Hindawi
Complexity
Volume 2021, Article ID 6694383, 11 pages
https://doi.org/10.1155/2021/6694383

Research Article

Impact of Defending Strategy Decision on DDoS Attack

Chunming Zhang

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

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

Received 14 October 2020; Revised 15 November 2020; Accepted 4 March 2021; Published 16 March 2021

Academic Editor: Wei Wang

Distributed denial-of-service (DDoS) attack is a serious threat to cybersecurity. Many strategies used to defend against DDoS attacks have been proposed recently. To study the impact of defense strategy selection on DDoS attack behavior, the current study uses logistic function as basis to propose a dynamic model of DDoS attacks with defending strategy decisions. Thereafter, the attacked threshold of this model is calculated. The existence and stability of attack-free and attacked equilibria are proved. Lastly, some effective strategies to mitigate DDoS attacks are suggested through parameter analysis.

1. Introduction

A distributed denial-of-service (DDoS) attack is a cyber-attack in which hackers attempt to make a website or computer unavailable by flooding or crashing the website with too much traffic [1, 2]. Given the rapid development of cloud computing, big data, and artificial intelligence, distributed denial-of-service (DDoS) attacks have become one among the most critical threats to network security [3, 4]; for example, in February 2018, the official website of the PyeongChang Winter Olympics Organizing Committee was forced to shut down during the Winter Olympic Games due to a DDoS attack [5]; in March 2018, GitHub suffered a DDoS attack with the maximum peak traffic reaching 1.7 TBPS [6]; in October 2019, Amazon Web Services was attached by DDoS for several hours, resulting in an outage affecting many websites [7]. Therefore, it is an important issue to study the dynamic behavior of DDoS attacks and propose defense strategies on this basis. Numerous models of DDoS attacks have been proposed in recent years. Haldar et al. [8] proposed a DDoS attack model based on the compartment model and obtained threshold conditions that determine the success or failure of such attacks. Kumar et al. [9] presented a dynamic model of DDoS attack in a computer network and studied the dynamic behavior of this model through numerical simulation. Hou et al. [10] investigated a DDoS attack model with a saturated contact infection rate and proved the stability of this model. Mishra et al. [11] considered the characteristics of DDoS attacks on the Internet of Things (IoT) and proposed a DDoS attack model on IoT, given the conditions for a successful attack. Furthermore, some effective defense strategies, such as installing defense software and upgrading firewalls, have been widely used to mitigate DDoS attacks [12, 13]. Several DDoS attack dynamic models with defending strategies have been proposed recently to study the impact of defending strategies on DDoS attacks. Zhang et al. [13] studied a differential dynamics model for DDoS attacks with four states, namely, weak-defensive, attacked, strong-defensive, and compromised nodes. The global stability conditions of the model are given, and some defending strategies are proposed to mitigate the DDoS attack. Zhang et al. [14] used mean-field theory as basis to develop a DDoS attack model on arbitrary networks. Some reasonable strategies for defending against DDoS attacks have been provided based on theoretical analysis. Rao et al. [15] proposed a DDoS attack model with quarantine strategy; mathematical analysis demonstrated that quarantining infected computers can effectively block DDoS attacks. Zhang et al. [16] constructed an optimal control model for DDoS attacks on the Internet of Things and obtained its optimal defense strategy. Huang et al. [17] proposed a new low-cost DDoS attack architecture and got three optimal attack strategies based on variational method. Li et al. [18] established a low-rate DDoS attack model based on cloud computing environment and proposed a strategy to mitigate low-rate DDoS attacks.

However, the existing dynamic models have assumed that defenders will adopt a defending strategy with a fixed probability. On the one hand, adopting defending strategies in the real world will benefit from mitigating DDoS attacks. On the other hand, defenders may choose not to adopt defense strategies owing to defensive costs, which can be considered a dilemma. As rational persons, defenders will compare the benefits and costs caused by DDoS attacks. If the benefits outweigh the costs, then defenders will be likely to adopt a defending strategy; otherwise, they will be less likely to adopt such a strategy. That is, defenders decide the probability of adopting a defending strategy based on a cost-benefit analysis. In addition, none of the existing defense strategy recommendations has analyzed the cost-benefit, so the defense strategies obtained are not feasible solutions.

To overcome the above shortcomings, this study uses the preceding discussions as bases to first propose a game theory-based DDoS attack model with defending strategy decisions. Our main contributions are summarized as follows:

(a) In order to study the impact of defense strategy decisions on the dynamic behavior of DDoS attacks, according to the above cost-benefit analysis, this research first constructs two smooth logistic functions, which can describe the defense strategy choices of the defender under different cost-benefit conditions. Based on the above logistic function and compartmental model theory, this paper first proposed a game-theoretic DDoS attack dynamics model with a cost-benefit function.

(b) The current study obtains the attack threshold of the above model, which is the condition for successful attack, and then the local stability of the attacked equilibrium and the attack-free equilibrium is proved, using the theory of differential stability. In addition, this study uses the analysis of the impact of parameters on model behavior as basis to propose some effective defending strategies to mitigate DDoS attacks. Some numerical experiments are also presented to verify the effectiveness of defending strategies.

The remainder of this paper is organized as follows. Section 2 proposes a novel DDoS attack model. Section 3 presents the mathematical properties of the proposed model. Section 4 provides some suggestions for the defense of DDoS attacks by analyzing the effects of parameters on model behavior. Section 5 concludes this study.

2. Model Descriptions and Cost-Benefit Analysis

This section proposes a dynamic model with defending strategy decision based on a cost-benefit analysis.

2.1. Differential Dynamic Model. A typical computer network system mainly consists of numerous client and server computers. Clients and servers often have different levels of cybervulnerabilities. Clients are considered to be relatively vulnerable to malware and flooding attacks. Servers are often equipped with firewalls. Although they are considerably resilient to malware, servers could still be vulnerable to flooding attacks.

A typical DDoS attack and defense is carried out in the following three-phase procedure, which is depicted in Figure 1.

2.1.1. Spreading Malware. Attackers attempt to spread malware to infect normal clients on networks by using fake emails or web links. Once normal clients have been affected by malware, they are controlled by attackers to become zombie clients capable of infecting other clients.

2.1.2. Launching Attacks. Attackers manipulate zombie clients to launch flooding attacks targeting at least one target server. Such attacks will compromise the target servers, thereby losing their abilities to provide services to the external environment.

2.1.3. Recovering. Defenders adopt some defense strategies, such as antivirus software or firewalls, to recover the attacked computers, including zombie clients and compromised servers.

The following reasonable assumptions can be obtained on bases of the preceding facts:

($H1$) Computers on the Internet can be divided into two parts: client and server parts. The total numbers of computers on the client and server parts are N_W and N_S, respectively [7].

($H2$) Computers on the client part can be classified into three classes: normal clients (W nodes), infected clients (I nodes), and recovered clients (R nodes) [19, 20]. Let $W(t)$, $I(t)$, and $R(t)$ represent the proportion of the W, I, and R nodes, respectively, in the total number of computers on the client part at time t. The total number is constantly equal to N_W:

$$W(t) + I(t) + R(t) \equiv 1. \tag{1}$$

($H3$) Computers on the server part can also be classified into three classes: normal servers (S nodes), compromised servers (C nodes), and recovered servers (D nodes). Let $S(t)$, $C(t)$, and $D(t)$ represent the proportion of the S, C, and D nodes, respectively, in the total number of computers on the server part at time t. The total number is constantly equal to NS:

$$S(t) + C(t) + D(t) \equiv 1. \tag{2}$$

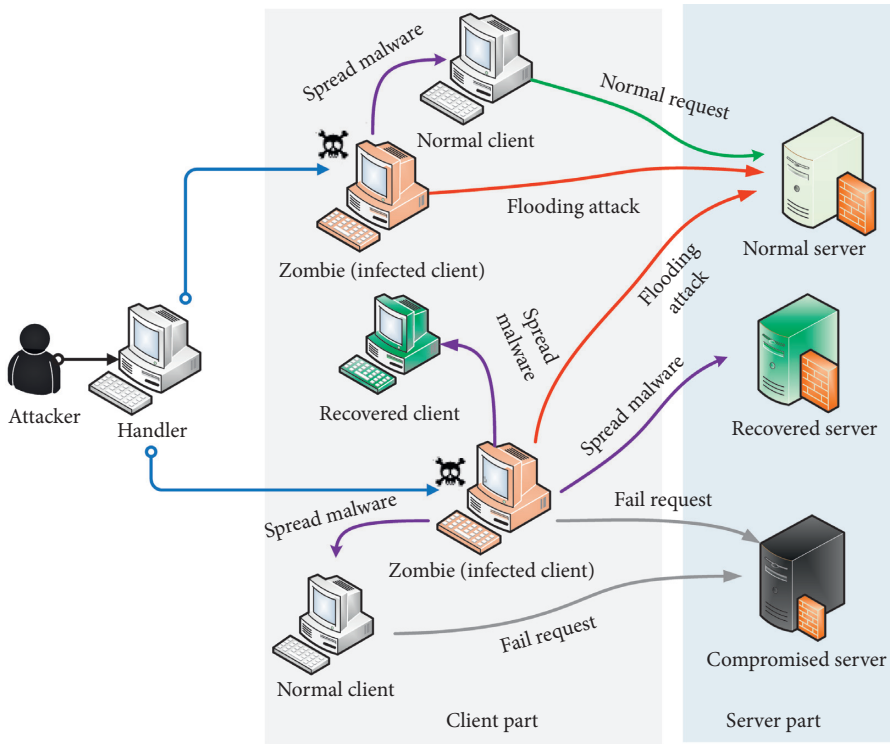

Figure 1: Schematic of a DDoS attack.

(*H*4) Owing the implementation of some dangerous operations, such as browsing phishing sites, a *W* node will be infected with a probability of β.

(*H*5) Owing to the execution of some positive measures, such as running antivirus software, an *I* node will recover with a probability of τ.

(*H*6) Owing to the reinstallation of an operation system, an *R* node becomes a *W* node with probability γ.

(*H*7) Owing to DDoS attacks, a *S* node will compromise with probability α.

(*H*8) Owing to the implementation of some positive measures, such as running firewall software, a *C* node becomes a *D* node with probability η.

(*H*9) Owing to the reinstallation of an operating system, a *D* node becomes a *S* node with probability δ.

(*H*10) Owing to the adoption of some defensive strategies, such as installing antivirus software, a *W* node becomes a *R* node with probability *f* [21, 22].

(*H*11) Owing to the implementation of some defensive strategies, such as upgrading firewall software, a *S* node becomes a *D* node with probability *g*. Probabilities *f* and *g* are determined by the cost-benefit analysis of defenders, which we will discuss in part *B* of this section.

Given the preceding assumptions, the following DDoS attack model can be obtained (see Figure 2):

$$\begin{cases} \dfrac{dW(t)}{dt} = -\beta W(t)I(t) + \gamma R(t) - fW(t), \\ \dfrac{dI(t)}{dt} = \beta W(t)I(t) - \tau I(t), \\ \dfrac{dR(t)}{dt} = \tau I(t) - \gamma R(t) + fW(t), \\ \dfrac{dS(t)}{dt} = -\alpha S(t)I(t) + \delta\, D(t) - gS(t), \\ \dfrac{dC(t)}{dt} = \alpha S(t)I(t) - \eta C(t), \\ \dfrac{dD(t)}{dt} = \eta C(t) + gS(t) - \delta\, D(t), \end{cases} \tag{3}$$

where $0 \le W(t), I(t), R(t), S(t), C(t), D(t) \le 1$, and $0 \le \alpha, \beta, \gamma, \eta, \tau, \delta \le 1$.

2.2. Cost-Benefit Analysis. Although defensive strategies may bring benefits, there are costs to adopting these defensive strategies, which is considered a dilemma for defenders. Logistic function can be used to describe the rational decision problem of whether to adopt defensive

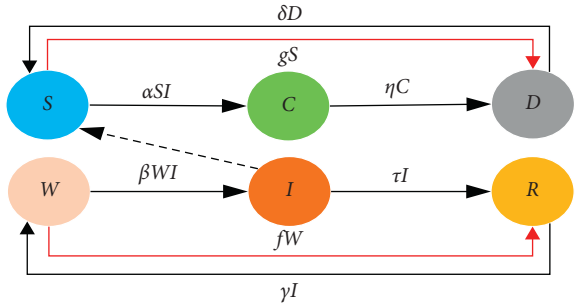

Figure 2: State transition diagram of the proposed model (dashed lines on the graph represent DDoS attacks, and red lines represent defense strategies).

strategies. When the cost of adopting a defending strategy is greater than the benefit, defenders will not adopt such a strategy. Otherwise, defenders will adopt this strategy. For the client part, the benefit is directly proportional to the loss of not adopting this strategy L_W, the number of computers infected $N_W I(t)$, and the probability of infection β. The cost of adopting this strategy is C_W. Thus, the total payoff of adopting this strategy for the client part is $\Delta\omega_W = \beta N_W L_W I(t) - C_W$. For the server part, let L_S represent the cost of not adopting a defending strategy and C_W represents the cost of adopting a defending strategy. The total payoff of adopting this strategy for the server part is $\Delta\omega_S = \alpha N_S L_S I(t) - C_S$.

To describe the strategic decision problem, we define the following two logistic functions. Figure 3 depicts the logistic equation [23–25].

$$f = \frac{\phi}{1 + e^{\Delta\omega_W}} = \frac{\phi}{1 + e^{\mu\left(N_W\beta L_W I(t) - C_W\right)}} = \frac{\phi e^{\mu C_W}}{e^{\mu C_W} + e^{\mu N_W \beta L_W I(t)}}, \tag{4}$$

$$g = \frac{\varphi}{1 + e^{\Delta\omega_S}} = \frac{\varphi}{1 + e^{\nu\left(N_S\alpha L_S I(t) - C_S\right)}} = \frac{\varphi e^{\nu C_S}}{e^{\nu C_S} + e^{\nu N_S \alpha L_S I(t)}}, \tag{5}$$

where μ and ν represent the smooth exponents of functions f and g, respectively, and ϕ and φ represent the maximum value of functions f and g, respectively. $0 \le \phi$ and $\varphi \le 1$.

3. Theoretical Analysis

This section investigates some mathematical properties of the proposed model, including equilibrium, attacked threshold, and stability of system (3).

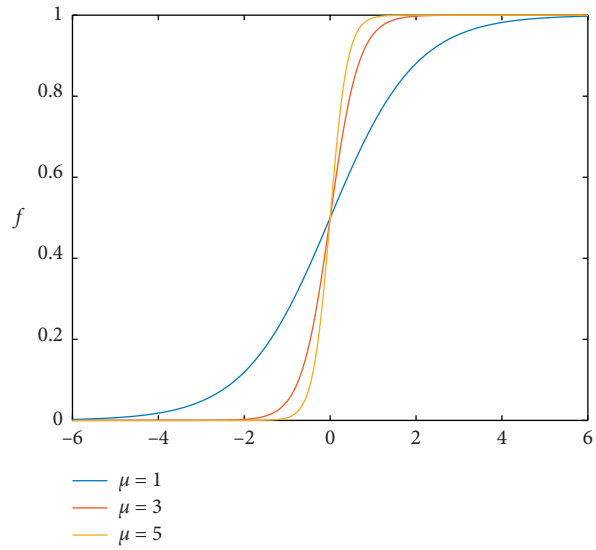

Figure 3: Logistic function.

Given that $W(t) + I(t) + R(t) \equiv 1$ and $S(t) + C(t) + D(t) \equiv 1$, we use a simple calculation to obtain $W(t) \equiv 1 - I(t) - R(t)$ and $S(t) \equiv 1 - C(t) - D(t)$. Hence, the first and fourth equations in system (3) can be represented by the other four equations in this system. Therefore, system (3) can be simplified to the following system:

$$\begin{cases} \dfrac{dI(t)}{dt} = \beta(1 - I(t) - R(t))I(t) - \tau I(t), \\ \dfrac{dR(t)}{dt} = \tau I(t) - \gamma R(t) + f(1 - I(t) - R(t)), \\ \dfrac{dC(t)}{dt} = \alpha(1 - C(t) - D(t))I(t) - \eta C(t), \\ \dfrac{dD(t)}{dt} = \eta C(t) + g(1 - C(t) - D(t)) - \delta D(t), \end{cases} \tag{6}$$

where $f = \phi e^{\mu C_W}/e^{\mu C_W} + e^{\mu N_W \beta L_W I(t)}$ and $g = \varphi e^{\nu C_S}/e^{\nu C_S} + e^{\nu N_S \alpha L_S I(t)}$. The parameter range of system (6) is as follows:

$$\Theta = \left\{(\alpha, \beta, \gamma, \eta, \tau, \phi, \varphi, \mu, \nu, L_W, L_S, C_W, C_S, N_W, N_S) \in R_+^{15}: 0 \le \alpha, \beta, \gamma, \eta, \tau, \phi, \varphi \le 1\right\}. \tag{7}$$

Evidently, the domain of system (6) is as follows:

$$\Omega = (I(t), R(t), C(t), D(t)) \in R_+^4: 0 \le I(t), R(t), C(t), D(t) \le 1. \tag{8}$$

Given that systems (3) and (6) are equivalent, the remainder of this paper mainly focuses on the properties of system (6).

3.1. Attack-Free Equilibrium

Theorem 1. *A unique attack-free equilibrium* $E_0 = (I_0, R_0, C_0, D_0) = (0, f_0/\gamma + f_0, 0, g_0/\delta + g_0)$ *is present in system (6), where* $f_0 = \phi e^{\mu C_W}/1 + e^{\mu C_W}$ *and* $g_0 = \varphi e^{\nu C_S}/1 + e^{\nu C_S}$.

Proof. By solving the following equations,

$$\begin{cases} \beta(1 - I(t) - R(t))I(t) - \tau I(t) = 0, \\ \tau I(t) - \gamma R(t) + f(1 - I(t) - R(t)) = 0, \\ \alpha(1 - C(t) - D(t))I(t) - \eta C(t) = 0, \\ \eta C(t) + g(1 - C(t) - D(t)) - \delta\ D(t) = 0. \end{cases} \tag{9}$$

E_0 is evidently a solution to equation (7). Thus, E_0 is constantly an attack-free equilibrium of system (6). □

Remark 1. An equilibrium represents a possible final state of DDoS attacks. Thereafter, attack-free equilibrium represents the possible final state of DDoS attack extinction.

The attacked threshold is a crucial parameter that determines whether computers on a network will experience DDoS attacks. This section calculates the attacked threshold by using the **FV** method proposed in [26, 27].

Let $y = (I(t), C(t))^{\mathrm{T}}$ and $y_0 = (I_0, C_0)^{\mathrm{T}}$. Accordingly, the following functions can be obtained:

$$\begin{aligned} F(y) &= \big(F_1(y), F_2(y)\big)^T \\ &= (\beta(1 - I(t) - R(t))I(t), \\ &\quad \alpha\big(1 - C(t) - D(t)\big)I(t))^T, \end{aligned} \tag{10}$$

$$V(y) = \big(V_1(y), V_2(y)\big)^T = (\tau I(t), \eta C(t))^T. \tag{11}$$

By considering the partial derivative of I and C at E_0, we obtain as follows:

$$\mathbf{F} = \begin{pmatrix} \dfrac{\partial F_1(y_0)}{\partial I} & \dfrac{\partial F_1(y_0)}{\partial C} \\ \dfrac{\partial F_2(y_0)}{\partial I} & \dfrac{\partial F_2(y_0)}{\partial C} \end{pmatrix} = \begin{pmatrix} \beta(1 - R_0) & 0 \\ \alpha(1 - D_0) & 0 \end{pmatrix}, \tag{12}$$

$$\mathbf{V} = \begin{pmatrix} \dfrac{\partial V_1(y_0)}{\partial A} & \dfrac{\partial V_1(y_0)}{\partial C} \\ \dfrac{\partial V_2(y_0)}{\partial A} & \dfrac{\partial V_2(y_0)}{\partial C} \end{pmatrix} = \begin{pmatrix} \tau & 0 \\ 0 & \eta \end{pmatrix}. \tag{13}$$

By calculation, we obtain as follows:

$$\mathbf{FV}^{-1} = \begin{pmatrix} \beta(1 - R_0) & 0 \\ \alpha(1 - D_0) & 0 \end{pmatrix} \begin{pmatrix} \dfrac{1}{\tau} & 0 \\ 0 & \dfrac{1}{\eta} \end{pmatrix} = \begin{pmatrix} \dfrac{\beta}{\tau}(1 - R_0) & 0 \\ \dfrac{\alpha}{\tau}(1 - D_0) & 0 \end{pmatrix}. \tag{14}$$

The attacked threshold can be obtained by calculating the eigenvalue of $\mathbf{FV}^{-1}$. Lastly, the two eigenvalues of $\mathbf{FV}^{-1}$ are calculated as $\rho(\mathbf{FV}^{-1}) = 0$ and $\rho(\mathbf{FV}^{-1}) = \beta/\tau(1 - R_0)$, while the eigenvalue $\rho(\mathbf{FV}^{-1}) = 0$ is disregarded. Hence, the attacked threshold can be obtained as follows:

$$T_0 = \frac{\beta}{\tau}(1 - R_0) = \frac{\beta\gamma\big(1 + e^{\mu C_W}\big)}{\tau\big(\gamma + (\gamma + \phi)e^{\mu C_W}\big)}. \tag{15}$$

Theorem 2. *When system (6) is considered,* E_0 *is locally asymptotically stable if* $T_0 < 1$.

Proof. When system (6) is considered, the Jacobian matrix at E_0 is as follows:

$$\begin{bmatrix} \beta - \tau - \dfrac{\beta f_0}{\gamma + f_0} & 0 & 0 & 0 \\ \tau + f_0'\left(1 - \dfrac{\beta f_0}{\gamma + f_0}\right) - f_0 & -\gamma - f_0 & 0 & 0 \\ \alpha\left(1 - \dfrac{g_0}{\delta + g_0}\right) & 0 & -\eta & 0 \\ \left(1 - \dfrac{g_0}{\delta + g_0}\right)g_0' & 0 & \eta - g_0 - \delta & -g_0 \end{bmatrix}. \tag{16}$$

The corresponding characteristic equation can be deduced as follows:

$$\begin{bmatrix} \beta - \tau - \dfrac{\beta f_0}{\gamma + f_0} - \lambda & 0 & 0 & 0 \\ \tau + f_0'\left(1 - \dfrac{\beta f_0}{\gamma + f_0}\right) - f_0 & -\gamma - f_0 - \lambda & 0 & 0 \\ \alpha\left(1 - \dfrac{g_0}{\delta + g_0}\right) & 0 & -\eta - \lambda & 0 \\ \left(1 - \dfrac{g_0}{\delta + g_0}\right)g_0' & 0 & \eta - g_0 - \delta & -g_0 - \lambda \end{bmatrix},$$

$$= (-\eta - \lambda)(-g_0 - \lambda)(-\gamma - f_0 - \lambda)\left(\beta - \tau - \frac{\beta f_0}{\gamma + f_0} - \lambda\right). \tag{17}$$

Equation (17) has three negative roots $\lambda_1 = -\eta < 0$, $\lambda_2 = -g_0 < 0$, and $\lambda_3 = -f_0 - \gamma < 0$. The remaining root is determined by the following equation:

$$\beta - \tau - \frac{\beta f_0}{\gamma + f_0} - \lambda = 0. \tag{18}$$

As $T_0 = \beta/\tau(1 - R_0) = \beta/\tau(1 - f_0/\gamma + f_0) < 1$, by calculation, we obtain as follows:

$$\lambda_4 = \beta - \tau - \frac{\beta f_0}{\gamma + f_0} < 0. \tag{19}$$

All roots of the characteristic equation (17) are negative. Thus, E_0 is locally asymptotically stable if $T_0 < 1$. □

Remark 2. Theorem 2 shows that DDoS attacks would die out if $T_0 < 1$.

Example 1. Consider system (6) with $\alpha = 0.02$, $\beta = 0.01$, $\gamma = 0.1$, $\delta = 0.1$, $\eta = 0.02$, $\tau = 0.005$, $\delta = 0.03$, $\phi = 0.6$, $\varphi = 0.5$, $\mu = 1$, $\nu = 1$, $N_W = 1000$, $N_S = 1000$, $L_W = 1$, $L_S = 1$, $C_W = 1$, and $C_S = 2$. By calculation, $E_0 = (0,\ 0.814,\ 0,\ 0.936)^T$ and $T_0 = 0.371 < 1$ satisfies the condition of Theorem 2. Hence, the system is locally asymptotically stable at E_0 (see Figure 4).

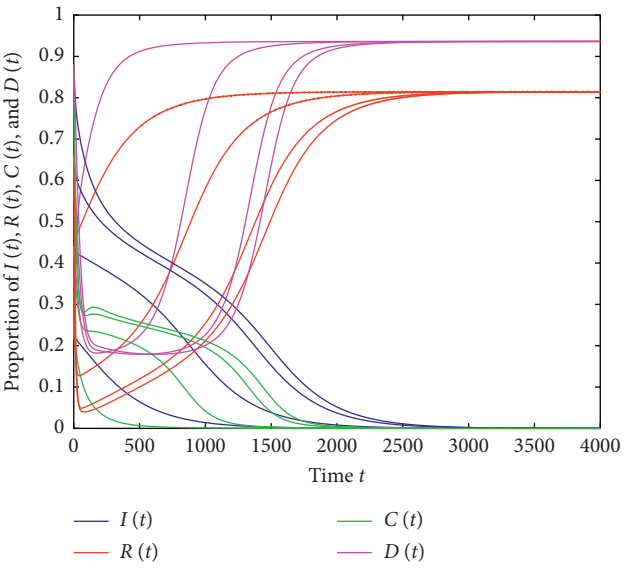

FIGURE 4: Stability of the attack-free solution E_0.

3.2. Attacked Equilibrium

Theorem 3. *Consider system (6) on domain Ω. If $T_0 > 1$, then system (6) has an attacked equilibrium:*

$$E_1 = (I_1, R_1, C_1, D_1)^T, \tag{20}$$

$$I_1 = \frac{x}{\mu N_W \beta L_W}, \tag{21}$$

$$R_1 = 1 - I_1 - \frac{\tau}{\beta}, \tag{22}$$

$$C_1 = \frac{\delta \alpha I_1}{\alpha I_1 (\eta + \delta) + \eta (g_1 + \delta)}, \tag{23}$$

$$D_1 = 1 - C_1 - \frac{\eta C_1}{\alpha I_1}, \tag{24}$$

where $g_1 = \varphi e^{\nu C_S}/e^{\nu C_S} + e^{\nu N_S \alpha L_S I_1}$ and x is a positive solution of the transcendental equation as follows:

$$(\tau + \gamma) x e^x + \left(\frac{\tau}{\beta}\gamma - \gamma\right)\mu N_W \beta L_W e^x + (\tau + \gamma)x + \mu N_W \beta L_W e^{\mu C_W}\left(\frac{\tau}{\beta}\gamma - \gamma + \frac{\tau}{\beta}\phi\right) = 0. \tag{25}$$

Proof. By solving equation (9), we can obtain $R = 1 - I - \tau/\beta$, $C = \delta\alpha I/\alpha I(\eta + \delta) + \eta(g_1 + \delta)$, $D = 1 - C - \eta C/\alpha I$, and $I = x/\mu N_W \beta L_W$ x $(0 \le x \le \mu N_W \beta L_W)$ is the root of equation (24).

Thereafter, we examine the existence of the solution of equation (24).

Equation (24) can be organized as follows:

Let

$$G_1(x) = (\tau + \gamma)x + \mu N_W \beta L_W \left(\frac{\gamma\tau}{\beta} - \gamma\right), \tag{26}$$

$$G_2(x) = -\frac{\phi e^{\mu C_W}}{e^{\mu C_W} + e^x}\frac{\tau}{\beta}\mu N_W \beta L_W. \tag{27}$$

As $G_1'(x) = \tau + \gamma > 0$, function G_1 is an increasing function. As $G_2'(x) = \phi e^{\mu C_W} e^x/(e^{\mu C_W} + e^x)^2 \tau/\beta\mu N_W \beta L_W > 0$, function G_2 is also an increasing function.

As $G_1(0) = \mu N_W \beta L_W(\gamma\tau/\beta - t\gamma)$ and $G_2(0) = -\phi e^{\mu C_W}/e^{\mu C_W} + 1\tau/\beta\mu N_W \beta L_W$, according to $T_0 = \beta\gamma(1 + e^{\mu C_W})/\tau(\gamma + (\gamma + \phi)e^{\mu C_W}) > 1$, we have $G_2(0) > G_1(0)$. As $G_1(\mu N_W \beta L_W) = \mu N_W \beta L_W(\tau + \gamma\tau/\beta) > 0$ and $G_2(\mu N_W \beta L_W) = -\phi e^{\mu C_W}/e^{\mu C_W} + e^{\mu N_W \beta L_W}\tau/\beta\mu N_W \beta L_W < 0$, $G_1(\mu N_W \beta L_W) > G_2(\mu N_W \beta L_W)$. Therefore, transcendental equation (24) has at least one solution x $(0 \le x \le \mu N_W \beta L_W)$.

The proof is complete. □

Remark 3. The attacked equilibrium represents the possible final state of DDoS attacks.

Theorem 4. *Consider system (6). If $-(a_{11} + a_{22}) > 0$, $a_{11}a_{22} - a_{12}a_{21} > 0$, $-(b_{11} + b_{22}) > 0$, and $b_{11}b_{22} - b_{12}b_{21} > 0$, then E_1 is locally asymptotically stable:*

$$a_{11} = \beta(1 - 2I_1 - R_1) - \tau, \tag{28}$$

$$a_{12} = -\beta I_1, \tag{29}$$

$$a_{21} = \tau - f_1 + (1 - I_1 - R_1) f_1', \tag{30}$$

$$a_{22} = -\gamma - f_1, \tag{31}$$

$$b_{11} = -\alpha I_1 - \eta, \tag{32}$$

$$b_{12} = -\alpha I_1, \tag{33}$$

$$b_{21} = \eta - g_1, \tag{34}$$

$$b_{22} = -g_1 - \delta, \tag{35}$$

$$f_1 = \frac{\phi e^{\mu C_W}}{e^{\mu C_W} + e^{\mu N_W \beta L_W I_1}}, \tag{36}$$

$$g_1 = \frac{\varphi e^{\nu C_S}}{e^{\nu C_S} + e^{\nu N_S \alpha L_S I_1}}, \tag{37}$$

$$f_1' = \frac{\mu N_W \beta L_W \phi e^{\mu C_W} e^{\mu N_W \beta L_W I_1}}{\left(e^{\mu C_W} + e^{\mu N_W \beta L_W I_1}\right)^2}, \tag{38}$$

$$g_1' = \frac{\nu N_S \alpha L_S \varphi e^{\nu C_S} e^{\nu N_S \alpha L_S I_1}}{\left(e^{\nu C_S} + e^{\nu N_S \alpha L_S I_1}\right)^2}. \tag{39}$$

Proof. For system (6), the Jacobian matrix at E_1 is

$$\begin{pmatrix} \beta(1 - 2I_1 - R_1) - \tau & -\beta I_1 & 0 & 0 \\ \tau - f_1 + (1 - I_1 - R_1) f_1' & -\gamma - f_1 & 0 & 0 \\ \alpha(1 - C_1 - D_1) & 0 & -\alpha I_1 - \eta & -\alpha I_1 \\ (1 - C_1 - D_1) g_1' & 0 & \eta - g_1 & -g_1 - \delta \end{pmatrix}. \tag{40}$$

The corresponding characteristic equation of the Jacobian matrix (40) can be deduced as follows:

$$\begin{pmatrix} \beta(1 - 2I_1 - R_1) - \tau - \lambda & -\beta I_1 & 0 & 0 \\ \tau - f_1 + (1 - I_1 - R_1) f_1' & -\gamma - f_1 - \lambda & 0 & 0 \\ \alpha(1 - C_1 - D_1) & 0 & -\alpha I_1 - \eta - \lambda & -\alpha I_1 \\ (1 - C_1 - D_1) g_1' & 0 & \eta - g_1 & -g_1 - \delta - \lambda \end{pmatrix} = \begin{pmatrix} a_{11} - \lambda & a_{12} \\ a_{21} & a_{22} - \lambda \end{pmatrix} \begin{pmatrix} b_{11} - \lambda & b_{12} \\ b_{21} & b_{22} - \lambda \end{pmatrix} = 0, \tag{41}$$

where

$$a_{11} = \beta(1 - 2I_1 - R_1) - \tau, a_{12} = -\beta I_1, a_{21} = \tau - f_1 + (1 - I_1 - R_1) f_1', a_{22} = -\gamma - f_1, b_{11} = -\alpha I_1 - \eta,$$
$$b_{12} = -\alpha I_1, b_{21} = \eta - g_1, b_{22} = -g_1 - \delta, g_1 = \frac{\varphi e^{\nu C_S}}{e^{\nu C_S} + e^{\nu N_S \alpha L_S I_1}}, f_1 = \frac{\phi e^{\mu C_W}}{e^{\mu C_W} + e^{\mu N_W \beta L_W I_1}}, f_1' = \frac{\mu N_W \beta L_W \phi e^{\mu C_W} e^{\mu N_W \beta L_W I_1}}{\left(e^{\mu C_W} + e^{\mu N_W \beta L_W I_1}\right)^2}, \tag{42}$$
$$g_1' = \frac{\nu N_S \alpha L_S \varphi e^{\nu C_S} e^{\nu N_S \alpha L_S I_1}}{\left(e^{\nu C_S} + e^{\nu N_S \alpha L_S I_1}\right)^2}.$$

By calculation, the roots of the characteristic equation (41) are determined by the following two equations:

$$\begin{aligned} \lambda^2 - (a_{11} + a_{22})\lambda + a_{11}a_{22} - a_{12}a_{21} = 0, \\ \lambda^2 - (b_{11} + b_{22})\lambda + b_{11}b_{22} - b_{12}b_{21} = 0. \end{aligned} \tag{43}$$

The Hurwitz criterion [28, 29] indicates sufficient conditions for all roots of the characteristic equation (30) to be negative are $-(a_{11} + a_{22}) > 0$, $a_{11}a_{22} - a_{12}a_{21} > 0$, $-(b_{11} + b_{22}) > 0$, and $b_{11}b_{22} - b_{12}b_{21} > 0$.

The proof is complete. □

Remark 4. Theorems 3 and 4 imply that DDoS attacks would persist if conditions in theorems are satisfied.

Example 2. Consider system (6) with $\alpha = 0.02$, $\beta = 0.05$, $\gamma = 0.1$, $\delta = 0.1$, $\eta = 0.02$, $\tau = 0.004$, $\delta = 0.03$, $\phi = 0.6$, $\varphi = 0.5$, $\mu = 1$, $\nu = 1$, $N_W = 1000$, $N_S = 1000$, $L_W = 1$, $L_S = 1$, $C_W = 1$, and $C_S = 2$. By calculation, $E_1 = (0.885, 0.035, 0.358, 0.238)^T$, $T_0 = 2.321 > 1$, $-(a_{11} + a_{22}) = 0.144 > 0$, $a_{11}a_{22} - a_{12}a_{21} = 0.0046 > 0$, $-(b_{11} + b_{22}) = 0.068 > 0$, and $b_{11}b_{22} - b_{12}b_{21} = 0.0015 > 0$ satisfy the condition of Theorem 4. Hence, the system is locally asymptotically stable at E_1 (see Figure 5).

4. Further Discussion

This section investigates the impact of some parameters on the dynamic behavior of the proposed model.

From Theorem 2, T_0 is an important parameter that determines whether DDoS attacks are successful. If $T_0 < 1$, then the attacks will not succeed. Hence, we need to take some measures to make T_0 considerably below one.

Given that $T_0 = \beta\gamma(1 + e^{\mu C_W})/\tau(\gamma + (\gamma + \phi)e^{\mu C_W})$, taking the derivative with respect to β, γ, τ, ϕ, μ, and C_W, we obtain the following:

$$\begin{cases} \dfrac{\partial T_0}{\partial \beta} = \dfrac{\gamma\left(1+e^{\mu C_W}\right)}{\tau\left(\gamma+(\gamma+\phi)e^{\mu C_W}\right)} > 0, \\ \dfrac{\partial T_0}{\partial \gamma} = \dfrac{\beta\phi}{\tau\gamma^2}\dfrac{e^{\mu C_W}\left(1+e^{\mu C_W}\right)}{\left[1+(1+(\phi/\gamma))e^{\mu C_W}\right]^2} > 0, \\ \dfrac{\partial T_0}{\partial \phi} = -\dfrac{\beta\gamma\left(1+e^{\mu C_W}\right)e^{\mu C_W}}{\tau\left[\gamma+(\gamma+\phi)e^{\mu C_W}\right]^2} < 0, \\ \dfrac{\partial T_0}{\partial \tau} = -\dfrac{1}{\tau^2}\dfrac{\beta\gamma\left(1+e^{\mu C_W}\right)}{\left(\gamma+(\gamma+\phi)e^{\mu C_W}\right)} < 0, \\ \dfrac{\partial T_0}{\partial \mu} = -\dfrac{\beta\phi\gamma}{\tau}\dfrac{C_W e^{\mu C_W}}{\left[\gamma+(\gamma+\phi)e^{\mu C_W}\right]^2} < 0, \\ \dfrac{\partial T_0}{\partial C_W} = -\dfrac{\beta\phi\gamma}{\tau}\dfrac{\mu e^{\mu C_W}}{\left[\gamma+(\gamma+\phi)e^{\mu C_W}\right]^2} < 0. \end{cases} \tag{44}$$

T_0 is strictly increasing with parameters β and γ (see Figures 6 and 7) and strictly decreasing with ϕ, τ, μ, and C_W (see Figures 8–11).

Some reasonable suggestions for computers on the client prat to mitigate the DDoS attack are provided as follows based on the preceding calculation:

(1) Adopting some defensive strategies (e.g., installing firewalls) on the client part, the infected probability β can be remarkably reduced.

(2) Keeping defensive software updates in time on the client part, γ can be maintained low.

(3) Upgrading antivirus software, τ will be enhanced.

(4) Strengthening defense strength on the client part will enhance ϕ.

(5) Decreasing the cost of the defending strategy will reduce C_W.

Accordingly, controlling the preceding parameters will be conducive to the mitigation of DDoS attacks on the client part. Thereafter, we focus on the defensive strategies for computers on the server part.

As $C_1 = \delta\alpha I_1/\alpha I_1(\eta+\delta)+\eta(g_1+\delta)$, where $g_1 = \varphi e^{\nu C_S}/e^{\nu C_S}+e^{\nu N_S \alpha L_S I_1}$, parameters δ, α, ν, φ, η, N_S, C_S, and L_S are independent of I_1. Thus, we investigate the effects of these parameters on C_1:

$$\frac{\partial C_1}{\partial \delta} = \frac{\alpha I_1(\alpha I_1\eta+\eta g_1)}{\left[\alpha I_1(\eta+\delta)+\eta(g_1+\delta)\right]^2} > 0. \tag{45}$$

C_1 is strictly increasing with parameter δ:

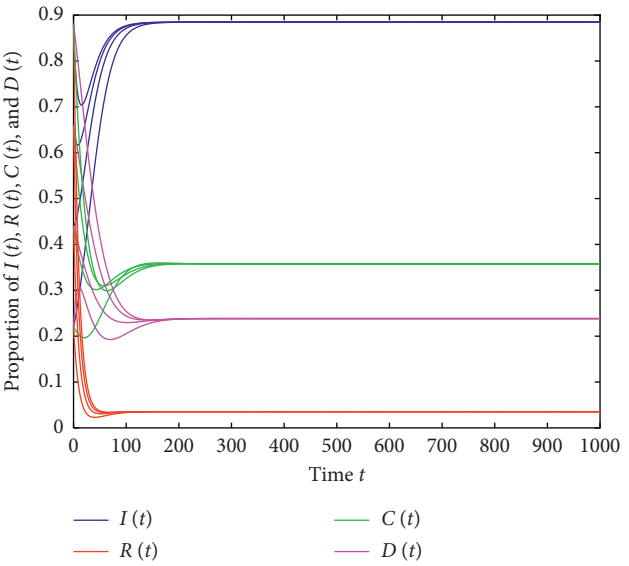

Figure 5: Stability of the attacked solution E_1.

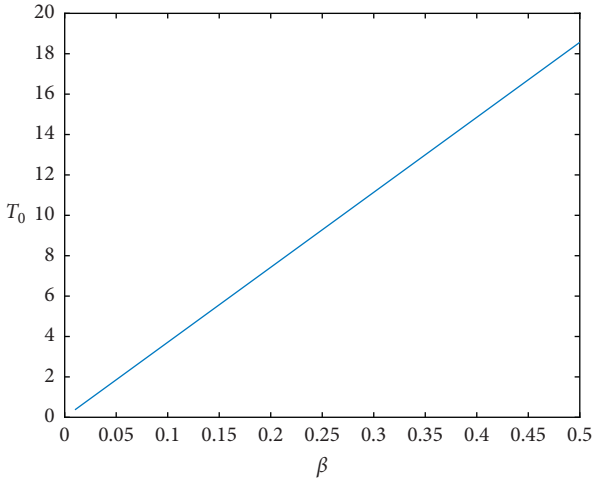

Figure 6: T_0 versus β in the case where $\gamma = 0.1$, $\phi = 0.6$, $\tau = 0.005$, $\mu = 1$, and $C_W = 1$.

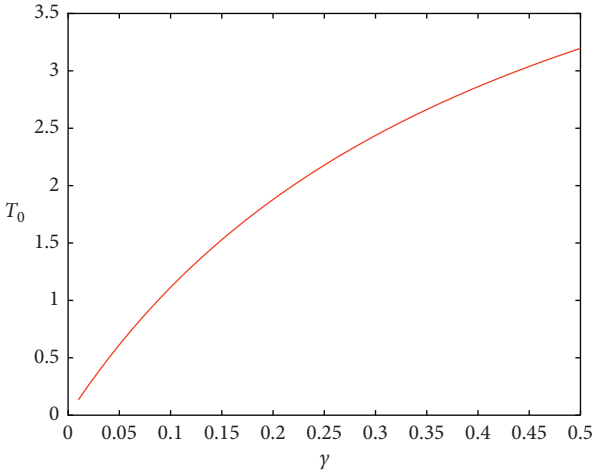

Figure 7: T_0 versus γ in the case where $\beta = 0.03$, $\phi = 0.6$, $\tau = 0.005$, $\mu = 1$, and $C_W = 1$.

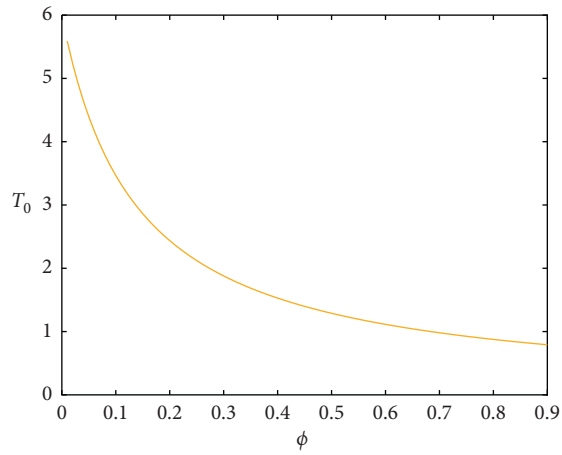

Figure 8: T_0 versus ϕ in the case where $\beta = 0.03$, $\gamma = 0.1$, $\tau = 0.005$, $\mu = 1$, and $C_W = 1$.

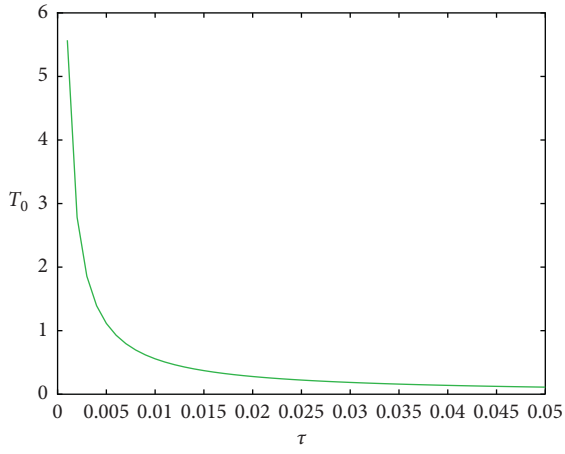

Figure 9: T_0 versus τ in the case where $\beta = 0.03$, $\gamma = 0.1$, $\phi = 0.6$, $\mu = 1$, and $C_W = 1$.

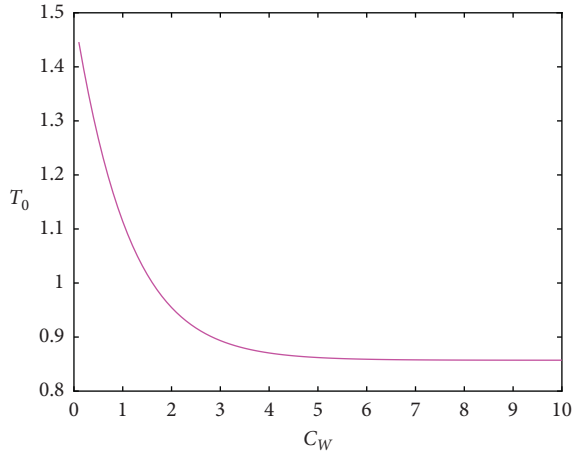

Figure 10: T_0 versus C_W in the case where $\beta = 0.03$, $\gamma = 0.1$, $\phi = 0.6$, $\mu = 1$, and $\tau = 0.005$.

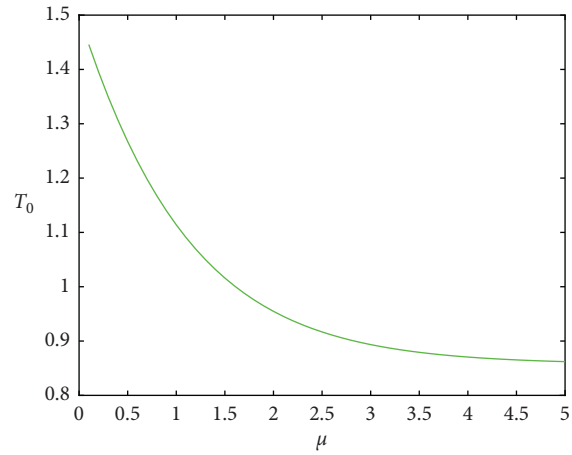

Figure 11: T_0 versus μ in the case where $\beta = 0.03$, $\gamma = 0.1$, $\phi = 0.6$, $C_W = 1$, and $\tau = 0.005$.

$$C_1 = \frac{\delta I_1}{I_1(\eta + \delta) + \eta 1/\alpha\left(\left(\varphi e^{\nu C_S}/e^{\nu C_S} + e^{\nu N_S \alpha L_S I_1}\right) + \delta\right)}. \quad (46)$$

From the preceding form of C_1, we can see that C_1 increases with an increase in α.

$$C_1 = \frac{\delta \alpha I_1}{\alpha I_1(\eta + \delta) + \eta\left(\left(\varphi/1 + e^{\nu\left(N_S \alpha L_S I_1 - C_S\right)}\right) + \delta\right)}. \quad (47)$$

From the form of C_1, we can see that C_1 increases with an increase in ν, N_S, and L_S, and C_1 decreases with an increase in φ, η, and C_S.

The following defense strategies are proposed for computers on the server part to deduce DDoS attacks:

(1) Detecting possible security holes may facilitate the reduction in α.

(2) Restarting computers on the server part will significantly increase η.

(3) Upgrading defensive software of DDoS attack, δ will decrease.

(4) Strengthening defense strength on the server part will enhance φ.

(5) Decreasing the cost of the defending strategy will reduce C_S.

(6) Increasing the number of computers on the server part facilitates the enhancement of N_S.

Controlling these parameters is conducive to the mitigation of DDoS attacks on the server part.

5. Conclusion

This paper studies the decision-making problem of DDoS attack defense strategy. In order to mitigate DDoS risk with minimum defending loss and cost, based on game theory, this paper establishes a dynamic differential system with the defense cost and loss function. We perform analytical analysis to show that the attack model has two equilibria, i.e., an attack-free equilibrium E_0 and an attacked equilibrium

E_1. The attacked threshold T_0 is an important parameter that determines whether DDoS attacks are successful or failed. Some beneficial recommendations to mitigate DDoS attacks are provided after conducting some numerical experiments of the proposed model with different parameters. These suggestions for effective defense against DDoS attacks include installing firewalls, upgrading antivirus software, reducing defense costs, and detecting possible security holes. This research not only has strong theoretical value but can also be widely used in the following fields: (1) advanced persistent threats: study the dynamic behavior of DDoS attack and defense with advanced persistent threat characteristics [30, 31]; (2) Honeynet defense: study the influence of honeynet defense on the dynamic behavior of DDoS attacks [32]; (3) smart grid: study the dynamic behavior of DDoS attack and defense on the smart grid [16].

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM Special Interest Group on Data Communication*, vol. 34, no. 2, pp. 39–53, 2004.

[2] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[3] P. Passeri, "Cyber attacks statistics," 2016.

[4] P. Passeri, "Symantec internet security threat report," 2019.

[5] S. Sharwood, "Winter olympics website downed by cyber attack," 2020.

[6] S. Ranger, "GitHub hit with the largest DDoS attack ever seen," 2020.

[7] N. Arboleda, "AWS hit by DDoS attack dragging half of web down," 2020.

[8] K. Haldar and B. K. Mishra, "A mathematical model for a distributed attack on targeted resources in a computer network," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 9, pp. 3149–3160, Sep. 2014.

[9] U. Kumar and S. K. Pandey, "Dynamic model on DDoS attack in computer network," 2016.

[10] W. T. Hou and H. Wang, "Study of a mathematical model for a distributed attack on targeted resources in a computer network," *Journal of Natural Science of Heilongjiang University*, vol. 3, pp. 315–321, 2016.

[11] B. K. Mishra, A. K. Keshri, D. K. Mallick, and B. K. Mishra, "Mathematical model on distributed denial of service attack through Internet of things in a network," *Nonlinear Engineering*, vol. 8, no. 1, pp. 486–495, 2018.

[12] C. Zhang and J. Xiao, "Stability analysis of an advanced persistent distributed denial-of-service attack dynamical model," *Security and Communication Networks*, vol. 2018, pp. 1–10, 2018.

[13] C. M. Zhang, J. B. Peng, and J. W. Xiao, "Advanced persistent distributed denial of service attack model on scale-free networks," 2018.

[14] C. M. Zhang, J. B. Peng, and J. W. Xiao, "An advanced persistent distributed denial-of-service attacked dynamical model on networks," *Discrete Dynamics in Nature and Society*, vol. 2019, 2019.

[15] Y. S. Rao, A. K Keshri, B. K. Mishra, and T. C. Pand, "Distributed denial of service attack on targeted resources in a computer network for critical infrastructure: a differential e-epidemic model," *Physica A: Statistical Mechanics and Its Applications*, vol. 2019, 2019.

[16] C. Zhang, F. Luo, M. Sun, and G. Ranzi, "Modeling and defending advanced metering infrastructure subjected to distributed denial-of-service attacks," *IEEE Transactions on Network Science and Engineering*, vol. 99, p. 1, 2020.

[17] K. Huang, L. X. Yang, X. Yang, Y. Xiang, and Y. Y. Tang, "A low-cost distributed denial-of-service attack architecture," *IEEE Access*, vol. 99, pp. 1–9, 2020.

[18] Z. Li, H. Jin, D. Zou, and B. Yuan, "Exploring new opportunities to defeat low-rate DDoS attack in container-based cloud environment," *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, no. 3, pp. 695–706, 2020.

[19] X. Zhong, F. Deng, and H. Ouyang, "Sharp threshold for the dynamics of a SIRS epidemic model with general awareness-induced incidence and four independent brownian motions," *IEEE Access*, vol. 8, pp. 29648–29657, 2020.

[20] E. González and M. J. Villena, "On the spatial dynamics of vaccination: a spatial SIRS-V model," *Computers & Mathematics with Applications*, vol. 80, no. 5, pp. 733–743, 2020.

[21] H. Zhang, F. Fu, W. Zhang, and B. Wang, "Rational behavior is a 'double-edged sword' when considering voluntary vaccination," *Physica A: Statistical Mechanics and Its Applications*, vol. 391, no. 20, pp. 4807–4815, 2012.

[22] G. Liu, S. Peng, H. Qiu, B. Shi, and Y. W. Chen, "Voluntary vaccination through perceiving epidemic severity in social networks," *Complexity*, vol. 2019, 2019.

[23] J. Yang, M. Martcheva, and Y. Chen, "Imitation dynamics of vaccine decision-making behaviours based on the game theory," *Journal of Biological Dynamics*, vol. 10, no. 1, pp. 31–58, 2016.

[24] F. Xu and C. Ross, "Disease control through voluntary vaccination decisions based on the smoothed best response," *Computational and Mathematical Methods in Medicine*, vol. 2014, 2014.

[25] J. S. Cramer, *Logit Models from Economics and Other Fields*, Cambridge University Press, Cambridge, UK, 2003.

[26] X. Zhou and J. Cui, "Analysis of stability and bifurcation for an SEIV epidemic model with vaccination and nonlinear incidence rate," *Nonlinear Dynamics*, vol. 63, no. 4, pp. 639–653, 2011.

[27] C. Gan, X. Yang, W. Liu, and Q. Zhu, "A propagation model of computer virus with nonlinear vaccination probability," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 92–100, 2014.

[28] R. C. Robinson, "An introduction to dynamical systems: continuous and discrete," *American Mathematical Society*, vol. 2012, 2012.

[29] 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, 2017.

[30] L.-X. Yang, P. Li, Y. Zhang, X. Yang, Y. Xiang, and W. Zhou, "Effective repair strategy against advanced persistent threat: a

differential game approach," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1713–1728, 2019.

[31] L.-X. Yang, P. Li, X. Yang, Y. Xiang, F. Jiang, and W. Zhou, "Effective quarantine and recovery scheme against advanced persistent threat," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 1, 2020.

[32] J. Ren, C. Zhang, and Q. Hao, "A theoretical method to evaluate honeynet potency," *Future Generation Computer Systems*, vol. 116, pp. 76–85, 2021.