Research Article

Stability Analysis of an Advanced Persistent Distributed Denial-of-Service Attack Dynamical Model

Chunming Zhang and Jingwei Xiao

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

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

Received 27 December 2017; Accepted 22 April 2018; Published 24 May 2018

Academic Editor: Angel M. Del Rey

Copyright © 2018 Chunming Zhang and Jingwei Xiao. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The advanced persistent distributed denial-of-service (APDDoS) attack is a fairly significant threat to cybersecurity. Formulating a mathematical model for accurate prediction of APDDoS attack is important. However, the dynamical model of APDDoS attack has barely been reported. This paper first proposes a novel dynamical model of APDDoS attack to understand the mechanisms of APDDoS attack. Then, the attacked threshold of this model is calculated. The global stability of attack-free and attacked equilibrium are both proved. The influences of the model's parameters on attacked equilibrium are discussed. Eventually, the main conclusions of the theoretical analysis are examined through computer simulations.

1. Introduction

Cyberattack has already become one of the greatest threats to cybersecurity [1–4]. With the rapid development of information technologies, a considerable number of cyberattack methods have been emerging in the past few decades, such as SQL injection (SQLi) attack, distributed denial-of-service (DDoS) attack, targeted attack, and account hijackings [5]. In particular, DDoS attack has become one of the most popular methods of hackers due to its strong covertness and low cost. Recently, several cases have been widely reported; for instance, in November, 2016, five Russian banks have suffered a persistent DDoS attack for almost 12 hours, which caused unnumbered economic losses and social turbulence [6]. What is more, in August, 2017, Ukraine's national postal service has been hit by a two-day-long cyberattack [7].

Denial-of-service attack (DoS attack) is a cyberattack, where the attackers attempt to disrupt the servers which are going to respond to the requests. When these attacks of DoS attack originate from many different computers and networks, this attack mode can be referred to as distributed denial-of-service attack (DDoS attack). On the other hand, the dynamical models of advanced persistent threats (APTs) have already attracted the attention of researchers [8–12]. An

advanced persistent threat is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity [13]. The computers with defensive ability in network cannot be successfully attacked easily by a standard DDoS attack (only DDoS attack once), which means that a standard DDoS attack does little harm to the network. But nowadays, there are numerous hackers with clear aim, well resource, and exceptional skills. Therefore, they are able to launch continuous and long-term attack, which is also called APDDoS attack in this paper. In this way, attackers of APDDoS attack would cause a bigger threat to cybersecurity [14].

Although the APDDoS attack has been mentioned in numerous papers [15–18], the dynamical models of APDDoS attack have rarely been reported yet. In this context, this paper proposes a dynamical model of APDDoS attack, which can help to figure out the mechanism of APDDoS attack.

In reality, different computer has different defensive ability. For example, the computer with low level of defensive ability is more likely to be attacked, while the high level of defensive ability makes the computer not be totally affected easily, so that the flooding attack is the only one way to attack the high-defensive computer. Hence, this paper divides the computers into two parts which are weak-defensive

FIGURE 1: Schematic diagram of APDDoS attack.

computers and strong-defensive computers. Meanwhile, the procedures of APDDoS attack can be typically classified into two phases, including spreading computer worms and launching flooding attacks (see Figure 1).

(1) *Spreading Computer Worms.* As to infect more computers with low level of defensive ability, hackers are attempting to spread more computer worms on networks (such as Internet and WWW) by sending fake and malicious emails or links, which are going to lure people to click on them and thus lead them to visit virus websites and then download malware unconsciously. So, zombie in here is used to denote the infected computer or an infectious local network. Then, worms can also be diffused through the zombie to its neighbors under the control of the hackers.

(2) *Launching Flooding Attacks.* After successfully intruding the computer and gaining the control of zombies, the hackers will send instructions to the zombies so as to launch APDDoS attacks to computers with extraordinary high-defensive levels. Owing to the strong disruptive power of

APDDoS attacks, some high-defensive computers will still be intruded and broken down. So, compromised computer is utilizing to represent the high-defensive computer, which has been broken down.

The rest of this paper is organized as follows. In Section 2, a dynamical model of APDDoS attack is proposed; then the model is analyzed in Section 3; some further discussions are provided in Section 4; finally, the summary of this paper is given in Section 5.

2. Model Description

This paper makes the hypothesis that computers can be classified into two parts: weak-defensive computers and strong-defensive computers.

The weak-defensive computers consist of two groups, weak-defensive nodes (not infected yet) and attacked nodes.

(i) *Weak-defensive node,* which has not been infected by worms or malwares yet, lacks in defending the malicious attacks, for existing some system vulnerabilities and device

defects or being without the defense of antivirus software. It is also called W node for short.

(ii) Attack node, the zombie that can infect other W nodes and launch attacks controlled by hackers, can be also represented by A node briefly.

The strong-defensive computers also can be divided into two groups, strong-defensive nodes (not compromised yet) and compromised nodes.

(i) Strong-defensive node, which provides considerable power of filtering and self-defensive ability, represents the computer with firewall equipped. In general, strong-defensive node acts as server in the network, and it is also called S node in this paper.

(ii) Compromised node, which denotes the state that S node becomes compromised and cannot respond to the requests after the attacks, is called C node in this paper.

Based on the above facts, the following assumptions can be obtained.

(H1) The system is closed; the total number of systems is constant. Hence, $W(t) + A(t) + S(t) + C(t) \equiv 1$.

(H2) Due to opening the phishing emails or text or performing some operations which would damage system security, W node is infected with the probability of β .

(H3) Due to executing some positive measures, like reinstalling operation system, A node recovers with the probability of γ .

(H4) Due to the APDDoS attacks, S node is compromised with the probability of α .

(H5) With the assistance of firewall, p , used to describe the self-protection ability of S node, represents the ability of resisting attack of APDDoS. And $1/p$ should be proportional to the rate that S node compromised. Besides, p must be greater than 1.

(H6) Due to some positive measures, like restarting the computer, C node turns to an S node with the probability of η .

(H7) As the system is divided into two separated parts, the parameters ϕ and $1 - \phi$ are used to, respectively, denote the rate of the weak part and the strong part. So the following equations hold, $\phi = W(t) + A(t)$ and $1 - \phi = S(t) + C(t)$.

According to (H1)–(H7), the following dynamical system is got (see Figure 2).

$$\begin{aligned} \frac{dW(t)}{dt} &= -\beta W(t) A(t) + \gamma A(t), \\ \frac{dA(t)}{dt} &= \beta W A(t) - \gamma A(t), \\ \frac{dS(t)}{dt} &= -\frac{\alpha S(t) A(t)}{p} + \eta C(t), \\ \frac{dC(t)}{dt} &= \frac{\alpha S(t) A(t)}{p} - \eta C(t), \end{aligned} \quad (1)$$

where $0 \leq W(t), A(t) \leq \phi$, $0 \leq S(t), C(t) \leq 1 - \phi$, and $0 \leq \alpha, \beta, \gamma, \eta, p \leq 1$.

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

3. Theoretical Analysis of the Dynamical Model

This section focuses on the mathematical properties of the dynamical model, such as equilibriums, threshold, and the local and global stability of system (1).

As $W(t) + A(t) = \phi$ and $S(t) + C(t) = 1 - \phi$, the equations of system (1) can be deduced into a two-dimensional system as follows:

$$\begin{aligned} \frac{dA(t)}{dt} &= \beta (\phi - A(t)) A(t) - \gamma A(t), \\ \frac{dC(t)}{dt} &= \frac{\alpha (1 - \phi - C(t)) A(t)}{p} - \eta C(t), \end{aligned} \quad (2)$$

where $0 \leq A(t) \leq \phi \leq 1$ and $0 \leq C(t) \leq 1 - \phi \leq 1$. The simply connected compact set can be obtained that $\Omega = \{(A(t), C(t)) \in R_+^2 : A(t) \in [0, \phi], C(t) \in [0, 1 - \phi]\}$.

Since system (1) and system (2) are equivalent, we are going to examine the properties of system (2).

3.1. Equilibriums

Theorem 1. System (2) has a unique attack-free equilibrium E_0 .

Proof. Letting $A(t) = A_0 = 0$ and $C(t) = C_0 = 0$, then the unique attack-free equilibrium E_0 is shown as follows:

$$E_0 = (A_0, C_0)^T = (0, 0)^T. \quad (3)$$

□

Theorem 2. System (2) has a unique attack-free equilibrium:

$$E^* = (A^*, C^*) = \left(\phi - \frac{\gamma}{\beta}, \frac{\alpha (1 - \phi) (\beta \phi - \gamma)}{p \beta \eta + \alpha (\beta \phi - \gamma)} \right). \quad (4)$$

It is easy to prove, so the proof has been omitted here.

3.2. Attacked Threshold. In this paper, propagation threshold is a vital indicator that determines whether system will suffer APDDoS attack.

According to method described in Appendix, there are four statuses in system (1), so let

$$x = (x_1, x_2, x_3, x_4)^T = (A(t), C(t), W(t), S(t))^T, \quad (5)$$

and the following vectors can be obtained that

$$F(x) = \begin{bmatrix} \beta x_1 x_3 \\ \frac{\alpha}{p} x_1 x_4 \\ 0 \\ 0 \end{bmatrix},$$

$$V^- = \begin{bmatrix} \gamma x_1 \\ \eta x_2 \\ \beta x_1 x_3 \\ \frac{\alpha}{p} x_1 x_4 \end{bmatrix}, \quad (6)$$

$$V^+ = \begin{bmatrix} 0 \\ 0 \\ \gamma x_1 \\ \eta x_2 \end{bmatrix},$$

which satisfies E_0 where $x_1^* = 0$, $x_2^* = 0$, $x_3^* = \phi$, $x_4^* = 1 - \phi$. So

$$F = \begin{pmatrix} \beta x_3 & 0 \\ \frac{\alpha}{p} x_4 & 0 \end{pmatrix}, \quad (7)$$

$$V = \begin{pmatrix} \gamma & 0 \\ 0 & \eta \end{pmatrix}.$$

Then $R_0 = \rho(FV^{-1}) = \phi\beta/\gamma$, where R_0 is strictly increasing with respect to the parameters ϕ and β and strictly decreasing with respect to γ .

Example 3. Fixing $\gamma = 0.3$ and changing the parameters β and ϕ , the value of R_0 is shown in Figure 3.

Example 4. Fixing the $\beta = 0.3$ and varying the parameters γ and ϕ , the value of R_0 is shown in Figure 4.

3.3. The Global Stability of Attack-Free Equilibrium

Theorem 5. E_0 is globally asymptotically stable when $R_0 < 1$.

Proof. Consider the following Lyapunov function with an undermined coefficient

$$V(A(t), C(t)) = A(t) + \frac{1}{2}\kappa C(t)^2, \quad (8)$$

FIGURE 3: Example 3.

FIGURE 4: Example 4.

where κ is a positive constant to be determined. Besides, $A(t) \geq 0$ and $C(t) \geq 0$, so V is nonnegative.

The time derivative of V along an orbit of system (2) is

$$\begin{aligned} \frac{dV}{dt} &= A' + \kappa C C' \\ &= \beta(\phi - A)A - \gamma A \\ &\quad + \kappa C \left[\frac{\alpha(1 - \phi - C)}{p} A - \eta C \right] \\ &= (\beta\phi - \gamma)A - \beta \left[A^2 - \kappa \frac{\alpha(1 - \phi)}{p\beta} CA + \frac{\kappa\eta}{\beta} C^2 \right] \\ &\quad - \frac{\alpha\kappa}{p} AC^2. \end{aligned} \quad (9)$$

FIGURE 5: (a) and (b) represent the variety of the proportion of $C(t)$ and $A(t)$ in different initial conditions by time-varying diagram and phase diagram, respectively.

As $R_0 = \phi\beta/\gamma < 1$, then $\beta\phi - \gamma < 0$ and $(\beta\phi - \gamma)A(t) \leq 0$ are obtained. And another part, $\beta[A^2 - \kappa(\alpha(1 - \phi)/p\beta)CA + (\kappa\eta/\beta)C^2]$, can be deduced into

$$\begin{aligned} & \beta \left(A - \frac{\kappa\alpha(1 - \phi)}{2p\beta} C \right)^2 \\ & - \beta \left[\left(\frac{\kappa\alpha(1 - \phi)}{2p\beta} \right)^2 - \frac{\kappa\eta}{\beta} \right] C^2. \end{aligned} \quad (10)$$

Obviously, $\beta(A - (\kappa\alpha(1 - \phi)/2p\beta)C)^2 \geq 0$. When

$$\left(\frac{\kappa\alpha(1 - \phi)}{2p\beta} \right)^2 - \frac{\kappa\eta}{\beta} \leq 0, \quad (11)$$

then the inequality $\beta[A^2 - \kappa(\alpha(1 - \phi)/p\beta)CA + (\kappa\eta/\beta)C^2] \geq 0$ holds.

Considering inequality (11), let $\kappa = 4\eta p^2/\alpha^2(1 - \phi)^2 > 0$, so $(\kappa\alpha(1 - \phi)/2p\beta)^2 - \kappa\eta/\beta = 0$. Finally, the remaining part, $(\alpha\kappa/p)AC^2$, is nonnegative, for $\kappa > 0$. Hence, only if $A(t) = C(t) = 0$, that $(A(t), C(t))^T \in E_0$, $dV/dt = 0$. $dV/dt < 0$, when $(A(t), C(t))^T \in \Omega - E_0$. The result confirms the stability principle in [19].

The proof is completed. $\square$

Example 6. In system (2) with $\alpha = 0.1$, $\gamma = 0.37$, $\eta = 0.05$, $\beta = 0.65$, $\phi = 0.5$, $p = 1.2$, where $R_0 = 0.8784 < 1$, computers will not suffer from APDDoS attacks and the attack-free equilibrium is globally asymptotically stable (see Figure 5).

3.4. The Global Stability of Attacked Equilibrium. Firstly, the local stability of attacked equilibrium of system (2) will be demonstrated.

Lemma 7. E^* is locally asymptotically stable when $R_0 > 1$.

Proof. The Jacobian of the linearized system (2) evaluated at E^* is as follows:

$$J = \begin{pmatrix} \beta\phi - 2\beta A^* - \gamma & 0 \\ -\frac{\alpha(1 - \phi - C^*)}{p} & -\left(\frac{\alpha A^*}{p} + \eta\right) \end{pmatrix}, \quad (12)$$

and the corresponding characteristic equation is

$$[\lambda - (\beta\phi - 2\beta A^* - \gamma)] \left[\lambda + \left(\frac{\alpha A^*}{p} + \eta \right) \right] = 0. \quad (13)$$

Clearly, two roots of (13) are $\lambda_1 = -\alpha A^*/p - \eta$ and $\lambda_2 = \beta\phi - 2\beta A^* - \gamma$, so the possibility of these two roots will be discussed next. As $A^* = \phi - \gamma/\beta > 0$, it is easy to get that $\lambda_1 < 0$. Besides, the equation of λ_2 can be rewritten into $\lambda_2 = -\beta\phi + \gamma$ and $\lambda_2 < -1 < 0$, for $R_0 = \beta\phi - \gamma > 1$. Hence, the two roots of (13) both have negative real parts. Further, the conclusion of this result follows by the Lyapunov theorem, conforming to the Hurwitz criterion [19].

The proof is completed. $\square$

Second, the global behaviors of the equilibrium of E^* will be examined.

Lemma 8. The simplified system admits no periodic orbit in the interior of Ω [20].

Proof. Let

$$\begin{aligned} f_1(x) &= \beta(\phi - A(t))A(t) - \gamma A(t), \\ f_2(x) &= \frac{\alpha(1 - \phi - C(t))}{p}A(t) - \eta C(t). \end{aligned} \quad (14)$$

FIGURE 6: (a) and (b) represent the variety of proportion of $C(t)$ and $A(t)$ in different initial conditions by time-varying diagram and phase diagram, respectively.

Define $D(A, C) = 1/A$; then

$$\frac{\partial(Df_1)}{\partial L} + \frac{\partial(Df_2)}{\partial A} = -\beta - \frac{\alpha}{p} - \frac{\eta}{A} < 0. \quad (15)$$

The result follows the Bendixson–Dulac criterion [20]. $\square$

Lemma 9. *System (2) admits no periodic orbit that passes through a point on $\partial\Omega$, that is the boundary of Ω .*

Proof. As for the smoothness of all orbits of system (2), all conditions can be enumerated as follows.

(a) There is no periodic orbit that passes through a corner of Ω , i.e., either $(0, 0)$ or $(\phi, 0)$ or $(0, 1 - \phi)$, or $(\phi, 1 - \phi)$.

(b) If there is a periodic orbit passes through a noncorner point on $\partial\Omega$, then this orbit must be tangent to $\partial\Omega$ at this point. $\square$

On the contrary, suppose that there is a periodic orbit Γ that passes through a noncorner point $(\bar{A}, \bar{C})$ on $\partial\Omega$; then there are four possibilities.

Case 1. $0 < \bar{A} < \phi, \bar{C} = 0$. Then $dC/dt|_{(\bar{A}, \bar{C})} = (\alpha(1-\phi)/p)\bar{A} > 0$, implying that Γ is not tangent to $\partial\Omega$ at this point, which leads to a contradiction.

Case 2. $0 < \bar{C} < 1 - \phi, \bar{A} = 0$. Then $dA/dt|_{(\bar{A}, \bar{C})} = 0$, implying that Γ is not tangent to $\partial\Omega$ at this point, which is self-contradictory.

Case 3. $0 < \bar{A} < \phi, \bar{C} = 1 - \phi$. Then $dC/dt|_{(\bar{A}, \bar{C})} = -\eta(1-\phi) < 0$, implying that Γ is not tangent to $\partial\Omega$ at this point, which leads to a contradiction.

Case 4. $0 < \bar{C} < 1 - \phi, \bar{A} = \phi$. Then $dA/dt|_{(\bar{A}, \bar{C})} = -\phi\gamma < 0$, implying that Γ is not tangent to $\partial\Omega$ at this point, which is also a contradiction.

Theorem 10. *E^* is globally asymptotically stable when $R_0 > 1$.*

Proof. The claimed result follows by combining Lemmas 7–9 with the generalized Poincaré–Bendixson theorem [20]. $\square$

Example 11. Under system (2) with $\alpha = 0.1, \gamma = 0.2, \eta = 0.05, \beta = 0.8, \phi = 0.5, p = 1.2$, where $R_0 = 2.0$, computers in this situation will under the attack of APDDoS, and thus the attacked equilibrium E^* is globally asymptotically stable (see Figure 6).

Example 12. Under system (2) with $\alpha = 0.1, \gamma = 0.3, \eta = 0.05, \beta = 0.7, \phi = 0.5, p = 1.2$ that $R_0 = 1.1667$, computers will suffer APDDoS attack, also the attacked equilibrium E^* is globally asymptotically stable (see Figure 7).

4. Further Discussion

In this section, the impact of parameters on the attacked equilibrium E^* of system (2) will be discussed.

In Section 3, the attacked equilibrium E^* can be rewritten into

$$\begin{aligned} E^* = (A^*, C^*) &= \left(\frac{\gamma}{\beta} (R_0 - 1), \frac{\alpha\gamma(1-\phi)(R_0 - 1)}{p\beta\eta + \alpha\gamma(R_0 - 1)} \right) \\ &= \left(\phi - \frac{\gamma}{\beta}, \frac{\alpha(1-\phi)(\beta\phi - \gamma)}{p\beta\eta + \alpha(\beta\phi - \gamma)} \right). \end{aligned} \quad (16)$$

FIGURE 7: (a) and (b) represent the variety of proportion of $C(t)$ and $A(t)$ in different initial conditions by time-varying diagram and phase diagram, respectively.

By calculation,

$$\begin{aligned} C^* &= \frac{\alpha\gamma(1-\phi)(R_0-1)}{p\beta\eta + \alpha\gamma(R_0-1)} = \frac{\alpha(1-\phi)(\beta\phi-\gamma)}{p\beta\eta + \alpha(\beta\phi-\gamma)} \\ &= \frac{(1-\phi)}{p\beta\eta/\alpha(\beta\phi-\gamma) + 1}. \end{aligned} \quad (17)$$

So, it is easy to get the following conclusions:

- (1) A^* is strictly increasing with respect to parameters ϕ and β .
- (2) C^* is strictly increasing with respect to parameter α , and C^* is strictly decreasing with respect to parameters p and η .

- (3) Both of A^* and C^* are strictly decreasing with respect to parameter γ .

Now, let us consider the influence of ϕ and β on the proportion of C^* . The following relations can be gained:

$$\begin{aligned} \frac{\partial C^*}{\partial \beta} &= \alpha \frac{[\alpha(\beta\phi-\gamma) + p\beta\eta]\phi(1-\phi) - (\alpha\phi + p\eta)(1-\phi)(\beta\phi-\gamma)}{[\alpha(\beta\phi-\gamma) + p\beta\eta]^2} \quad (18) \\ &= \frac{\alpha p \eta \gamma}{[\alpha(\beta\phi-\gamma) + p\beta\eta]^2} > 0. \end{aligned}$$

Hence, C^* is strictly increasing with respect to the parameters β .

Then, focusing on the influence of ϕ , the relation between C^* and ϕ is shown as follows:

$$\frac{\partial C^*}{\partial \phi} = \frac{[\alpha(\beta\phi-\gamma) + p\beta\eta]\alpha[\beta(1-\phi) - (\beta\phi-\gamma)] - \alpha^2\beta(1-\phi)(\beta\phi-\gamma)}{[\alpha(\beta\phi-\gamma) + p\beta\eta]^2}. \quad (19)$$

So the following function has been constructed:

$$\begin{aligned} f(\phi) &= -\alpha\beta^2\phi^2 + 2(\alpha\beta\gamma - p\beta^2\eta)\phi + p\beta\eta(\beta + \gamma) \\ &\quad - \alpha\gamma^2, \end{aligned} \quad (20)$$

when ϕ is the positive root of function (20) and C^* will get its maximum or minimum.

Finally the discussion of the value of ϕ will be shown as follows.

Let Δ represent the discriminant which determines whether the function $f(\phi)$ has real root and how many it has. By definition, it is easy to get $\Delta = 4p\beta^3\eta\Lambda$, where $\Lambda = p\beta\eta + \alpha\beta - \alpha\gamma$. $f(\phi)$ exists in two real roots if $\Lambda > 0$. Let ϕ_1 and ϕ_2 ($\phi_1 \leq \phi_2$) denote the two real roots of $f(\phi)$ if $\Delta \geq 0$. Also the axis of symmetry of the function $f(\phi)$, $\gamma/\beta - p\eta/\alpha$, can be obtained easily.

FIGURE 8: Example 13.

Case 1. $\Lambda \leq 0$, which also means $p\beta\eta + \alpha\beta - \alpha\gamma < 0$, the inequality can be derived as

$$\begin{aligned} p\beta\eta + \alpha\beta - \alpha\gamma &> \beta\eta + \alpha\beta - \alpha\gamma \\ &= \beta \left(\eta + \alpha \left(1 - \frac{\gamma}{\beta} \right) \right). \end{aligned} \quad (21)$$

$\phi \in (0, 1)$ and $\phi > \gamma/\beta$ ($R_0 > 1$) infer that $\gamma/\beta < 1$, which means $\beta(\eta + \alpha(1 - \gamma/\beta)) > 0$; thus, that contradicts $p\beta\eta + \alpha\beta - \alpha\gamma < 0$. Therefore, the attacked equilibrium does not exist, and this condition is not satisfied when $R_0 > 1$.

Case 2. $\Lambda > 0$, and $\phi_1 < 0$, $\phi_2 \in (0, 1)$. Considering the positive value ϕ_2 , C^* increases with respect to ϕ when $\phi \in (0, \phi_2]$, and C^* decreases with respect to ϕ when $\phi \in (\phi_2, 1)$. So $C^*|_{\phi=\phi_2}$ is the local maximum of C^* (see Figure 8).

Case 3. $\Lambda > 0$, and $\phi_1, \phi_2 \in (0, 1)$. When $\phi \leq \phi_1$, the attacked equilibrium does not exist because $\phi_1 < \gamma/\beta - p\eta/\alpha < \gamma/\beta$ and $R_0 < 1$. Hence, C^* increases with respect to ϕ when $\phi \in (\phi_1, \phi_2]$, and C^* decreases with respect to ϕ when $\phi \in (\phi_2, 1)$. Here the only concern about the condition is that $\phi = \phi_2$, where $C^*|_{\phi=\phi_2}$ is the local maximum of C^* , respectively (see Figure 9).

Case 4. $\Lambda > 0$, and $\phi_1 < 0$, $\phi_2 > 1$. If $\phi_1 < 0$, $\phi_2 > 1$, then

$$\begin{aligned} \phi_1 &= \frac{-2(\alpha\beta\gamma - p\beta^2\eta) - \sqrt{\Delta}}{-2\alpha\beta^2} < 0, \\ \phi_2 &= \frac{-2(\alpha\beta\gamma - p\beta^2\eta) + \sqrt{\Delta}}{-2\alpha\beta^2} > 1; \end{aligned} \quad (22)$$

FIGURE 9: Example 14.

these two inequalities can be further derived as

$$\begin{aligned} p\beta\eta - \alpha\gamma &> \sqrt{\Delta} > 0, \\ -\alpha\beta - (p\beta\eta - \alpha\gamma) &> \sqrt{\Delta}; \end{aligned} \quad (23)$$

however, these two formulas are contradictory. Hence, this condition does not hold.

Case 5. $\Lambda > 0$, and $\phi_1, \phi_2 > 1$. Then $\gamma/\beta - p\eta/\alpha > 1$; the axis of symmetry of the function $f(\phi)$ is on the right side of $\phi = 1$, which means $\gamma/\beta > 1 > \phi$. So this condition does not hold.

According to the above discussion, only Cases 2 and 3 may have attacked equilibrium.

(4) When the attacked equilibrium exists, C^* will increase at first, and then C^* will decrease.

Example 13. Fixing $\alpha = 0.8$, $\gamma = 0.2$, $\eta = 0.1$, $\beta = 0.8$, $p = 1.0$, and varying ϕ , the change of $C(t)$ in system (2) is shown in Figure 8. By calculation, $\phi_1 = -0.2057$ (has been ignored because of $\phi = \phi_1 < 0$), $\phi_2 = 0.4557$ (see Figure 8).

Example 14. Fixing $\alpha = 0.8$, $\gamma = 0.3$, $\eta = 0.1$, $\beta = 0.6$, $p = 1.0$, and varying ϕ , the proportion of $C(t)$ in system (2) is shown in Figure 9. By calculation, $\phi_1 = 0.0955$, $\phi_2 = 0.6545$, so C^* exists as a maximum (see Figure 9).

According to above conclusion, there are some suggestions as follows.

(1) Regular antivirus and strengthening the precaution of malwares will help to reduce β and enlarge γ and can decrease A node.

(2) Also strengthening the precaution of malwares, which will enlarge γ , can help to decrease C nodes.

(3) Enhancing the firewall's abilities, like filter and information processing, helps to increase p and prevent S nodes from becoming C nodes.

(4) Reinstalling operation system or changing the hardware of computer, which also means to enlarge η or γ , will be useful to turn C nodes to S nodes or make A nodes become W nodes.

(5) Practically, it is hard to reduce α by controlling or decreasing the destructive power of malware, but it is available to inhibit the propagation of malware by enhancing the firewall's abilities of spying and controlling.

(6) By taking some special strategies, it is feasible to change the structure of the network, which also means to change ϕ , like installing firewall. Besides, according to the discussion of the parameter of ϕ , it must be regarded that the proportion of C nodes will get its maximum in special ϕ , which will cause enormous damage.

5. Conclusion

This paper aims at modelling a dynamical APDDoS attack model. And some properties of this novel model have been deeply researched, like threshold, equilibriums, and stability. The numerical simulations have been got at the same time. Finally, by analyzing the respective influences of system parameters, some suggestions are proposed to reduce the harm of DDoS attacks

Appendix

Referring to the method of calculating the propagation threshold in [21], the calculation process is shown as follows.

In an n -dimensional system, let $x = (x_1, x_2, \dots, x_n)^T$ denote the number of individuals in each compartment with $x_i \geq 0$. And let $X = \{x \geq 0 \mid x_i = 0, i = 1, \dots, m\}$ denote the set of disease states. Also let $F_i(x)$ be the rate of appearance of new infections in compartment i , V_i^+ be the rate of transfer of individuals into compartment i , and V_i^- be the rate of transfer of individuals out of compartment i .

Then the above model consists of nonnegative initial condition together with the following system of equations:

$$\dot{x}_i = f_i(x) = F_i(x) - V_i(x), \quad i = 1, \dots, n, \quad (\text{A.1})$$

where $V_i(x) = V_i^-(x) - V_i^+(x)$ and the functions satisfy the following 5 assumptions:

(A1) If $x \geq 0$, then $F_i, V_i^+, V_i^- \geq 0$ for $i = 1, \dots, n$.

(A2) If $x_i = 0$, then $V_i^- = 0$. In particular, if $x \in X$, then $V_i^- = 0$ for $i = 1, \dots, m$.

(A3) $F_i(x) = 0$ if $i > m$.

(A4) If $x \in X$ then $F_i(x) = 0$ and $V_i^+(x) = 0$ for $i = 1, \dots, m$.

(A5) If $F(x)$ is a set of zeros, then all eigenvalues of $Df(x_0)$, which is the derivative $[\partial f_i / \partial x_i]$ evaluated at the equilibrium, x_0 , have negative real parts.

And then, the derivatives $DF(x_0)$ and $DV(x_0)$ are partitioned as

$$\begin{aligned} DF(x_0) &= \begin{pmatrix} \mathbf{F} & 0 \\ 0 & 0 \end{pmatrix}, \\ DV(x_0) &= \begin{pmatrix} \mathbf{V} & 0 \\ J_3 & J_4 \end{pmatrix}, \end{aligned} \quad (\text{A.2})$$

where $\mathbf{F}$ and $\mathbf{V}$ are the $m \times m$ matrices defined by

$$\begin{aligned} \mathbf{F} &= \left[\frac{\partial F_i}{\partial x_j}(x_0) \right], \\ \mathbf{V} &= \left[\frac{\partial V_i}{\partial x_j}(x_0) \right], \end{aligned} \quad (\text{A.3})$$

with $0 \leq i, j \leq m$.

Further, $\mathbf{F}$ is nonnegative, $\mathbf{V}$ is a matrix, and all eigenvalues of J_4 have positive real part. $\rho(\mathbf{FV}^{-1})$, the spectral radius of $\mathbf{FV}^{-1}$, is a threshold parameter.

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] R. Zheng, W. Lu, and S. Xu, "Active cyber defense dynamics exhibiting rich phenomena," in *Proceedings of the Symposium and Bootcamp on the Science of Security, HotSoS '15*, p. 2, ACM, 2015.
- [2] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 40, no. 4, pp. 853–865, 2010.
- [3] S. Xu, "Emergent behavior in cybersecurity," in *Proceedings of the the 2014 Symposium and Bootcamp*, pp. 1-2, Raleigh, North Carolina, April 2014.
- [4] 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: Simulation and Computation for Engineering and Environmental Systems*, vol. 43, pp. 110–125, 2017.
- [5] <http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics>.
- [6] <http://www.bbc.com/news/technology-37941216>.
- [7] <http://www.bbc.com/news/technology-40886418>.
- [8] C. Tankard, "Advanced Persistent threats and how to monitor and deter them," *Network Security*, vol. 2011, no. 8, pp. 16–19, 2011.

- [9] S. Rass, S. König, and S. Schauer, "Defending against advanced persistent threats using game-theory," *PLoS ONE*, vol. 12, no. 1, Article ID e0168675, 2017.
- [10] B. Schneier, "Attack trees," *Doctor Dobbs Journal*, vol. 24, no. 12, pp. 21–29, 1999.
- [11] A. K. Sood and R. J. Enbody, "Targeted cyberattacks: a superset of advanced persistent threats," *IEEE Security and Privacy*, vol. 11, no. 1, pp. 54–61, 2013.
- [12] L.-X. Yang, P. Li, X. Yang, and Y. Y. Tang, "Security evaluation of the cyber networks under advanced persistent threats," *IEEE Access*, vol. 5, pp. 20111–20123, 2017.
- [13] https://en.wikipedia.org/wiki/Advanced_persistent_threat.
- [14] W. Liu and S. Zhong, "Web malware spread modelling and optimal control strategies," *Scientific Reports*, vol. 7, Article ID 42308, 2017.
- [15] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the source," *IEEE International Conference on Network Protocols IEEE Computer Society*, vol. 154, no. 3-4, pp. 312–321, 2002.
- [16] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and Software-Defined Networking," *Computer Networks*, vol. 81, pp. 308–319, 2015.
- [17] Q. Yan, F. R. Yu, Q. X. Gong, and J. Q. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.
- [18] L. X. Yang, X. Yang, and Y. Y. Tang, "A bi-virus competing spreading model with generic infection rates," *IEEE Network Science and Engineering*, vol. 5, no. 1, pp. 2–13, 2018.
- [19] J. P. LaSalle, "The stability of dynamical systems," *SIAM Journal on Mathematical Analysis*, vol. 25, 1976.
- [20] R. C. Robinson, "An introduction to dynamical systems: continuous and discrete," *American Mathematical Society*, vol. 19, 2012.
- [21] P. van den Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," *Mathematical Biosciences*, vol. 180, no. 1-2, pp. 29–48, 2002.