \le 0$; $f(P(t_0)) \le 1$ implies $f'(P(t_0)) > 0$, and $f(P(t_0)) = 1$ implies $f'(P(t_0)) \ge 0$.

Let

$$U(P(t)) = \max\{F(P(t)) - 1, 0\},$$
$$V(P(t)) = \min\{1 - f(P(t)), 0\}. \quad (30)$$

Obviously, $U(P(t))$ and $V(P(t))$ are continuous and nonnegative.

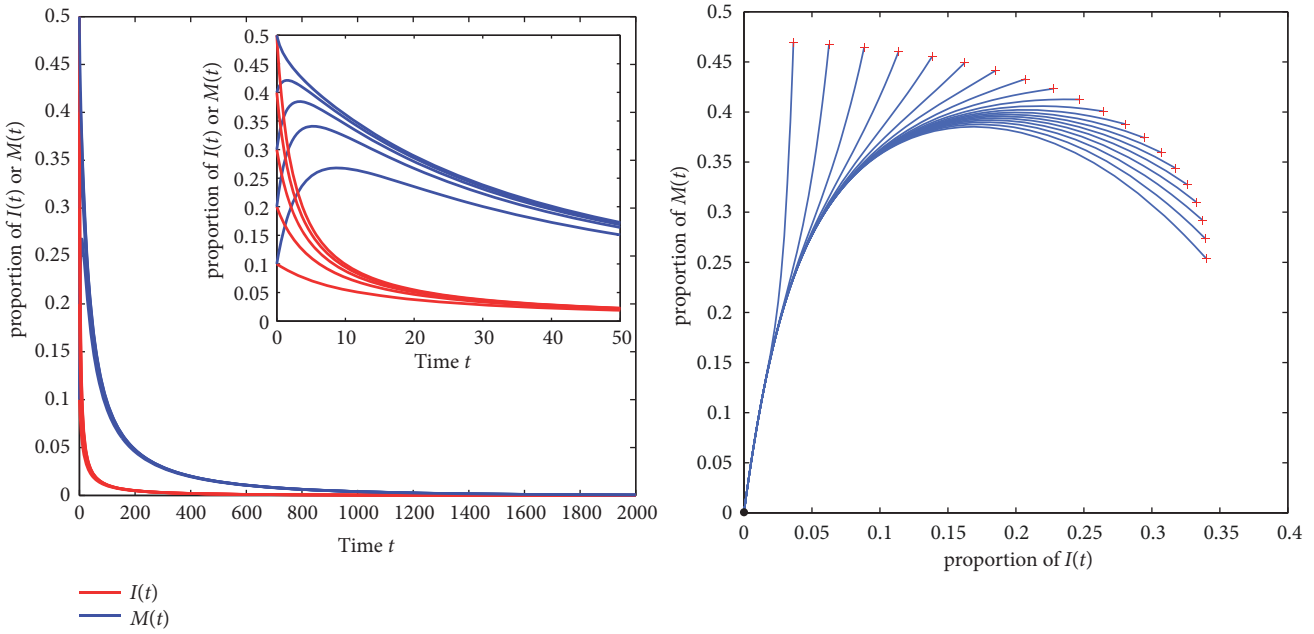

Figure 3: Global stability of attack-free solution on full-connected network.

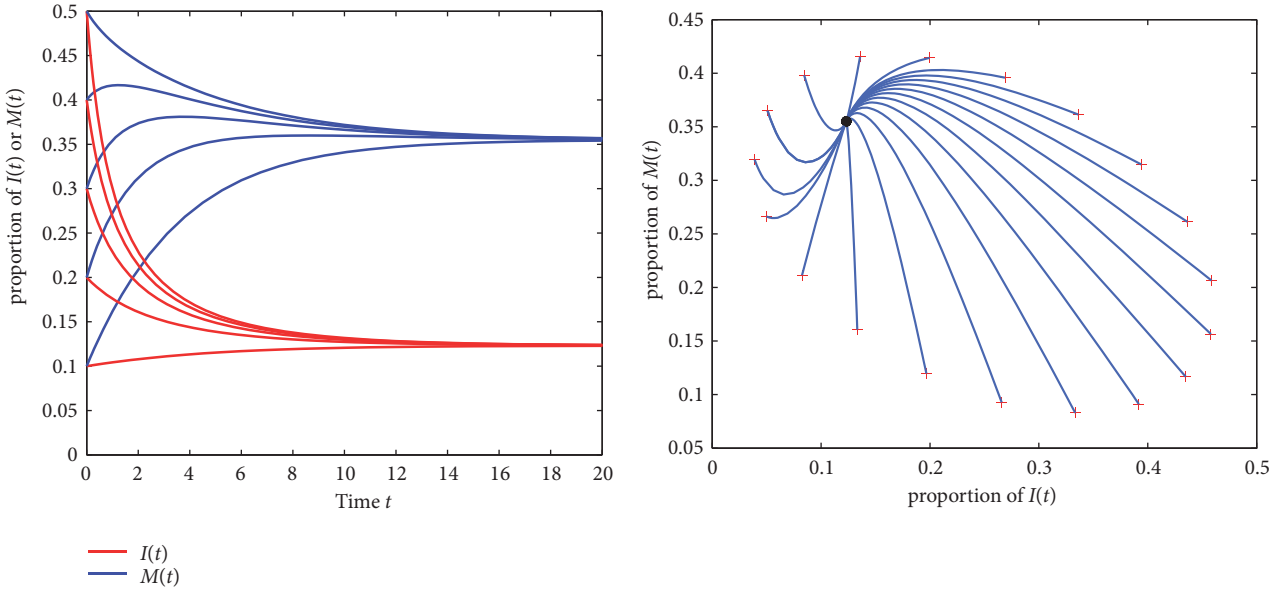

Figure 4: Global attractivity of attacked solution on full-connected network.

Besides,

$$U'(P(t)) \le 0,$$
$$V'(P(t)) \le 0. \tag{31}$$

Let

$$H_U = \left\{P(t) \in \Omega : U'(P(t)) = 0\right\},$$
$$H_V = \left\{P(t) \in \Omega : V'(P(t)) = 0\right\}. \tag{32}$$

Then

$$H_U = \left\{P(t) : 0 \le P(t) \le P_j^*\right\} \cup \{0\},$$
$$H_V = \{P(t) : 0 \le P(t) \le 1\} \cup \{0\}. \tag{33}$$

Any solution of system (5) starting in Ω approaches $H_U \cap H_V = \{P^*\} \cup \{0\}$ follows from the LaSalle Invariance Principle [26]. Therefore, the claimed follows from ${P_j}^* > 0$ is globally attractive. □

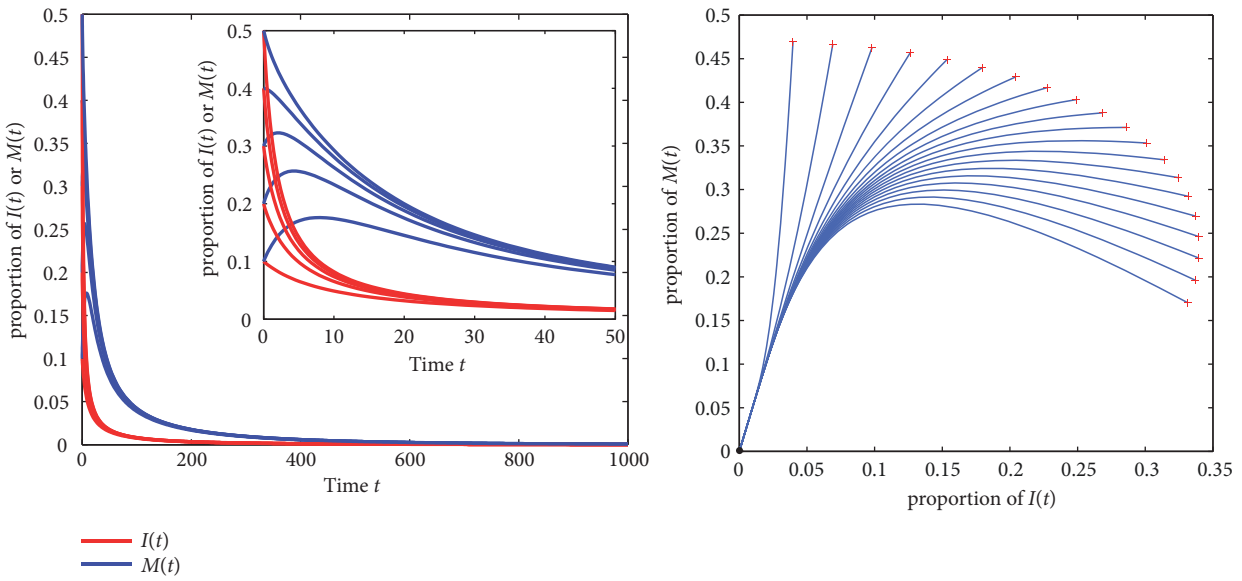

Figure 5: Global stability of attack-free solution on stochastic network.

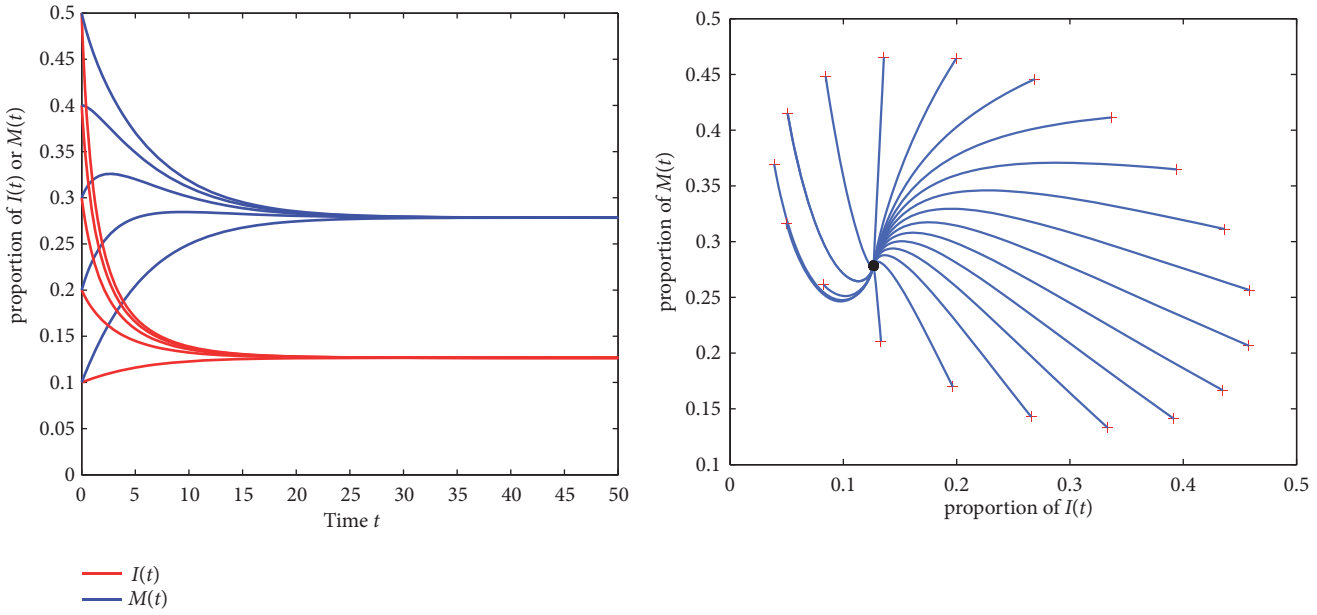

Figure 6: Global stability of attack-free solution on stochastic network.

Conjecture 11. *The attacked equilibrium* $P^* = (P_1^*, P_2^* \cdots, P_{2N}^*)^T$ *is globally asymptotically stable if* $\lambda_{\max} > R_0$.

4. Further Discussions

In order to control APDDoS attack, $\lambda_{\max} < R_0$ must be satisfied. To different parameters on R_0. Let us do the following calculations:

$$\frac{\partial R_0}{\partial \gamma} = \frac{1}{\beta\phi} > 0,$$

$$\frac{\partial R_0}{\partial \beta} = -\frac{\gamma}{\beta^2\phi} < 0,$$
$$\frac{\partial R_0}{\partial \phi} = -\frac{\gamma}{\beta^2\phi} < 0. \tag{34}$$

From these computational results, the following conclusions can be got:

(a) Reducing the infection rate β could be help to control APDDoS attack.

(b) Raising the cure rate γ conduces to the suppression of APDDoS attack.

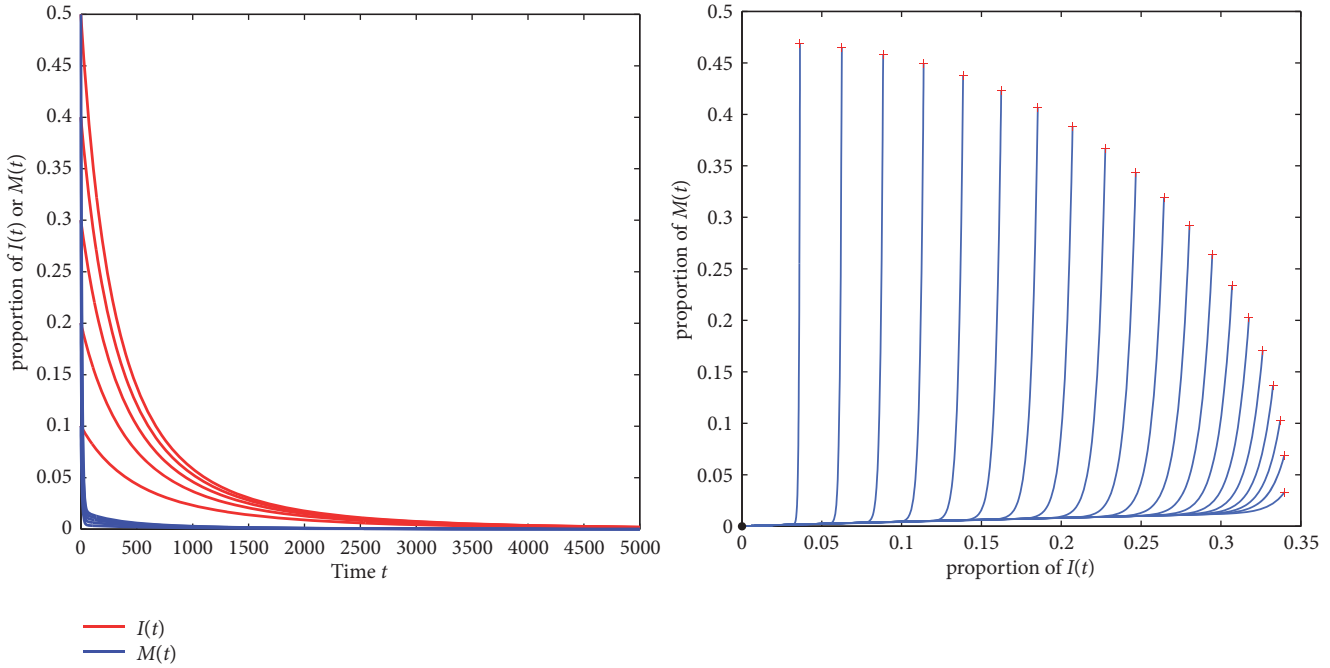

Figure 7: Global stability of attack-free solution on scale-free network.

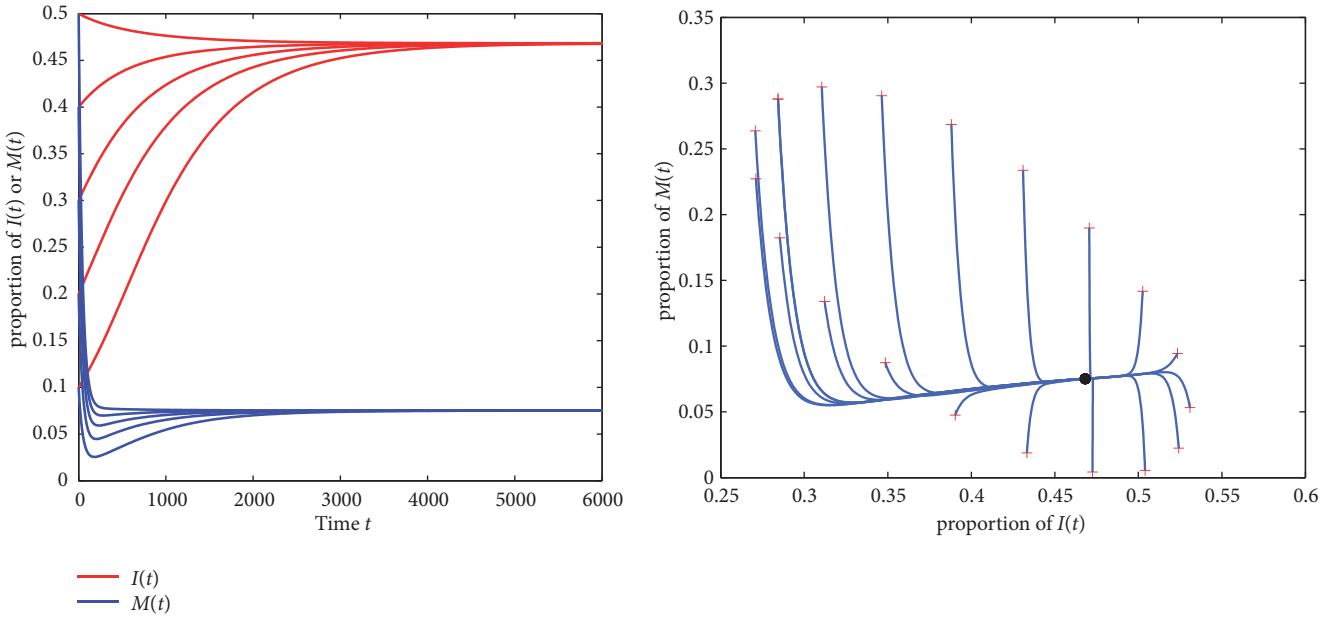

Figure 8: Global stability of attack-free solution on scale-free network.

(c) Reducing the rate ϕ conduces to the suppression of APDDoS attack.

(d) Reducing the value of $\lambda_{\max}$ leads to the restraint of APDDoS attack.

Based on the above discussions, the corresponding practical suggestions are as follows:

(i) Install antivirus software or firewall and update it regularly.

(ii) Improve the defensive level of computer.

(iii) Filter IP addresses so as to reduce the number of IP addresses that can access computer on networks.

5. Numerical Simulations

This section gives some examples about equilibriums of system (5) under the distinguish networks and optimal dynamic control strategies for disrupting APDDoS attack.

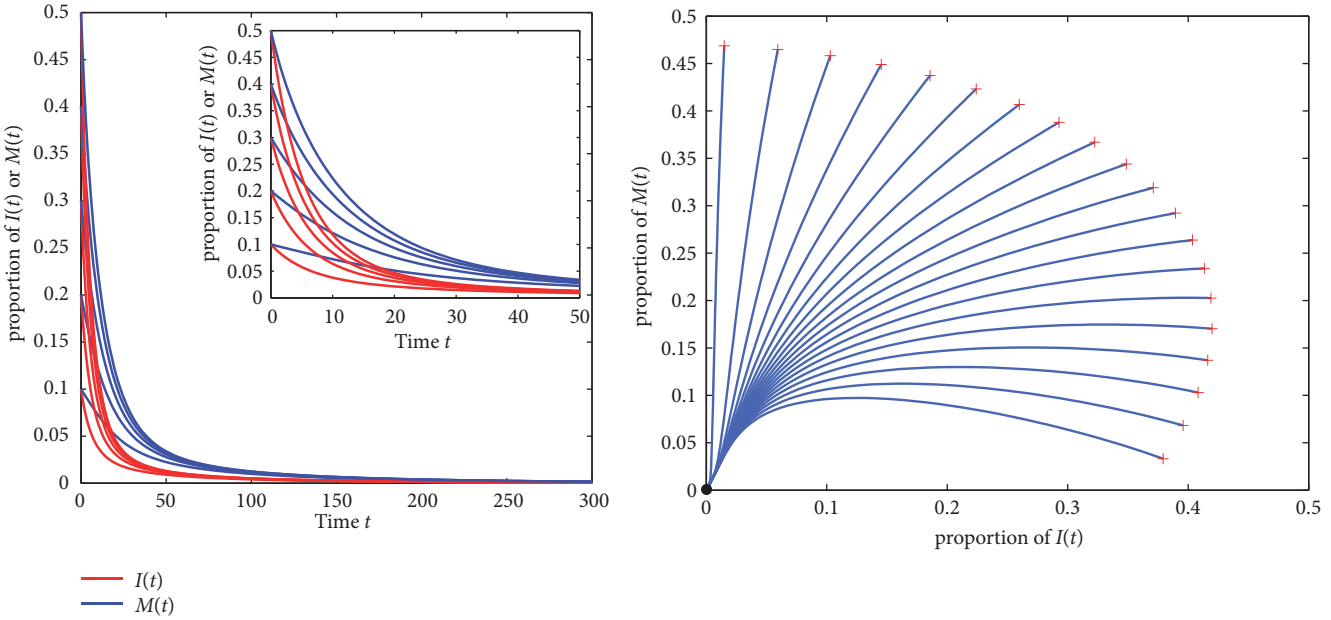

Figure 9: Global stability of attack-free solution on realistic network.

The paper discusses the equilibrium of system on four different kinds of networks: full-connected network, stochastic network, scale-free network which uses Barabasi-Albert method, and realistic network.

First, consider system (5) under the fully connected network.

Example 1. Consider a network with 200 nodes and every node is connected to other nodes, which is full-connected network. With β= 0.004, α= 0.01, γ= 0.4, η=0.1, ϕ=0.5 where the threshold of the system is 200 > $\lambda_{\max}$ =199, the attack-free equilibrium is globally stable (see Figure 3).

Example 2. Consider a network that nodes are fully connected to other with 200 nodes. With β= 0.01, α = 0.01, γ = 0.75, η =0.1, ϕ=0.5 where the threshold of the system is 150 < $\lambda_{\max}$ = 199, the attacked equilibrium is attractivity (see Figure 4).

Then consider system (5) under the network of stochastic network.

Example 3. Consider a network that nodes are connected randomly to other with 200 nodes. With β= 0.01, α= 0.01, γ= 0.5, η=0.1, ϕ=0.5 where the threshold of the system is 100 > $\lambda_{\max}$ = 99.305, the attack-free equilibrium is globally stable (see Figure 5).

Example 4. Consider a network whose nodes are connected randomly to other with 200 nodes. With β = 0.017, α= 0.01, γ= 0.75, η=0.1, ϕ=0.5 where the threshold of the system is 74.117 < $\lambda_{\max}$ = 99.305, the attacked equilibrium is attractivity (see Figure 6).

Now, let us consider system (5) under the network of scale-free network.

Example 5. Consider a network whose nodes are connected to other with 200 nodes. With β = 0.001, α= 0.002, γ= 0.0035, η=0.1, ϕ=0.5 where the threshold of the system is 7.0 > $\lambda_{\max}$ = 5.894, the attack-free equilibrium is globally stable(see Figure 7).

Example 6. Consider a network whose nodes are connected to other with 200 nodes. With β = 0.001, α= 0.002, γ= 0.0026, η=0.1, ϕ=0.5 where the threshold of the system is 5.2 < $\lambda_{\max}$ = 5.894, the attacked equilibrium is attractivity(see Figure 8).

Finally, consider system (5) under realistic network [27].

Example 7. Consider a network whose nodes are connected to other with 300 nodes. With β = 0.01, α= 0.013, γ= 0.18, η=0.1, ϕ =0.5 where the threshold of the system is 36.0 > $\lambda_{\max}$ = 34.4732, the attack-free equilibrium is globally stable(see Figure 9).

Example 8. Consider a network that nodes are connected randomly to other with 300 nodes. With β = 0.01, α= 0.013, γ= 0.05, η=0.1, ϕ =0.5 where the threshold of the system is 10.0 < $\lambda_{\max}$ = 34.4732, the attacked equilibrium is attractivity(see Figure 10).

6. Conclusion

This paper puts forward a novel dynamical model of APDDoS attack on networks. Then, a systematic analysis of this model is showed. After that, a new sufficient condition for the

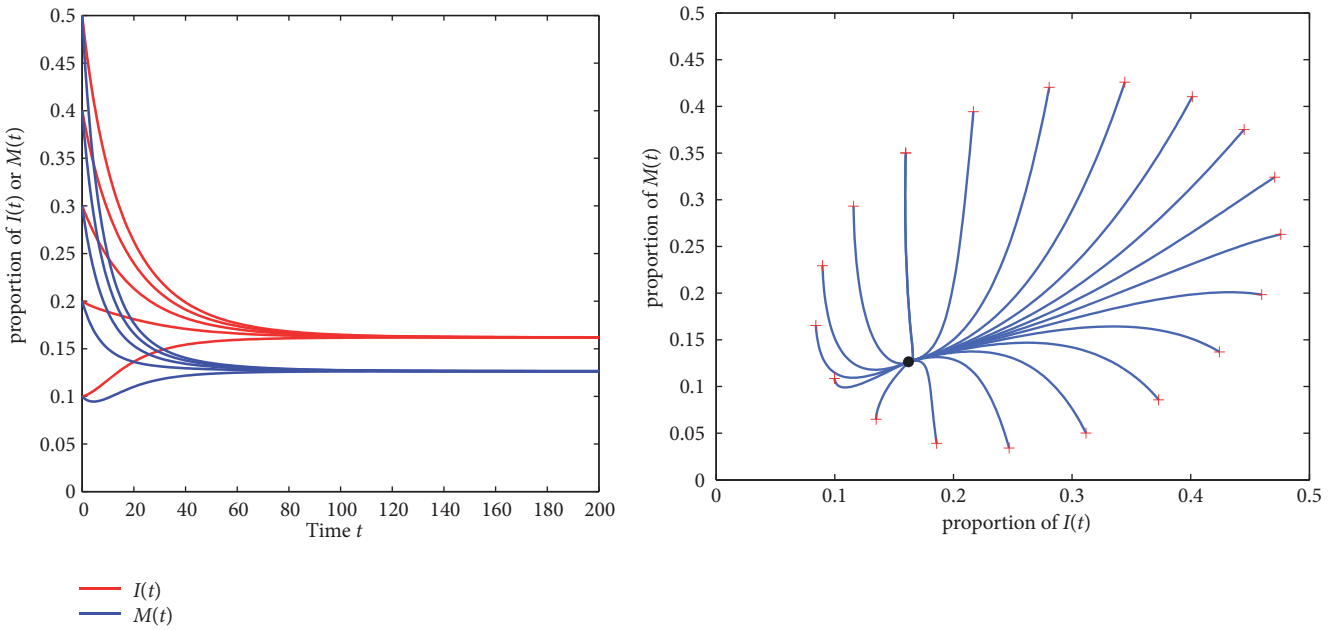

Figure 10: Global stability of attack-free solution on realistic network.

global stability of attack-free equilibrium is obtained. Next, the sufficient condition for the global attractivity of attacked equilibrium also is studied. Eventually, some numerical simulations are given to show the main results of this paper.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the Natural Science Foundation of Guangdong Province, China (no. 2014A030310239).

References

[1] http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics.

[2] A. Hussain, J. Heidemann, and C. Papadopoulos, "A framework for classifying denial of service attacks," in *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '03)*, ACM, Karlsruhe, Germany, August 2003.

[3] https://www.cybereason.com/blog/advanced-persistent-threat-apt.

[4] https://en.wikipedia.org/wiki/Denial-of-service_attack#Advanced_persistent_DoS.

[5] https://www.difesaesicurezza.com/en/defence-and-security/new-cyber-attack-hit-2018-winter-olympics-pyeongchang-likely-ddos/.

[6] https://githubengineering.com/ddos-incident-report/.

[7] P. V. Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 1–14, 2009.

[8] P. V. Mieghem and E. Cator, "Epidemics in networks with nodal self-infection and the epidemic threshold," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 86, no. 1, Article ID 016116, 2012.

[9] R. Pastor-Satorras, C. Castellano, P. Van Mieghem, and A. Vespignani, "Epidemic processes in complex networks," *Reviews of Modern Physics*, vol. 87, no. 3, pp. 120–131, 2015.

[10] Z.-K. Zhang, C. Liu, X.-X. Zhan, X. Lu, C.-X. Zhang, and Y.-C. Zhang, "Dynamics of information diffusion and its applications on complex networks," *Physics Reports*, vol. 651, pp. 1–34, 2016.

[11] M. Youssef and C. Scoglio, "An individual-based approach to SIR epidemics in contact networks," *Journal of Theoretical Biology*, vol. 283, pp. 136–144, 2011.

[12] S. Xu, W. Lu, and L. Xu, "Push- and pull-based epidemic spreading in networks: Thresholds and deeper insights," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 7, no. 3, Article ID 2348835, pp. 1–26, 2012.

[13] L. X. Yang, M. Draief, and X. Yang, "Heterogeneous virus propagation in networks: a theoretical study," *Mathematical Methods in the Applied Sciences*, vol. 40, no. 5, pp. 1396–1413, 2017.

[14] L.-X. Yang, X. Yang, and Y. Yan Tang, "A bi-virus competing spreading model with generic infection rates," *IEEE Transactions on Network Science and Engineering*, vol. 5, no. 1, pp. 2–13, 2017.

[15] C. Zhang, T. Feng, Y. Zhao, and G. Jiang, "A new model for capturing the spread of computer viruses on complex-networks," *Discrete Dynamics in Nature and Society*, Article ID 956893, 9 pages, 2013.

[16] L.-X. Yang and X.-F. Yang, "The spread of computer viruses over a reduced scale-free network," *Physica A: Statistical Mechanics and its Applications*, vol. 396, pp. 173–184, 2014.

[17] C. Zhang and H. Huang, "Optimal control strategy for a novel computer virus propagation model on scale-free networks," *Physica A: Statistical Mechanics and its Applications*, vol. 451, pp. 251–265, 2016.

[18] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 343–359, Oakland, Calif, USA, May 1991.

[19] B. K. Mishra and S. K. Pandey, "Dynamic model of worm s with vertical transmission in computer network," *Applied Mathematics and Computation*, vol. 217, no. 21, pp. 8438–8446, 2011.

[20] J. Ren, X. Yang, Q. Zhu, L. Yang, and C. Zhang, "A novel computer virus model and its dynamics," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 1, pp. 376–384, 2012.

[21] C. Gan and X. Yang, "Theoretical and experimental analysis of the impacts of removable storage media and antivirus software on viral spread," *Communications in Nonlinear Science and Numerical Simulation*, vol. 22, no. 1-3, pp. 167–174, 2015.

[22] J. A. Yorke, "Invariance for ordinary differential equations," *Mathematical Systems Theory*, vol. 1, no. 4, pp. 353–372, 1967.

[23] A. Lajmanovich and J. A. Yorke, "A deterministic model for gonorrhea in a nonhomogeneous population," *Mathematical Biosciences*, vol. 28, no. 3-4, pp. 221–236, 1976.

[24] C. Gan, "Modeling and analysis of the effect of network eigenvalue on viral spread," *Nonlinear Dynamics*, vol. 84, no. 3, pp. 1727–1733, 2016.

[25] H. L. Smith and P. Waltman, *The Theory of the Chemostat*, Cambridge University Press, Cambridge, UK, 1995.

[26] R. C. Robinson, *An Introduction to Dynamical Systems: Continuous and Discrete*, Prentice Hall, Englewood Cliffs, 2004.

[27] L.-X. Yang, X. Yang, and Y. Wu, "The impact of patch forwarding on the prevalence of computer virus: a theoretical assessment approach," *Applied Mathematical Modelling*, vol. 43, pp. 110–125, 2017.