symmetry

MDPI

Article

A Novel Model for Distributed Denial of Service Attack Analysis and Interactivity

Ashraf Ahmad [1], Yousef AbuHour [2,*] and Firas Alghanim [1]

[1] King Hussein School of Computing Sciences, Princess Sumaya University for Technology, Amman 11941, Jordan; a.ahmad@psut.edu.jo (A.A.); f.ghanim@psut.edu.jo (F.A.)
[2] Jordan Design Development Bureau (JODDB), National Encryption Center, Amman 11180, Jordan
* Correspondence: yousef.abu.hour@gmail.com

Abstract: A Distributed Denial of Service (DDoS) attack is a type of cybercrime that renders a target service unavailable by overwhelming it with traffic from several sources (attack nodes). In this paper, we focus on DDoS attacks on a computer network by spreading bots throughout the network. A mathematical differential equation model is proposed to represent the dynamism of nodes at different compartments of the model. The model considers two levels of security, with the assumption that the recovered nodes do not return to the same security level. In previous models, the recovered nodes are returned to be suspect on the same security level, which is an unrealistic assumption. Moreover, it is assumed that the attacker can use the infected target nodes to attack again. With such epidemic-like assumptions of infection, different cases are presented and discussed, and the stability of the model is analyzed as well; reversing the symmetry transformation of attacking nodes population is also proven. The proposed model has many parameters in order to precisely describe the infection movement and propagation. Numerical simulation methods are used to solve the developed system of equations using MATLAB, with the intention of finding the best counteraction to control DDoS spread throughout a network.

Keywords: computer networks; differential equations; dynamic equilibrium; network servers; non-linear dynamical systems; non-linear equations; numerical analysis; numerical simulation

Citation: Ahmad, A.; AbuHour, Y.; Alghanim, F. A Novel Model for Distributed Denial of Service Attack Analysis and Interactivity. *Symmetry* **2021**, *13*, 2443. https://doi.org/10.3390/sym13122443

Academic Editor: Jan Awrejcewicz

Received: 10 November 2021
Accepted: 7 December 2021
Published: 17 December 2021

1. Introduction

A Denial of Service attack (DoS attack) is a cyberattack in which the attacker attempts to reduce the access or completely shut down the resources of either a machine or a network and make them unavailable to their legitimate users [1]. The DoS attack has been known to the scientific community since the early 1980s. In 1983, Gligor provided one of the first descriptions of a DoS attack in an operating system [1].

A Distributed Denial of Service (DDoS) attack is a large-scale DoS attack in which the attacking system consists of a large number of compromised computers that are targeting the victim's system. Usually, a DDoS attack consists of two stages; in the first stage, the attacking system compromises a large number of vulnerable computers in order to use them as a part of the attacking attempt during the second stage, wherein the victim's system is attacked.

A famous example was in July 2001, when more than 350,000 computers were infected with the Code Red worm in less than 14 h. Then, the worm attempted to launch a DDoS attack against the White House website. However, it was easy to disable the second stage of the attack due to its features [2].

An example of a DoS attack is the SYN flood attack in which the attacker exploits part of the Transmission Control Protocol (TCP), specifically, the handshake process. TCP is a host-to-host communication protocol designed to send data packets over the Internet. In this attack, the attacking system repeatedly sends SYN packets to the victim's system without responding to the SYN/ACK packets sent by the server. Thus, the connection

remains in a half-open state, and due to a large number of connections, the victim's system cannot respond to any new connection. One of the early SYN flood attacks occurred in September 1996, when an attacker shut down the New York City Internet service provider, Panix, for almost a week [3]. In the first quarter of 2018, 57.3% of DDoS attacks were SYN flood attacks [4].

Another protocol that can be misused to attack the victim's system is the Internet Control Message Protocol (ICMP). ICMP is a supporting protocol that is used to send error messages and operational information. In the first quarter of 2018, 6.1% of DDoS attacks were ICMP attacks [4]. An example of ICMP flooding attacks is the ping flooding attack, which is one of the simplest DoS attacks. Ping is a computer network utility to test the reachability of a host on a particular Internet Protocol (IP) address. In the ping flooding attack, the attacking system repeatedly sends more ping packets than the victim's system can handle.

In general, DoS attacks can be categorized into two types: crash the service or flood the service. In the "crash the service" attack, the attacking system aims to crash or freeze the victim's system by exploiting a software vulnerability it has. On the other hand, the "flood the service" attack aims to flood the victim's system with useless traffic in order to overload the system and prevent the legitimate traffic from being served [5].

DDoS attacks can be very dangerous and may cause serious damage. In February 2000, Yahoo, Buy.com, eBay, CNN.com, Amazon.com, Dell, ZDNet, E*Trade, and Excite were targets of a 15-year-old Canadian nicknamed "Mafiaboy" [6,7]. The estimated damages of the attack were $1.7 billion [8].

Another example is Dyn, an Internet performance management and web application security company that was compromised in October 2016. During this time, their Managed Domain Name System (DNS) infrastructure came under two DDoS attacks [9]. These attacks were caused by up to 100,000 malicious endpoints in which a large amount of the traffic originated from Mirai-based botnets [9]. Websites such as Twitter, Spotify, PayPal, HSBC, BankWest, and Ticketmaster suffered from connectivity problems [10]. As a result, 8% of Dyn's customers dropped the company as their DNS service provider [10].

The concept of symmetry is one of the important things that is closely related to systems of differential equations in the theory of dynamical systems. This correlation was discussed in [11–13]. According to [14], considering an autonomous dynamical system of differential equation such as:

$$\frac{d\omega}{dt} = \mathcal{F}(\omega), \tag{1}$$

where $\omega \in \mathbf{R}^n$, and the transformation $\mathcal{T} : \mathbf{R}^n \to \mathbf{R}^n$ is a reversing symmetry of (1) if:

$$\frac{d}{dt}(\mathcal{T}\omega) = -\mathcal{F}(\mathcal{T}\omega), \tag{2}$$

In this case, system (2) is invariant with respect to the transformation $(t, \omega) \to (-t, \mathcal{T})$, which holds in our attack population study and is described in the numerical analysis section.

The problem of stability in dynamic systems is one of the fundamental problems in various fields of science and modern technology [15,16]. Because of its importance, the concept of symmetry and its impact on this work is referred to in the proposed study.

In this work, we use non-linear differential equation systems to describe and analyze DDoS attacks on highly protected systems, such as main enterprise servers, and poorly protected systems, such as normal users' devices. We propose a new variable that illustrates the degree of protection among those different system types in order to study the different possible scenarios, which will lead to a more comprehensive description that covers the impact of such attacks on targeted networks. We also prove that depending on backup servers alone is not an efficient solution for this kind of attacks, but can actually complicate the problem and waste resources. The research also describes the botnet and its effect on the targeted devices, which is an important aspect of the work because we study both the

attacking and the targeted societies. It is also significant to mention that our model is more realistic than others because the recovered nodes will have high-level security after the attack, which is an assumption that has usually been omitted in previous models. Moreover, this dynamical system of equation is generally much faster than botnet simulation, although the simulation is more accurate. Other techniques, such as machine learning, have been used to learn the behavior of DDoS and botnet; however, they do not give the analytical strength and dynamics of an equations model approach.

The rest of this paper is organized as follows: Background and relevant literature are presented in Section 2. The model formulation, design, and basic properties are introduced in Section 3. Section 4 presents the numerical analysis and discussion to approximate the solution and show the stability and comparison. Finally, Section 5 concludes the paper.

2. Background

DDoS, or Distributed Denial of Service, is a common cyberattack technique that hackers favor since it is not easy to counter, allows the attacker to remain undetected, and has a low attack cost [17]. In a typical Denial of Service (DoS) attack, attackers attempt to block one or more servers on the network from serving legitimate users. This type of assault is known as Distributed Denial of Service (DDoS) since it originates from multiple sources [18,19]. Attackers can infect a node by injecting a kind of Trojan horse, for example, in a variety of ways, including embedding it in free games or media downloads, or by attaching it to emails. The attacker then uses the injected code to interact with an external entity, which starts a massive attack on the victim's nodes, preventing them from working and providing the necessary services correctly [20].

In DDoS, it is critical to look into the propagation characteristics of infection. Suspicious objects can easily spread throughout a network, posing a major security risk. Because the network infrastructure must be resistant to these attacks, the isolation of infected nodes is essential for avoiding the spread of the infection. Infected nodes are disconnected from the rest of the network until they can be recovered. So far, the containment strategy's intervention has resulted in significant modifications in infection solutions, which have been fine tuned to protect systems from DDoS attacks. To comprehend and analyze these attacks, mathematical models have been developed [21]. Because infection via malicious objects is analogous to real diseases, the epidemic model has proven to be a valuable tool for understanding how they propagate throughout a computer network [22,23]. Epidemiological models are essentially dynamic since they divide the entire population of nodes into multiple compartments, such as infected, susceptible, or recovered [24]. Differential equations can describe the movement of a node from one compartment to another. This system is then examined to see whether or not stability has been achieved. Another advantage of such models is the inclusion of an epidemic threshold, which aids in determining whether the epidemic will persist or go away [25].

Several researchers have utilized mathematical techniques to create a model of the DDoS attack that can be investigated and analyzed. Mishra et al. [26] created a model to simulate a cyberattack on an IoT network based primarily on the Mirai botnet malware. They looked at the model's equilibrium and stability and ran numerical simulations of several scenarios. The model was created to analyze a DDoS attack spread on a targeted network using a previously constructed IoT botnet and to explain the wireless transmission of attacks in a network that could create a zombie army. Zhang [27] used a game theory-based DDoS attack model to address some of the flaws in earlier assumptions, such as the idea that defenders will utilize a fixed-probability defending technique or that they will not adopt defense tactics because of defensive costs. Zhang [27] developed two smooth logistic functions to represent the defender's defense strategy options under various cost–benefit scenarios in order to investigate the impact of defense strategy decisions on the dynamic behavior of DDoS attacks. They also used the theory of differential stability to find the attack threshold, which determines the conditions for a successful attack, and to prove the attack equilibrium and the attack-free equilibrium.

3. Model Formulation and Basic Properties

The model is designed by splitting the total network into attack and target populations at time t. The attack population has the following two compartments: a percentage of the susceptible, denoted by $S_a(t)$, and a percentage of the infectious, denoted by $I_a(t)$. Hence, the total percentage of this population is $S_a(t) + I_a(t) = 1$.

On the other hand, we assumed that the target population was divided into two sub-populations, which are:

(i) Low-security population, which has the following three compartments: a percentage of the susceptible, denoted by $S_l(t)$, a percentage of the infectious, denoted by $I_l(t)$, and a percentage of the recovered, denoted by $R_l(t)$;
(ii) High-security population, which has the following three compartments: a percentage of the susceptible, denoted by $S_h(t)$, a percentage of the infectious, denoted by $I_h(t)$, and a percentage of the recovered, denoted by $R_h(t)$.

Therefore, the total percentage of this population is $S_l(t) + I_l(t) + R_l(t) + S_h(t) + I_h(t) + R_h(t) = 1$.

The equations of the model are obtained as follows: Nodes are recruited into the attack population at a rate μ. Susceptible nodes of the attack population may be infected with infectious nodes at rate βI, in which β is the effective contact rate. The attack population is decreased by natural death, μ, and the recovery rate of target population nodes that become suspicious again is ξ. Thus, the changing rate of the attack population for both susceptible and infected nodes are given, respectively, by the following:

$$\begin{aligned} \frac{dS_a}{dt} &= \mu - \beta S_a I_a - \mu S_a + \xi I_a, \\ \frac{dI_a}{dt} &= \beta S_a I_a - (\xi + \mu) I_a. \end{aligned} \tag{3}$$

Lemma 1. *The transformation $\mathcal{T} : \mathbf{R}^n \to \mathbf{R}^n$ is a reversing symmetry for an invariable attack population, without disconnected nodes.*

Proof. $\mu = 0$ since the population is invariable, and all nodes are connected for the run time of the DDoS attack. Now, by letting $(t, \mathbf{x}) \to (-t, \mathcal{T}\mathbf{x})$ for $\mathbf{x} = (S_a, I_a)$, where $\mathcal{T}(S_a, I_a) = (I_a, S_a)$, then the proof of the lemma can clearly be concluded. □

Target susceptible nodes may be infected at rate λ:

$$\lambda = \beta[I_a + \eta(I_h + I_l)], \tag{4}$$

where η is the modification parameter which accounts for the attack transmission of the infected target nodes for the assumed reduction (in the I_l and I_h compartments). Furthermore, the infected nodes are recovered at a rate γ_l, and the recovered nodes are fortified at a rate ξ_l in order to become suspect at a high-security level.

Thus, the changing rate of the low-security population of the susceptible, infected, and recovered nodes are given, respectively, by the following:

$$\begin{aligned} \frac{dS_l}{dt} &= -\lambda S_l, \\ \frac{dI_l}{dt} &= \lambda S_l - \gamma_l I_l, \\ \frac{dR_l}{dt} &= \gamma_l I_l - \xi_l R_l. \end{aligned} \tag{5}$$

It is further assumed that the high-security level is imperfect, so that the high-security susceptible nodes may be infected at a reduced rate $(1 - \epsilon)\lambda$, in which ϵ represents the firewall efficiency.

Additionally, the infected nodes are recovered at a rate γ_h, then these recovered nodes may be infected again at a rate ξ_h.

Thus, the changing rate of the low-security population of the susceptible, infected, and recovered nodes are given, respectively, by the following equations:

$$\begin{aligned}
\frac{dS_h}{dt} &= -\lambda(1-\epsilon)S_h + \xi_h R_h + \xi_l R_l, \\
\frac{dI_h}{dt} &= \lambda(1-\epsilon)S_h - \gamma_h I_h, \\
\frac{dR_h}{dt} &= \gamma_h I_h - \xi_h R_h.
\end{aligned}$$

Combining the aforementioned derivations and assumptions, the model of the DDoS attack on a computer network is expressed in the following equations, model (6), with a schematic presentation in Figure 1, and a description of the parameters in Table 1.

$$\begin{aligned}
\frac{dS_a}{dt} &= \mu - \beta S_a I_a - \mu S_a + \xi I_a, \\
\frac{dI_a}{dt} &= \beta S_a I_a - (\xi + \mu) I_a, \\
\frac{dS_l}{dt} &= -\lambda S_l, \\
\frac{dI_l}{dt} &= \lambda S_l - \gamma_l I_l, \\
\frac{dR_l}{dt} &= \gamma_l I_l - \xi_l R_l, \\
\frac{dS_h}{dt} &= -\lambda(1-\epsilon)S_h + \xi_h R_h + \xi_l R_l, \\
\frac{dI_h}{dt} &= \lambda(1-\epsilon)S_h - \gamma_h I_h, \\
\frac{dR_h}{dt} &= \gamma_h I_h - \xi_h R_h.
\end{aligned} \tag{6}$$

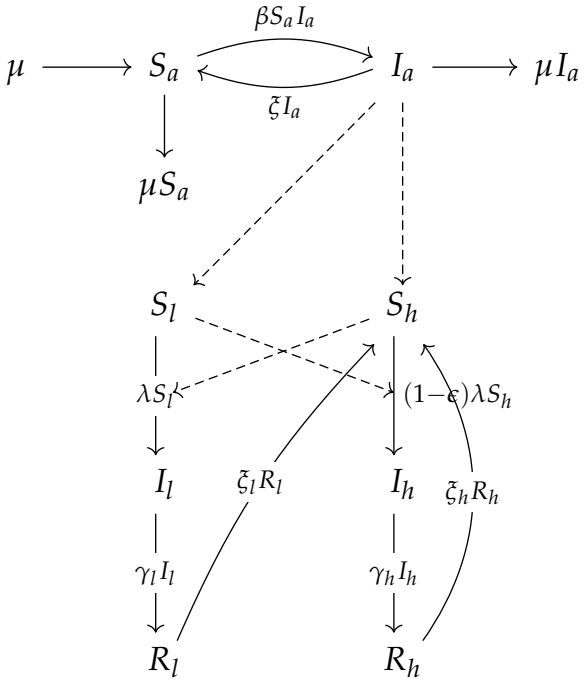

Figure 1. Schematic presentation of the target and attack populations of DDoS.

Table 1. Description of the system's parameters (6).

Parameter	Description
μ	recruitment rate
η	modification parameter that accounts for the attack transmission of the infected target nodes for the assumed reduction (in the I_l, I_h compartments)
β	effective contact rate
β_h	effective contact rate of the high-security population
β_l	effective contact rate of the low-security population
γ_h	rate of recovered high-security infected nodes
γ_l	rate of recovered low-security infected nodes
ξ	recovery rate of target population nodes that become suspicious again
ξ_h	rate of recovered high-security nodes that become infected again
ξ_l	rate of recovered low-security nodes that become infected again
ϵ	rate of firewall efficiency

The threshold value $\mathcal{R}_0$ can be defined as the average number of secondary infection nodes that a single infectious node can produce in a totally susceptible population. We first obtain the basic reproduction number separately for each population. The value of $\mathcal{R}_0$ for the target high-security population, denoted by R_{0h}, is defined as follows:

$$R_{0h} = \frac{\beta(1-\epsilon)}{\gamma_h},$$

and for the target low-security population, we have:

$$R_{0l} = \frac{\beta}{\gamma_l},$$

and for the attack population, we have:

$$R_{0a} = \frac{\beta}{\xi + \mu},$$

By combining these values, we can get a single threshold value as in the host–vector models in epidemiology with the use of the notation in [28]. The non-negative matrix, $\mathscr{F}$, of the new infection terms, and the $\mathscr{V}$-matrix of the transition terms associated with model (6) are given, respectively, by the following equations:

$$\mathscr{F} = \begin{pmatrix} \lambda(1-\epsilon)S_h \\ \lambda S_l \\ \beta S_a I_a \end{pmatrix} \text{ and } \mathscr{V} = \begin{pmatrix} \gamma_h I_h \\ \gamma_l I_l \\ (\xi+\mu) I_a \end{pmatrix},$$

the corresponding derivative of the two vector-valued functions, $\mathscr{F}$ and $\mathscr{V}$, are the following:

$$F = \begin{pmatrix} -\beta(\epsilon-1) & -\beta\eta(\epsilon-1) & -\beta\eta(\epsilon-1) \\ \beta & \beta\eta & \beta\eta \\ 0 & 0 & \beta \end{pmatrix} \text{ and } V = \begin{pmatrix} \gamma_h & 0 & 0 \\ 0 & \gamma_l & 0 \\ 0 & 0 & \mu+\xi \end{pmatrix}$$

It then follows that the control reproduction number [29], denoted by $\rho(FV^{-1})$, in which

$$FV^{-1} = \begin{pmatrix} \frac{\beta(1-\epsilon)}{\gamma_h} & \frac{\beta\eta(1-\epsilon)}{\gamma_l} & \frac{\beta\eta(1-\epsilon)}{\mu+\xi} \\ \frac{\beta}{\gamma_h} & \frac{\beta\eta}{\gamma_l} & \frac{\beta\eta}{\mu+\xi} \\ 0 & 0 & \frac{\beta}{\mu+\xi} \end{pmatrix},$$

ρ is defined as the spectral radius (maximum eigenvalue) of FV^{-1}, is given by

$$\begin{aligned} \mathcal{R}_0 = \rho(FV^{-1}) &= \max\{\frac{\beta}{\mu+\xi}, \frac{\beta(1-\epsilon)}{\gamma_h} + \frac{\beta}{\gamma_l}\} \\ &= \max\{R_{0a}, R_{0h} + R_{0l}\}. \end{aligned}$$

In the next subsection, the stability of the DDoS model is introduced. Moreover, it is shown that the threshold value R_{0a} alone can completely determine the overall dynamics of the model (6), and there is no need to consider the value of $\mathcal{R}_0$. On the other hand, if we have a perfect security level ($\epsilon = 1$), then the attack effect will disappear with time.

3.1. Local Stability of Infection-Free Equilibrium

In this subsection, we will investigate the stability of the proposed model (6). Furthermore, we will analyze the effect of the firewall efficiency at the high-security level ϵ. The free infection point of model (6) is as follows:

$$P_0 = (S_a^0, I_a^0, S_l^0, I_l^0, R_l^0, S_h^0, I_h^0, R_h^0) = (S_a^0, 0, S_l^0, 0, 0, S_h^0, 0, 0),$$

in which $S_a^0 = 1$ and $S_l^0 + S_h^0 = 1$. The variables $(S_a, I_a, S_l, I_l, R_l, S_h, I_h, R_h)$ of model (6) are non-negative with time. In other words, the solutions of the model (6) system with positive initial data will remain positive at time t. This finding is shown in Theorem 1.

Theorem 1. *The closed set* $D = \{x = (S_a, I_a, S_l, I_l, R_l, S_h, I_h, R_h) \in R_+^8 : x_i \geq 0, S_a + I_a \leq 1$ *and* $S_l + I_l + R_l + S_h + I_h + R_h \leq 1\}$ *is positive invariant.*

The proposed model (see Figure 1), given by model (6), is locally asymptotically stable (LAS) at the infection-free equilibrium P_0 *if* $\mathcal{R}_0 \leq 1$, *and unstable if* $\mathcal{R}_0 > 1$.

The existence of endemic equilibria (that is, equilibria where the infected compartments of the model are non-zero) of model (6) is established. Let $P_* = (S_a^*, I_a^*, S_l^*, I_l^*, R_l^*, S_h^*, I_h^*, R_h^*)$ represent any arbitrary endemic equilibrium point of model (6). To simplify the proposed model, we can solve the system of the attack population by solving the first and second equations in model (6) and get the following:

$$\frac{dI_a}{dt} = \beta(1 - I_a)I_a - (\xi + \mu)I_a \text{ and } S_a = 1 - I_a.$$

Hence, the solution is as follows:

$$\begin{aligned} I_a &= \frac{(\xi + \mu - \beta)\exp[(\xi + \mu - \beta)(t - I_a(0))]}{\beta\exp[(\xi + \mu - \beta)(t - I_a(0))] + 1}, \\ S_a &= 1 - \frac{(\xi + \mu - \beta)\exp[(\xi + \mu - \beta)(t - I_a(0))]}{\beta\exp[(\xi + \mu - \beta)(t - I_a(0))] + 1}, \end{aligned} \tag{7}$$

Since the formula we get is explicit, we can easily study the stability of the attack population by taking the limit of (7):

$$\lim_{t\to\infty} \frac{(\xi + \mu - \beta)\exp[(\xi + \mu - \beta)(t - I_a(0))]}{\beta\exp[(\xi + \mu - \beta)(t - I_a(0))] + 1} = \frac{\beta - \xi - \mu}{\beta} \tag{8}$$

$$= I^*, \tag{9}$$

if $\xi + \mu - \beta < 0$.

Furthermore, let

$$\lambda^* = \beta(I_a^* + \eta(I_h^* + I_l^*)). \tag{10}$$

When $\mathcal{R}_0 > 1$, then for a long time t (as t goes to infinity), the low-security population will be $S_l^* = I_l^* = R_l^* = 0$ (at endemic equilibria P^*), because the attack consumes all devices in the low-security population. On the other hand, the high-security population at the steady state of the system is the following:

$$I_h^* = \frac{\xi_h(1-\epsilon)\lambda^*}{\lambda^*(1-\epsilon)(\gamma_h+\xi_h)+\xi_h\gamma_h},$$

substitute model (6) in order to get:

$$\lambda^* = \beta\left(I_a^* + \frac{\eta\xi_h(1-\epsilon)\lambda^*}{\lambda^*(1-\epsilon)(\gamma_h+\xi_h)+\xi_h\gamma_h}\right), \tag{11}$$

rewrite (11) as the following:

$$a\lambda^{*2} + b\lambda^* + c = 0, \tag{12}$$

in order to get:

$$(1-\epsilon)(\gamma_h+\xi_h)\lambda^{*2} - [-\xi_h\gamma_h + \beta I_a^*(\gamma_h+\xi_h)(1-\epsilon) + \eta\beta\xi_h(1-\epsilon)]\lambda^* - \beta\xi_h\gamma_h I_a^* = 0,$$

$$(1-\epsilon)(\gamma_h+\xi_h)\lambda^{*2} - [-\xi_h\gamma_h + [(\beta-\xi-\mu)(\gamma_h+\xi_h) + \eta\beta\xi_h](1-\epsilon)]\lambda^* - \beta\xi_h\gamma_h\left(1-\frac{1}{R_{0a}}\right) = 0, \tag{13}$$

Based on (13), we can obtain the result in Theorem 2.

Theorem 2. *Model (6) has*

- *a unique endemic equilibrium if* $c < 0 \Leftrightarrow R_{0a} > 1$;
- *a unique endemic equilibrium if* $(b < 0$ *and* $c = 0)$ *or* $b^2 - 4ac = 0$;
- *two endemic equilibria if* $c > 0$, $b < 0$ *and* $b^2 - 4ac > 0$;
- *no endemic equilibrium otherwise.*

Case 1 shows that the model has a unique endemic equilibrium whenever $R_{0a} > 1$. While Case 3 shows that backward bifurcation is possible when

$$\mathcal{R}_0^c = 1 - \frac{[-\xi_h\gamma_h + \beta I_a^*(\gamma_h+\xi_h)(1-\epsilon) + \eta\beta\xi_h(1-\epsilon)]^2}{4(1-\epsilon)(\gamma_h+\xi_h)\beta\xi_h\gamma_h(1/R_{0h})},$$

Backward bifurcation is where locally asymptotically stable infection-free equilibrium and locally asymptotically stable endemic equilibrium co-exist.

3.2. No High-Security Level

In this subsection, we will analyze the proposed model when $\epsilon = 0$ (if there is no high-security level, the firewall efficiency drops). In this case, the recovered nodes return to be infected again. But when $\epsilon \neq 0$, the recovered nodes in the low-security level return to the S compartment in the high-security level.

If $\epsilon = 0$, we can conclude about parameters in the high-security population: the parameters in the target population are equal, i.e., $\xi_l = \xi_h$ and $\gamma_l = \gamma_h$, which means that

the attack is equally effective on both low and high populations. The system of the target population becomes:

$$\begin{aligned} \frac{dS_t}{dt} &= -\lambda S_t + \xi_t R_t, \\ \frac{dI_t}{dt} &= \lambda S_t - \gamma_t I_t, \\ \frac{dR_t}{dt} &= \gamma_t I_t - \xi_t R_t, \end{aligned} \tag{14}$$

in which $\lambda = \beta(I_a + \eta I_t)$, $S_t = S_l + S_h$, $I_t = I_l + I_h$, and $R_t = R_l + R_h$. In addition, the system of the attack population is still the same:

$$\begin{aligned} \frac{dS_a}{dt} &= \mu - \beta S_a I_a - \mu S_a + \xi I_a, \\ \frac{dI_a}{dt} &= \beta S_a I_a - (\xi + \mu) I_a. \end{aligned}$$

The system is infection-free (weak attack) at $P_0 = (1, 0, 1, 0, 0)$. The system is infected (successful attack) at the steady state, since $R_t = 1 - S_t - I_t$ and from the second equation of (system (14)):

$$S_t = \frac{\gamma_t I_t}{\beta(I^* + \eta I_t)}, \tag{15}$$

substitute Equation (15) in the first equation of (14) to get the value of I_t, which is the positive solution of the following quadratic equation:

$$-\beta\eta(\gamma_t + \xi_t) I_t^2 - (\beta\eta + \gamma_t\xi_t + \beta I_a^* - \xi_t\beta) I_t + \xi_t \beta I_a^* = 0 \tag{16}$$

Clearly, there is a unique positive solution for Equation (16) when $I_a^* \neq 0$ (infected solution), then I_t^0 is the positive solution of Equation (16). Therefore, $P^* = (S_a^*, I_a^*, S_t^*, I_t^*, R_t^*)$ is the infected solution. It can be noticed that from Equation (16), if $I_a^* = 0$, then $I_t^* = 0$. Thus, the reproduction number is as follows:

$$\mathcal{R}_0 = \max\left\{\frac{\beta}{\gamma_t}, \frac{\beta}{\xi+\mu}\right\} \text{ where } \frac{\beta}{\gamma_t} = R_{0t} \text{ and } \frac{\beta}{\xi+\mu} = R_{0a}.$$

Theorem 3. *The infection-free equilibrium P_0 of system (17) is locally asymptotically stable in D if $\mathcal{R}_0 < 1$ and is unstable if $\mathcal{R}_0 > 1$.*

$$J(P_0) = \begin{bmatrix} -\xi_t & -\xi_t - \beta\,\eta & -\beta \\ 0 & \beta\,\eta - \gamma_t & \beta \\ 0 & 0 & \beta - \mu - \xi \end{bmatrix}, \tag{17}$$

in which J is the Jacobian matrix. The characteristic equation for this matrix is given as follows:

$$(\nu + \xi_t)(\nu - \beta\,\eta + \gamma_t)(\nu - \beta + \mu + \xi) = 0$$

The roots of the characteristic equation are the eigenvalues of Equation (17), in which $\nu_1 = -\xi_t$, $\nu_2 = \beta\,\eta - \gamma_t$, and $\nu_3 = \beta - (\mu + \xi)$. The second and third eigenvalues become negative when the following conditions are met: $\beta\,\eta - \gamma_t < 0$ and $\beta - (\mu + \xi) < 0$, which are equivalent to both $R_{0t} < 1$ and $R_{0a} < 1$, imply $\mathcal{R}_0 < 1$.

Theorem 4. *The infection-free equilibrium P^* of system (18) is locally asymptotically stable if $\mathcal{R}_0 > 1$.*

$$J(P^*) = \begin{bmatrix} -\beta(I^* + \eta I_t^*) - \xi_t & -\beta\eta - \xi_t & -\beta S_t^* \\ \beta(I^* + \eta I_t^*) & \beta\eta S^* - \gamma_t & \beta S_t^* \\ 0 & 0 & -2\beta I_a^* + \beta - (\xi + \mu) \end{bmatrix}, \tag{18}$$

One of the eigenvalues is $-2\beta I_a^* + \beta - (\xi + \mu)$, which is reduced to become $-(\beta - (\xi + \mu)) < 0$, and is equivalent to $R_{0a} > 1$. The other two eigenvalues are the roots of the characteristic equation of (17):

$$\nu^2 + [\beta(I_a^* + \eta I_t^*) - \beta\eta S_t^* + \gamma_t]\nu + \beta(I_a^* + \eta I_t^*)(-\beta\eta S_t^* + \gamma_t) + \beta(\beta + \xi_t)(I_a^* + \eta I_t^*) = 0. \tag{19}$$

To get the negative sum and the positive product of the roots in Equation (19), the following condition must be met: $-\beta\eta S_a^* + \gamma_t < 0$, so, $1 < \dfrac{\beta\eta S_a^*}{\gamma_t} < R_{0t}$.

Hence, the endemic equilibrium P^* is locally asymptotically stable if $\mathcal{R}_0 > 1$.

Theorem 5. *The positive equilibrium point $P^* = (S_t^*, I_t^*, R_t^*)$ is globally asymptotically stable whenever $\mathcal{R}_0 > 1$.*

Proof.

$$\begin{aligned}
L(S_t, I_t) &= S_t - S_t^* \ln S_t + I_t - I_t^* \ln I_t \\
\frac{\partial L}{\partial t} &= S_t' - \frac{S_t^*}{S_t} S_t' + I_t' - \frac{I_t^*}{I_t} I_t' \\
&= -\lambda S_t + \xi_t R_t - \frac{S_t^*}{S_t}(-\lambda S_t + \xi_t R_t) \\
&+ \lambda S_t - \gamma_t I_t - \frac{I_t^*}{I_t}(\lambda S_t - \gamma_t I_t) \\
&= \xi_t R_t + \lambda S_t^* - \xi_t R_t \frac{S_t^*}{S_t} - \gamma_t I_t - \frac{I_t^*}{I_t}\lambda S_t - \gamma_t I_t^* \\
&= \xi_t R_t \left(1 - \frac{S_t^*}{S_t}\right) + \lambda S_t^* \left(1 - \frac{I_t^*}{I_t}\right) + \gamma_t I_t^* \left(-1 - \frac{I_t}{I_t^*}\right).
\end{aligned}$$

Let $\Gamma(R_t, \lambda) = \max\{\xi_t R_t, \lambda S_t^*, \gamma_t I_t^*\}$, $x = \frac{S_t^*}{S_t}$ and $y = \frac{I_t^*}{I_t}$

$$\begin{aligned}
\frac{\partial L}{\partial t} &= \Gamma(1 - \frac{S_t^*}{S_t} + 1 - \frac{I_t^*}{I_t} - 1 - \frac{I_t}{{}_t I^*}) \\
&= \Gamma\left(2 - y - \frac{1}{y}\right) + \Gamma(-1 - x).
\end{aligned} \tag{20}$$

Since the arithmetic mean is not less than the geometric mean, then $2 - x - \frac{1}{x} \leq 0$, and the equality holds if and only if $x = 1 \rightarrow I_t = I_t^*$. The time derivative of the Lyapunov function is negative from Equation (20). Thus, it follows from La Salle's Invariance Principle that the steady-state point P^* is globally asymptotically stable [30]. □

If we ignore the effect of the target population that attacks used, i.e., $\eta = 0$, then in this case $\lambda = \beta I_a$, substitute in (14); the obtained system will have the same result as that which Bimal et al. achieved [22], and the attack population will still be the same as in (3).

$$\begin{aligned}
\frac{dS_t}{dt} &= -\beta I_a S_t + \xi_t R_t, \\
\frac{dI_t}{dt} &= \beta I_a S_t - \gamma_t I_t, \\
\frac{dR_t}{dt} &= \gamma_t I_t - \xi_t R_t,
\end{aligned} \tag{21}$$

System (21) admits the trivial infection-free equilibrium $P_0 = (S_t^0 = 1, I_t^0 = 0, R_t^0 = 0)$. Moreover, it has a unique endemic equilibrium with positive components:

$S_t^* = \frac{\gamma\xi_t}{\gamma\xi_t+(\gamma+\xi_t)(\beta-\xi-\mu)}$, $I_t^* = \frac{\xi_t}{\left(\frac{\xi_t\gamma}{\beta-\xi-\mu}\right)+(\xi_t+\gamma)}$, $R_t^* = 1-((I_l+I_h)_t^* + (S_l+S_h)_t^*$.
and the basic reproduction number $\mathcal{R}_0$ for the target population is as follows:

$$R_{0t} = \frac{\beta}{\gamma},$$

and for the attacking population, it is the following:

$$R_{0a} = \frac{\beta}{\xi+\mu},$$

therefore, $\mathcal{R}_0|_{\epsilon=0,\eta=0} = \max\{\frac{\beta}{\mu+\xi}, \frac{\beta}{\gamma}\} = \max\{R_{0a}, R_{0t}\}$, if $\gamma \geq \xi+\mu$, then $\mathcal{R}_0 = R_{0a}$. The following theorems were proven by Bimal et al. [22]. These results show the local and global stability of Equation (21).

Theorem 6. *The infection-free equilibrium P_0 of system (21) is locally asymptotically stable in D if $R_{0a} < 1$ and is unstable if $R_{0a} > 1$ [22].*

From theorem 6, one can see that the trajectories of Equation (21) are converging to point P_0, which means that the system is locally asymptotically stable at P_0. In this case, the attack will disappear in the long run.

Theorem 7. *The endemic equilibrium P^* is locally asymptotically stable in the interior of D if $R_{0a} > 1$ [22].*

Theorem 8. *The unique endemic equilibrium point P^* is globally asymptotically stable in the interior of D if $\mathcal{R}_0 > 1$ [22].*

Theorems 7 and 8 show the local and global stability, respectively. In this case, the trajectories converge at P^* so that the attack will remain effective in the long run. For more details, the model was completely analyzed in [22].

We conclude from this study that relying on backup servers alone, without protection from this type of attack, does not provide a solution. If the attack continues for a long time, all backup servers will go down. This is demonstrated by the assumption that the number of disabled devices due to the attack is $I'(t) > M$, for a non-zero M, at time t.

Hence, the number of needed backup servers in time T (period of attack) will be $N_{backup} = \int_0^T I'(t)dt$. For a long time ($T$ goes to infinity), the value of $N_{backup} > T \times M$ will go to infinity.

3.3. Perfect High-Security Level

In this subsection, we will analyze the proposed model in a perfect high-security level ($\epsilon = 1$) in which no attack can pass the firewall. In this case, the recovered nodes from the low-security level become suspected and will not be attacked again. If $\epsilon = 1$, then for the zero initial conditions ($I_h(0)$) at high population, we can set $\xi_h = 0$ and $\gamma_h = 0$. We will prove that in this case, there is no epidemic solution, and the attack will disappear. Here, there is a unique equilibrium point which is P_0. Therefore, the proposed system (6) is converted to the following:

$$\begin{aligned}
\frac{dS_h}{dt} &= \xi_l R_l,\\
\frac{dS_l}{dt} &= -\lambda S_l,\\
\frac{dI_l}{dt} &= \lambda S_l - \gamma_l I_l,\\
\frac{dR_l}{dt} &= \gamma_l I_l - \xi_l R_l,\\
\frac{dS_a}{dt} &= \mu - \beta S_a I_a - \mu S + \xi I_a,\\
\frac{dI_a}{dt} &= \beta S_a I_a - (\xi + \mu) I_a.
\end{aligned} \tag{22}$$

in which $I_h(0) = 0$. The basic reproduction number $\mathcal{R}_0$ is computed as follows:

$$\mathcal{R}_0|_{\epsilon=1} = \max\{R_{0a}, R_{0l}\} = \max\left\{\frac{\beta}{\mu+\xi}, \frac{\beta}{\gamma_l}\right\}.$$

If there is a non-zero initial condition ($I(0) \neq 0$), then $\gamma_h \neq 0$. Hence, $\frac{dI_h}{dt} = -\gamma_h I_h$, which implies $I_h(t) = I(0) \times \exp(-\gamma t)$, and $I(t) \longrightarrow 0$ as $t \longrightarrow \infty$. Moreover, for the recovered nodes of the high-security level R_h, $\frac{dR_h}{dt} = c \times \exp(-\gamma t) - \xi_h R_h$ with $c = \gamma_h I(0)$ is solved to find $R_h = R_h(0)\, \mathrm{e}^{-\xi_h t} + \frac{c}{\xi_h - \gamma}\, \mathrm{e}^{-\gamma t}$. Therefore, $R_h(t) \longrightarrow 0$ as $t \longrightarrow \infty$. The following theorem summarizes these results and computations:

Theorem 9. *If $\epsilon = 1$, then for all values of $\mathcal{R}_0$ with $P_0 = (S^0, I^0, S_l^0, I_l^0, R_l^0, S_h^0, I_h^0, R_h^0) = (1, 0, S_l^0, 0, 0, S_h^0, 0, 0)$ is globally asymptotically stable in the interior of D, in which $S_l^0 + S_h^0 = 1$.*

In Figure 2, different values for the threshold number are chosen to explain the stability of system (6). It can be noticed how λ, which is the percentage of infected nodes as a function of time t, converge to λ^* or λ_0 depending on the value of $\mathcal{R}_0$. In words, if $\mathcal{R}_0 > 1$, then the values of λ converge to λ^* with time t, and if $\mathcal{R}_0 < 1$ then the values of λ converge to λ_0 with time t. The values of the used parameters are as follows:

$$(\beta, \epsilon, \eta, \gamma_l, \gamma_h, \xi_l, \xi, \xi_h, \mu) = (0.315,\ 1,\ 1,\ 0.029,\ 0.052,\ 0.85,\ 0.103,\ 0.302,\ 0.013)$$

with $R_{0a} = 2.7099$, and we set

$$(\beta, \epsilon, \eta, \gamma_l, \gamma_h, \xi_l, \xi, \xi_h, \mu) = (0.15,\ 1,\ 1,\ 0.0292,\ 0.283,\ 0.38,\ 0.1031,\ 0.302,\ 0.081)$$

then $R_{0a} = 0.8134$.

In the next section, different examples and experiments are proposed to solve system (6) and to show the stability.

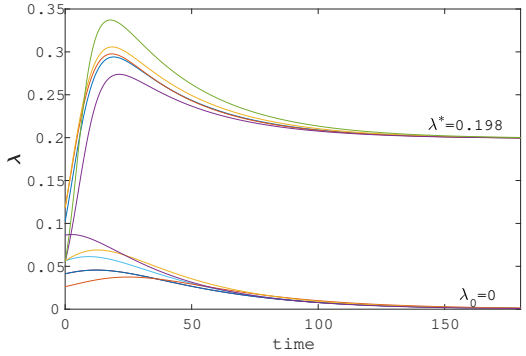

Figure 2. Simulations of the proposed model (6), showing the percentage of infected nodes as a function of time.

4. Numerical Analysis and Discussion

In this section, different examples and experiments are proposed to solve system (6). Furthermore, numerical techniques are used to approximate the solution. These examples illustrate the stability as well, and reversing symmetry transformation is shown.

Example 1. *Solve system (6), in which the values of the parameters are the following:* $(\beta, \epsilon, \eta, \gamma_l, \gamma_h, \xi_l, \xi, \xi_h, \mu) = (0.015, 0.61, 1, 0.029, 0.028, 0.05, 0.103, 0.302, 0.013)$ *with initial conditions* $(S(0), I(0), S_l(0), I_l(0), R_l(0), S_h(0), I_h(0), R_h(0)) = (0.875, 0.125, 0.375, 0.125, 0, 0.375, 0.125, 0)$, $R_{0a} = 0.129$, *and* $R_{0t} = 0.7204$.

Since $R_{0a}, R_{0t} < 0$ then $\mathcal{R}_0 < 1$. Therefore, it can be concluded that the system will be infection-free with time. Hence, the trajectories of the solution converge to $P_0 = (1, 0, 0.3, 0, 0, 0.7, 0, 0)$, as shown in Figure 3. Moreover, we notice that the attack node population is invariant with respect to the reversing symmetry transformation described in Lemma 1 for a small value of μ.

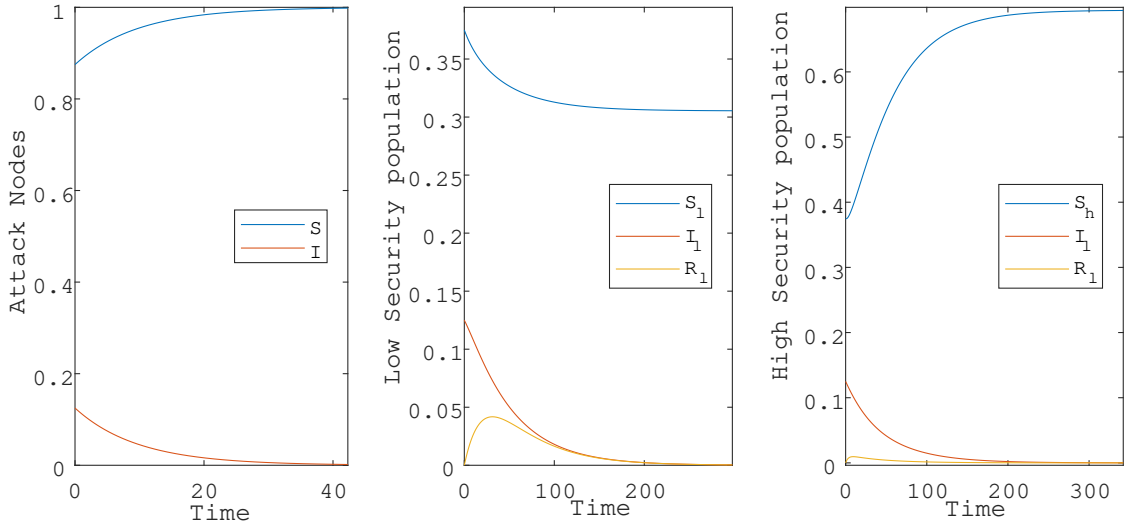

Figure 3. The solution of system (6) when the parameters are set, as in Example 1.

Example 2. *Solve system (6), in which the values of the parameters are chosen as:* $(\beta, \epsilon, \eta, \gamma_l, \gamma_h, \xi_l, \xi, \xi_h, \mu) = (0.34, 0.61, 1, 0.0102, 0.0102, 0.051, 0.068, 0.302, 0.0201)$ *with initial conditions* $(S(0), I(0), S_l(0), I_l(0), R_l(0), S_h(0), I_h(0), R_h(0)) = (0.875, 0.125, 0.375, 0.125, 0, 0.375, 0.125, 0)$, $R_{0a} = 3.9$, *and* $R_{0t} = 46.7117$.

It can be concluded that the system is epidemic since $\mathcal{R}_0 > 1$. Since $R_{0a}, R_{0t} > 1$, then $\mathcal{R}_0 > 1$. Therefore, the system will be infected, and the trajectories of the solution converge to P_*, as illustrated in Figure 4.

Example 3. *In this example, the solution of system (6) solved with perfect high and low-security levels.* $(\beta, \eta, \gamma_l, \gamma_h, \xi_l, \xi, \xi_h, \mu) = (0.15, 1, 0.0292, 0.0283, 0.051, 0.1031, 0.302, 0.01314)$ *with initial conditions* $(S(0), I(0), S_l(0), I_l(0), R_l(0), S_h(0), I_h(0), R_h(0)) = (0.875, 0.125, 0.375, 0.125, 0, 0.375, 0.125, 0)$.

Example 3 shows the efficiency of ϵ when we have a perfect high-security level. In Figure 5, class 1 ((1a), (1b), and (1c)) represent the solution when $\epsilon = 0$, and class 2 ((2a), (2b), and (2c)) represent the solution when $\epsilon = 1$. By comparing these two classes, it can be concluded that figures (1a) and (1b) and figures (2a) and (2b) are the same, but the difference between the two experiments is at the last stage when $\epsilon = 1$ (high-security), in

which the system is converted from epidemic to almost infection-free. Additionally, the attack node is invariant with respect to the reversing symmetry map for small death rate.

Example 4. *Solve system* (6) *for different values of* η ($\eta = 0, \eta = 0.5$)*, with parameters* $(\beta, \epsilon, \gamma_l, \gamma_h, \xi_l, \xi, \xi_h, \mu) = (0.831, 00.61, 0.0102, 0.0102, 0.3, 0.6851, 0.3, 0.5201)$ *with initial conditions* $(S(0), I(0), S_l(0), I_l(0), R_l(0), S_h(0), I_h(0), R_h(0)) = (0.875, 0.125, 0.375, 0.125, 0, 0.375, 0.125, 0)$.

In Figure 6, the first class ((1a), (1b), and (1c)) represents the solution of system (6) when $\eta = 0.5$, i.e., when the attacker exploited the infected target devices to attack other nodes. This effect is represented by η. Figures (2a), (2b), and (2c) in the second class represent the system when $\eta = 0$, i.e., when the attacker could not use the target infected devices to increase the effect of the attack. Therefore, it can be noticed that in the first class, the attack remains in the system since $R_{0t} > 1$ despite $R_{0a} < 1$. However, in the second class, the attack disappears because of $\eta = 0$. The result of Lemma 1 can also be noticed in the attack node population (1a) and (2a).

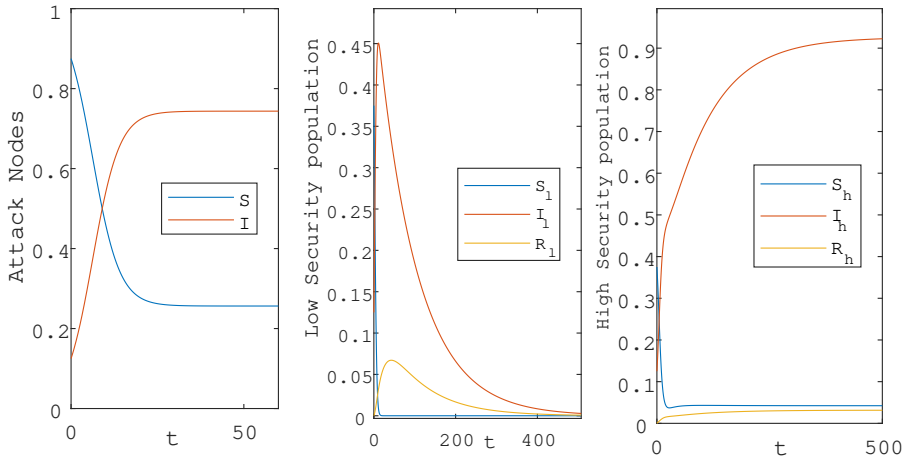

Figure 4. The infected solution of system (6), when the parameters are set as in Example 2.

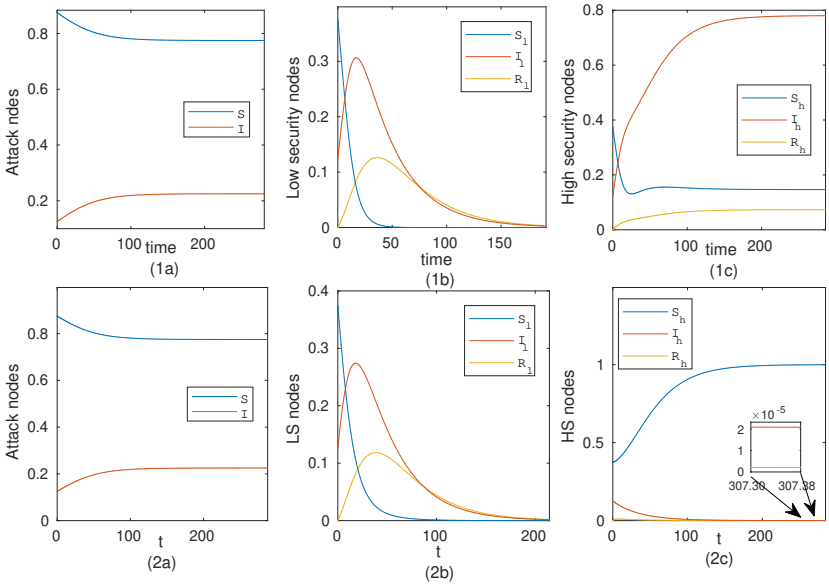

Figure 5. Class 1: the solutions of system (6), when $\epsilon = 0$. Class 2: the solutions of system (6), when $\epsilon = 1$, in which the values of the parameters are set as in Example 3. Sub-figures (**1a**,**2a**) simulate an attack population, and sub-figures (**1b**,**2b**), (**1c**,**2c**) simulate the target population with both low-security level and high-security level, respectively.

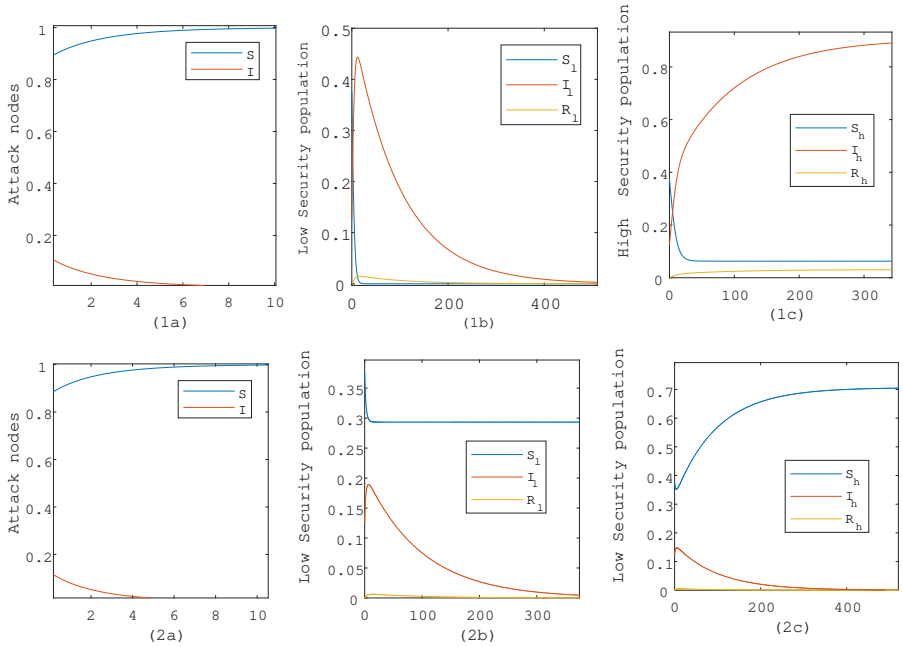

Figure 6. Class 1: the solutions of system (6), when $\eta = 0.5$. Class 2: the solutions of system (6), when $\eta = 0$, in which the values of the parameters are set as in Example 4. Sub-figures (**1a**,**2a**) simulate an attack population, and sub-figures (**1b**,**2b**), (**1c**,**2c**) simulate the target population with both low-security level and high-security level, respectively.

5. Conclusions

In this paper, we proposed a mathematical model to describe DDoS attacks. One of the most significant features of this model is considering a high-security level for the target population in which the recovered nodes upgrade their defense level to a higher level. In previous models, the recovered nodes did not have any upgrade on their defense level, which is an unrealistic assumption. Therefore, we set ϵ to represent the firewall efficiency after recovering. Furthermore, the modification parameter η was set to account for the attack transmission of the infected target nodes (in the I_l and I_h compartments). Moreover, we analyzed the proposed model for certain cases. The threshold value ($\mathcal{R}_0$) was found, and the stability was discussed. The reversing symmetry transformation $\mathcal{T}$ of the attack population was described. Finally, different examples were presented to illustrate the validity of the proposed model (6).

Author Contributions: Conceptualization, A.A. and Y.A.; methodology, A.A. and Y.A.; validation, F.A.; formal analysis, Y.A.; investigation, A.A.; resources, F.A.; data curation, A.A.; writing—original draft preparation, A.A. and Y.A.; writing—review and editing, F.A.; visualization, Y.A. and F.A.; supervision, A.A.; project administration, A.A.; funding acquisition, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author, upon reasonable request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Gligor, V.D. A Note on the Denial-of-Service Problem. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 25–27 April 1983; pp. 139–149.
2. Moore, D. The Spread of the Code-Red Worm (CRv2). 2001. Available online: http://www.caida.org/publications/papers/2002/codered/codered.pdf (accessed on 5 November 2021).
3. Calem, R.E. New York's Panix Service Is Crippled by Hacker Attack. 1996. Available online: https://archive.nytimes.com/www.nytimes.com/library/cyber/week/0914panix.html (accessed on 5 November 2021).
4. Alexander, K.; Oleg Kupreev, E.B. DDoS Attacks in Q1 2018. 2018. Available online: https://securelist.com/ddos-report-in-q1-2018/85373/ (accessed on 5 November 2021).
5. Peng, T.; Leckie, C.; Ramamohanarao, K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Comput. Surv. (CSUR)* **2007**, *39*, 3. [CrossRef]
6. Calce, M.; Silverman, C. *Mafiaboy: How I Cracked the Internet and Why It's Still Broken*; Penguin Group Canada: Toronto, ON, Canada, 2008.
7. Garber, L. Denial-of-service attacks rip the Internet. *IEEE Comput. Soc.* **2000**, *33*, 12–17. [CrossRef]
8. Loukas, G.; Öke, G. Protection against denial of service attacks: A survey. *Comput. J.* **2009**, *53*, 1020–1037. [CrossRef]
9. Hilton, S. Dyn Analysis Summary of Friday October 21 Attack. 2016. Available online: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ (accessed on 5 November 2021).
10. Weagle, S. Financial Impact of Mirai DDoS Attack on Dyn Revealed in New Data. 2017. Available online: https://www.corero.com/blog/financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data/ (accessed on 5 November 2021).
11. Awrejcewicz, J.; Losyeva, N.; Puzyrov, V. Stability and Boundedness of the Solutions of Multi-Parameter Dynamical Systems with Circulatory Forces. *Symmetry* **2020**, *12*, 1210. [CrossRef]
12. De la Sen, M.; Ibeas, A.; Agarwal, R.P. On Confinement and Quarantine Concerns on an SEIAR Epidemic Model with Simulated Parameterizations for the COVID-19 Pandemic. *Symmetry* **2020**, *12*, 1646. [CrossRef]
13. Lamb, J.S.; Roberts, J.A. Time-reversal symmetry in dynamical systems: A survey. *Phys. D Nonlinear Phenom.* **1998**, *112*, 1–39. [CrossRef]
14. Lamb, J.S.; Brands, H. Symmetries and reversing symmetries in kicked systems. In *Dynamics, Bifurcation and Symmetry*; Springer: Dordrecht, The Netherlands, 1994; pp. 181–196.
15. Liu, M.; Dassios, I.; Milano, F. On the stability analysis of systems of neutral delay differential equations. *Circuits Syst. Signal Process.* **2019**, *38*, 1639–1653. [CrossRef]
16. Kirillov, O.N. Classical results and modern approaches to nonconservative stability. In *Dynamic Stability and Bifurcation in Nonconservative Mechanics*; Springer: Cham, Switzerland, 2019; pp. 129–190.
17. Ten, C.W.; Manimaran, G.; Liu, C.C. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. In *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*; IEEE Press: Piscataway, NJ, USA, 2010; pp. 853–865.
18. Cybersecurity and Infrastructure Security Agency. Understanding Denial-of-Service Attacks. 2019. Available online: https://www.us-cert.gov/ncas/tips/ST04-015 (accessed on 16 June 2021).
19. Zargar, S.T.; Joshi, J.; Tipper, D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 2046–2069. [CrossRef]
20. Farraposo, S.; Gallon, L.; Owezarski, P. Network Security and DoS Attacks. Technical Report. LAAS-CNRS. 2005. Available online: https://www.miralishahidi.ir/resources/Security_and_DoS.pdf (accessed on 5 November 2021).
21. Gan, C.; Yang, X.; Zhu, Q.; Jin, J.; He, L. The spread of computer virus under the effect of external computers. *Nonlinear Dyn.* **2013**, *73*, 1615–1620. [CrossRef]
22. Haldar, K.; Mishra, B.K. A mathematical model for a distributed attack on targeted resources in a computer network. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 3149–3160. [CrossRef]
23. Mishra, B.K.; Haldar, K. e-Epidemic Models on the Attack and Defense of Malicious Objects in Networks. In *Theories and Simulations of Complex Social Systems*; Springer: Berlin/Heidelberg, Germany, 2014; Volume 52. [CrossRef]
24. Kermack, W.; McKendrick, A. Contributions to the mathematical theory of epidemics—I. *Bull. Math. Biol.* **1991**, *53*, 33–55. [CrossRef] [PubMed]
25. Rao, Y.S.; Keshri, A.K.; Mishra, B.K.; Panda, T.C. Distributed denial of service attack on targeted resources in a computer network for critical infrastructure: A differential e-epidemic model. *Phys. A Stat. Mech. Its Appl.* **2020**, *540*, 123240. [CrossRef]
26. Mishra, B.K.; Keshri, A.K.; Mallick, D.K.; Mishra, B.K. Mathematical model on distributed denial of service attack through Internet of things in a network. *Nonlinear Eng.* **2019**, *8*, 486–495. [CrossRef]
27. Zhang, C. Impact of Defending Strategy Decision on DDoS Attack. *Complexity* **2021**, *2021*, 6694383. [CrossRef]
28. Van den Driessche, P.; Watmough, J. Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission. *Math. Biosci.* **2002**, *180*, 29–48. [CrossRef]
29. Anderson, R. Transmission dynamics and control of infectious disease agents. *Popul. Biol. Infect. Dis.* **1982**, 149–176.
30. La Salle, J.; Lefschetz, S. Stability by Liapunov's Direct Method with Applications by Joseph L Salle and Solomon Lefschetz. *Phys. Today* **1962**, *15*, 59. [CrossRef]