IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 10, 2021, accepted August 18, 2021, date of publication August 26, 2021, date of current version September 3, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3108181

Dynamics of Botnet Propagation in Software Defined Networks Using Epidemic Models

JUAN FERNANDO BALAREZO, (Member, IEEE), SONG WANG, KARINA GOMEZ CHAVEZ, AKRAM AL-HOURANI, (Senior Member, IEEE), AND SITHAMPARANATHAN KANDEEPAN, (Senior Member, IEEE)

School of Engineering, RMIT University, Melbourne, VIC 3000, Australia

Corresponding author: Juan Fernando Balarezo (s3738234@student.rmit.edu.au)

The work of Juan Fernando Balarezo and Song Wang was supported by the Australian Government Research Training Program Scholarship.

ABSTRACT During COVID-19 the new normal became an increased reliance on remote connectivity, and that fact is far away to change any time soon. The increasing number of networked devices connected to the Internet is causing an exponential growth of botnets. Subsequently, the number of DDoS (Distributed Denial of Service) attacks registered around the world also increased, especially during the pandemic lockdown. Therefore, it is crucial to understand how botnets are formed and how bots propagate within networks. In particular, analytic modelling of the botnets epidemic process is an essential component for understanding DDoS attacks, and thus mitigate their impact. In this paper, we propose two analytic epidemic models; (i) the first one for enterprise Software Define Networks (SDN) based on the SEIRS (Susceptible - Exposed - Infected - Recovered) approach, while (ii) the second model is designed for service providers' SDN, and it is based on a novel extension of a SEIRS-SEIRS vector-borne approach. Both models illustrate how bots spread in different types of SDN networks. We found that bot infection behaves in a similar way to human epidemics, such as the novel COVID-19 outbreak. We present the calculation of the basic reproduction number R_o for both models and we test the system stability using the next generation matrix approach. We have validated the models using the final value theorem (FVT), with which we can determine the steady-state values that provide a better understanding of the propagation process.

INDEX TERMS Networks security, cyber-attack modelling, Distributed Denial of Service (DDoS), software defined networks (SDN).

I. INTRODUCTION

The COVID-19 pandemic triggered a significant change to virtualised environment for everyone, providing attackers a much larger field of opportunities. It was estimated that 20.4 billion devices were connected during 2020 [1], while at the same time the increase of botnets is exponential (Mirai: from 35k devices in 2017 up to 230k devices in 2019) and 4.83 million of DDoS (Distributed Denial of Service) attacks were registered in the first half of 2020 [2]. Showing us the importance of having reliable and secure online services. DDoS attacks represent the main threat to the availability of online applications, services and networks [3]. Then, indistinctly of the targets, adversaries or tactics being used, it is crucial that security professionals keep alert to safeguard the infrastructure and communication channels that connect the digital world. During the first half of 2020 adversaries increased their attacks against critical online platforms and services such as e-commerce, educational platforms, financial services, and healthcare services [2]. A radical change was evidenced in DDoS attack methodology, which changed into to shorter, faster, harder-hitting complex multi-vector attacks. Meaning that botnet size and their infection dynamics became key features in order to increase the chances of inducing a successful attack. Botnets have overwhelmed several critical infrastructure targets with massive DDoS attacks [1]–[4]. Remarkably, such traffic was generated from hundreds of thousands of infected hosts. This has been possible due to different factors, such as efficient spreading and keeping the botnets behavior simple, allowing it to infect many heterogeneous devices [4]. Many botnet variants have been developed following similar infection schemes, so that

The associate editor coordinating the review of this manuscript and approving it for publication was Tariq Umer.

they became the most used and effective way to generate DDoS attacks.

Mathematical models have become relevant in the study of infectious diseases [5]. Modelling epidemics allows to identify crucial parameters, which determine the infection dynamics. Epidemic mathematical models have proven to be practical experimental tools for analysing theories and assessing relevant parameters from data. Most of the proposed models for human epidemics in literature follow the compartment modelling approach, such as the single infection-vector diseases [6]–[9] and the multi-vector (zoonoses) diseases [10]–[14]. It is possible to develop epidemic models for SDN following the compartmental approach, since the affected population undergoes through an equivalent process as humans do with only slight differences, which are considered in our proposed models. Epidemic models have been extensively used as a mathematical tool that allows to understand malware spread across communication networks. Early examples that used such approach can be found in [15], [16], that were subsequently taken as a reference by different authors [17]–[24]. Modelling allows to identify key features of the infection process and provide insights on the proliferation dynamics, which helps to develop detection and mitigation countermeasures against malware distribution within networks.

The SDN architecture is divided into application plane, control plane, data plane and the communication channels between them (northbound and southbound channel). Central management, dynamic configuration and flexibility are some of the benefits brought by SDN [25]. However, with all these benefits, security challenges arise. The SDN centralised architecture is prone to DDoS attacks, especially the ones targeting the controller, switches or the communication channel between them. DDoS traffic generated by the forwarding devices or even the controllers, would make the attack more difficult to be detected and mitigated. And the number of compromised devices is crucial when launching a DDoS attack [26]. Hence, modelling the infection processes in SDN is essential since attackers would seek to infect as many devices as possible.

We aim to model the botnet infection process in SDN, with the same fashion as compartmental models follow in human epidemics. Such modeling method is required to understand how botnets can be propagated within SDN networks. Allowing to have a better insight about the bot recruitment cycle is essential within DDoS attacks. As mentioned before, there are some differences between human epidemics and malware infections, one of the most relevant is that in human epidemics the immune system prevents us from getting infected again [27]. Meanwhile, within the bot infection process, once a node recovers from the infection it can become susceptible to be infected again. The reason relies on that new vulnerabilities can be found to infect the devices again with the same malware. Or the attacker could perform small changes to the malware code so it won't be detected by anti-malware tools (polymorphic and metamorphic malware [28]). We propose two epidemic models to represent botnet propagation within SDN devices for two different scenarios. The first one for SDN enterprise networks which is a SEIRS model. The second one is designed for SDN service provider networks, and it is a SEIRS-SEIRS model. Both models illustrate how bots spread in different types of SDN networks. In our specific cases, the enterprise model is similar to the COVID-19 models proposed so far [6]. While the service provider (SP) model is comparable to zoonoses models, such as the Zika virus [10], where infection between different species is possible. For the SP model we propose that it is possible to have infection vectors from the controller to the switches and also among the last ones. Also, we proved how fast and critical the botnet infections are able to spread within the SDN network when the reproduction number R_o reaches values greater than 1. Finally, we validated the models by finding the steady-state values of the systems using the final value theorem (FVT). The steady-state values are relevant to our models since they allow to have a deeper understanding of the epidemic process. Such understanding in SDN is fundamental in the development of prevention and mitigation techniques. The proposed models allow to understand how maintaining and ensuring a low infection rate and a high recovery rate would stop the spread of botnet malware within SDN networks. Such achievement could be obtained by following well defined security methodologies and processes.

The rest of the article is organised as follows. Section II introduces the related work done so far regarding epidemic in communication networks. Section III presents the background of epidemic models in order to understand how they can be used in SDN epidemic processes. In Section IV we propose two epidemic models for SDN, the first one for enterprise networks and the second one for service provider networks. Section V presents the simulations that were carried out to evaluate the models. Finally, in Section VI we conclude this article.

II. RELATED WORK

Large-scale DDoS attacks involve threats from multiple categories, usually requiring multi-pronged defense mechanisms combining several defense approaches [29]. The efficiency of DDoS attacks depends on different aspects, one of the most important is the size of the botnet used to launch an attack [26]. Botnets creation process relies upon malware dissemination dynamics, accordingly, understanding such behaviour becomes relevant. Human epidemics and computational viruses share similar characteristics [15], so that the mathematical epidemiology theory [30] can be applied to analyse malware propagation within communication networks. Kephart and White were pioneers in adapting human epidemic models into malware modelling techniques [15], [16]. They proposed a SIS model in which PCs can be either susceptible or infected, but this assumption leaves out states that have to be included as part of the model. A device is not necessarily capable of spreading the malware at the time it gets infected. As in human epidemics, it may need an

incubation period in order to start spreading the malware over the rest of the network [17]. There is also the possibility of clearing the malware from the infected devices, which means that they can be recovered and will no longer be able to spread the infection. Finally, unlike human epidemics, a device that recovers from the infection not necessary gains immunity and it could be infected again. So devices can become susceptible again going over the infection process one more time.

Dadlani *et al.* [31] proposed a redefined SIS model, considering [15] approach, in which they incorporate different infection stages and propagation vectors for scale-free networks. Even though their approach did not consider the exposed and recovered states, the inclusion of infection delay and propagation vectors opened the door to their inclusion in future models. Chen *et al.* [32] defined a SIR model to characterise the dynamics of information dissemination within networks in order to identify an optimal control policy. In their model they proposed intermediate states between the susceptible and infected nodes and also between recovered and susceptible devices. For example a node could be susceptible yet potentially infected. However, this intermediate state should be given a more specific treatment. When a node is already infected but not yet infectious, it should be considered as an exposed node. Taynitskiy *et al.* [18] proposed a time continuous SIR model in which they included two different types of malware for homogeneous populations. However, it is possible to consider a heterogeneous environment in which cross-platform malicious code is designed to infiltrate and infect nodes running different operating systems [17]. These models do not take into account all the considerations that we propose. They only consider SIS approaches, leaving out states that have to be included to have a better comprehension of the propagation process.

Hosseini *et al.* [33] formulated a global approach of the SEIRS model to study the malware propagation dynamics in scale-free-networks (SFNs). SFNs could be social, economical or technological complex systems, in which a few nodes are linked to many other nodes of the population. Even though SFNs share some similarities, a narrowed approach for specific scenarios and types of networks is required. This will allow to identify inherent features and behaviours of each system, thus allowing to propose specific and optimised mitigation solutions. Proof of the need to design specific models according to the environment where they are developed is shown by Androulidakis *et al.* [34]. Where they proposed a SEIR epidemic model for Private Branch eXchanges (PBX) networks, proving that only 2 days were enough to spread the malware. However, the model does not consider the chance of the nodes being infected again after the malware is removed which is possible as we already stated. Models developed for specific scenarios and environments can be also found for mobile wireless sensors networks (WSN) [19], [20], [35], [36]; mobile devices [21], [37]; social networks [22], [38]; IoT networks [23]; industrial control system (ICS) networks [24].

Models regarding the epidemics infectious process in SDN networks have not been completely analysed and understood so far. Wang *et al.* [39] studied a heterogeneous SIS model to evaluate the security performance in SDN. Where they proposed a coloring algorithm to limit the ability of a malicious controller to compromise its neighboring controllers. Lui *et al.* [40] presented a SIS dynamic model with a time-varying community network to analyse the spreading processes of malware in SDN. However, these models did not consider the fact that the controllers can also infect the forwarding devices as we do in our models. As well as the previous models, necessary infection states were left behind, which are considered in our SEIRS models. Additionally, the estimation of the basic reproduction number and the stability analysis was not evaluated, which is done for the models we are presenting. Finally, we presented the theoretical model validation using the final value theorem (FVT), task that has not been done in any of the existing models so far.

It is important to mention that ordinary differential equations (ODEs) have been used to analyse epidemics dissemination dynamics within the different variants of the aforementioned research topics [32].

III. EPIDEMIC MODELLING BACKGROUND

In order to understand why and how epidemic models could be applied to analyse malware spread within communication networks, we have to analyse how epidemics are modelled for humans diseases. Mathematical models have become important tools in analysing the spread and control of infectious diseases [5]. Modelling diseases helps to recognise assumptions, variables, and parameters; such as thresholds, basic reproduction numbers, contact numbers, and replacement numbers, which determine the infection dynamics. Mathematical models in epidemics have proven to be useful experimental tools for analysing theories, estimating quantitative hypothesis, and assessing relevant parameters from data. In order to achieve optimised approaches to decrease the proliferation of diseases in communities it is required to understand their transmission behaviour. Epidemiology models are implemented to develop, evaluate, and improve the existing detection, prevention and control programs. Therefore, modelling contributes to the design and analysis of epidemiological data recollection, trends identification, and forecasting [5]. Said information, analysis and evaluation can be also applied to understand and prevent malware proliferation within communication networks such as SDN. Most human epidemics in the literature follow the compartment modelling approach [5], [6], [10]–[14], [41]–[45], in which the affected population moves within a finite number of discrete states as shown in Figure 1.

States or compartments are labeled according to the epidemiological class they belong to, which commonly include but not limited to: Susceptible (S), Exposed (E), Infected (I) and Recovered (R) [5]. Susceptible individuals are those who do not have immunity against the disease being analysed, which means they could be infected. For an individual to

FIGURE 1. Compartment model in human epidemics (S - Susceptible, E - Exposed, I - Infected, R - Recovered.)

become infected it needs to have contact with infected individuals so that the transmission can occur. Once it happens, the susceptible individual becomes exposed, which means that they are already infected but not yet infectious. After the incubation period ends, individuals move into the infected compartment, where they are infectious and able to spread the disease. Depending on the disease, individuals can either die or recover from it. Upon recovery, individuals move to the recovered state, in which they could have infection-acquired immunity [5] or become susceptible again depending on the disease. The first step to build a model is to choose which compartments need to be included based on the specific characteristics of the epidemic. From this selection the model is given an acronym to identify it. For example, within an scenario where susceptible individuals become exposed, then infected and finally recovered with permanent immunity, the identifier acronym for such model is SEIR. If individuals have temporary immunity so that they can regain their susceptibility, the model identifier is SEIRS. The dynamics of compartmental models are described by a system of nonlinear ordinary differential equations (ODEs) [42], which represent the evolution of the number of individuals within each state in time. To identify if the disease can spread among the susceptible individuals it is required to estimate the number of secondary cases produced by an infected individual during its infectiousness period of time [41]. This value is known as the basic reproduction number R_o. The calculation of R_o is obtained from the ODEs equations that indicate the appearance of new infected individuals and their state changes. This subsystem needs to be linearised so it can be described by a matrix which correlates the numbers of new infected individuals within the different categories in consecutive generations. This matrix is named as the next generation matrix (NGM) [41], [42]. The NGM matrix is used to calculate R_o when the system is at disease free equilibrium (DFE). In which,

$$R_o = \rho(\boldsymbol{FV}^{-1}), \tag{1}$$

where $\boldsymbol{F}$ is the transmission matrix which describes the production of new infections; $\boldsymbol{V}^{-1}$ is the transition matrix which describes the transfers of infections from one state to another; and ρ denotes the spectral radius of the resultant matrix $\boldsymbol{FV}^{-1}$. So we can say that R_o is the dominant eigenvalue of the $\boldsymbol{FV}^{-1}$ resultant matrix.

IV. SDN EPIDEMIC MODEL

In section II we explained how epidemics are modelled for humans diseases, where most of the proposed models in literature follow the compartment modelling approach [6], [10]–[14], [45]. In which the affected populations move between different states as shown in Figure 1. The botnet infection process in SDN can be modelled in a similar way as in human diseases since the affected population undergoes through an equivalent process with only slight differences, which are considered in our proposed models. Within human epidemics, the immune system prevents us from getting infected again [27]. However, within the bot infection process, after a node recovers from the infected state it can become susceptible to be infected again. This is possible because new vulnerabilities can be found to infect the devices again. Or the attacker could change the malware code so it won't be detected by anti-malware tools (polymorphic and metamorphic malware [28]).

The SDN centralised architecture is prone to DDoS attacks, specially the ones that target the controller, switches or the communication channel between them. If the DDoS traffic is generated by the forwarding devices or even the controllers, it would make the attack stealthier, increasing the probabilities of success. Also as proven in [26], the number of compromised devices is crucial when launching a DDoS attack. Attackers would seek to infect as many SDN devices as possible, then modelling the infection processes is essential. We propose two epidemic models to represent botnet propagation within SDN devices for two different scenarios. The first one for SDN enterprise networks is a SEIRS model. The second one is designed for SDN service provider networks, and it is a SEIRS-SEIRS model. Both models illustrate how bots spread in different types of SDN networks. The existing models in literature do not take into account all the considerations that we study, they only contemplate SIS approaches. Leaving out the exposed and recovered states that are required in order to have a more precise analysis of the infection process. Therefore, we compare our models with the approaches used for Zika and COVID-19 diseases because they share equivalent infection vectors. In specific, the enterprise model is similar to the COVID-19 models proposed so far [6]. While the service provider (SP) model is comparable to zoonoses models, such as the Zika virus [10], where infection among different species is possible. For the SP model we propose that is possible to have infection vectors from the controller to the switches and also amid the last ones.

A. ENTERPRISE EPIDEMIC MODEL

Enterprise SDN networks architecture is smaller and simpler than service provider SDN networks. Thus, the enterprise SDN can be managed by one centralised controller, and in some specific cases there could be a standby controller for high availability of the network. Meaning that there is only one infection vector among the forwarding devices. Under this scenario, we propose a compartmental epidemic model in

which the forwarding devices could be affected by malware and afterwards the infection will spread amid the switches population as represented in Figure 2.

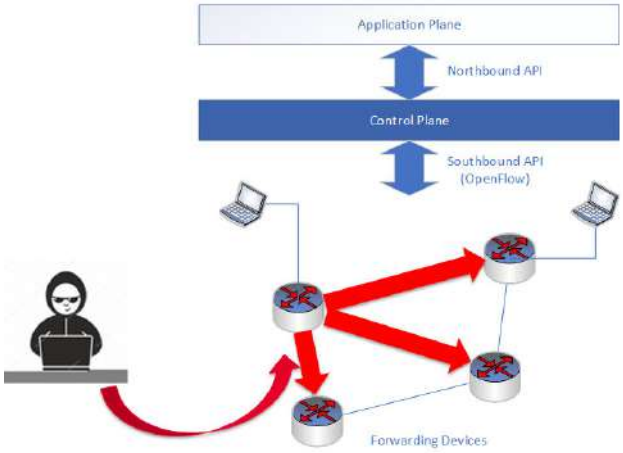


FIGURE 2. Enterprise infection scenario.

Our enterprise system is represented with a state diagram in Figure 3 according to the compartmental modelling approach.

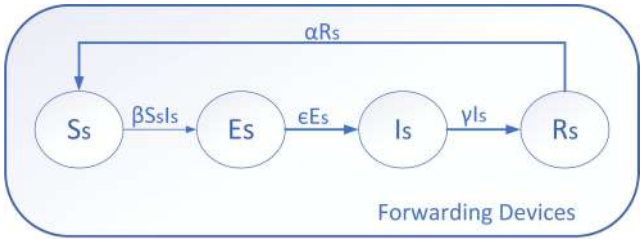


FIGURE 3. Enterprise model state diagram.

The enterprise epidemic model is represented by the following system of ordinary differential equations (ODEs):

$$\begin{aligned}\frac{dS_S}{dt} &= -\beta S_S I_S + \alpha R_S \\ \frac{dE_S}{dt} &= \beta S_S I_S - \epsilon E_S \\ \frac{dI_S}{dt} &= \epsilon E_S - \gamma I_S \\ \frac{dR_S}{dt} &= \gamma I_S - \alpha R_S \end{aligned} \tag{2}$$

where, S_S are the susceptible class nodes of total population, E_S are the exposed class nodes of total population, I_S are the infectious class nodes, R_S are the recovered class nodes. Furthermore, we define the compartments as asset of ω_E as follows:

$$\omega_E = \{S_S, E_S, I_S, R_S\} \tag{3}$$

β is the transition rate of the nodes from susceptible class to exposed class. ϵ is the transition rate of nodes from exposed class to infectious class, γ is the recovery rate, α is the transition rate of nodes from recovered class to susceptible class due loss of immunity. The total population is given by:

$$S_S + E_S + I_S + R_S = 1 \tag{4}$$

The next step is to determine the basic reproduction number R_o to analyse the dynamics of the system. R_o is the average number of new cases within an infection process caused by one infected individual, considering a population of susceptible devices only [42]. A R_o with a value lower than 1 indicates that one infected device produces less than one new infected device during its infectious period, then the infection won't proliferate. Contrariwise, when R_o is greater than 1, each infectious device is capable to infect, on average, to more than one susceptible device and spread the infection all over the population. We used the next generation matrix (NGM) approach [41], [42] in order to calculate R_o when the system is at disease free equilibrium (DFE) by using equation (1). Where $\boldsymbol{F}$ is the transmission matrix which describes the production of new infections; $\boldsymbol{V^{-1}}$ is the transition matrix which describes the transfers of infections from one state to another; and ρ denotes the spectral radius of the resultant matrix $\boldsymbol{FV^{-1}}$. For our model the resultant matrices $\boldsymbol{F}$ and $\boldsymbol{V^{-1}}$ are:

$$\boldsymbol{F} = \begin{pmatrix} 0 & \beta S_S \\ 0 & 0 \end{pmatrix} \tag{5}$$

and,

$$\boldsymbol{V^{-1}} = \begin{pmatrix} 1/\epsilon & 0 \\ 1/\gamma & 1/\gamma \end{pmatrix} \tag{6}$$

then:

$$\boldsymbol{FV^{-1}} = \begin{pmatrix} \beta S_S/\gamma & \beta S_S/\gamma \\ 0 & 0 \end{pmatrix} \tag{7}$$

After building the next generation matrix for compartmental epidemic models the reproduction number R_o is the dominant eigenvalue of the matrix $\boldsymbol{FV^{-1}}$ [42], so that:

$$R_o = \frac{\beta S_S}{\gamma} \tag{8}$$

TABLE 1. Enterprise epidemic model notations.

Parameter	Notation
Susceptible class nodes	S_S
Exposed class nodes	E_S
Infected class nodes	I_S
Recovered class nodes	R_S
S_S to E_S transition rate	β
E_S to I_S transition rate	ϵ
I_S to R_S transition rate	γ
R_S to S_S transition rate	α
Enterprise system	ω_E
Basic reproduction number	R_o
Transmission matrix	$\boldsymbol{F}$
Transition matrix	$\boldsymbol{V^{-1}}$

B. SERVICE PROVIDER EPIDEMIC MODEL

Service provider (SP) SDN networks architecture is more complex and by far it includes more devices than the enterprise SDN networks. Meaning that more devices could be

infected and become part of a more threatening botnet. In order to have an scalable and manageable network within SP SDN, more than one controller is required. This means that there are two infection vectors. The first one between all the controllers of the system. The second one considers the spread vector from the controllers to the forwarding devices. And once the later become infectious they are able to proliferate the infection between the rest of the forwarding devices. Under these considerations, we propose a compartmental epidemic model in which the controllers could be affected by malware and afterwards the infection will spread between them and also the forwarding devices population as represented in Figure 4.

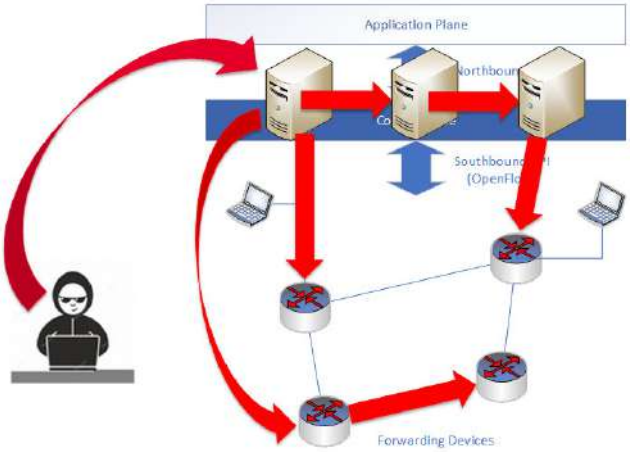


FIGURE 4. Service provider infection scenario.

The proposed SP system is represented with an state diagram in Figure 5 according to the compartmental modelling approach, in which it is possible to appreciate that the controllers network infected compartment affects also the forwarding devices susceptible compartment. This behaviour is reflected in the mathematical representation of the system.

The SP epidemic model is represented by a system of ordinary differential equations (ODEs) as follows:

$$\begin{aligned}
\frac{dS_S}{dt} &= -\beta_S S_S(I_C + I_S) + \alpha_S R_S \\
\frac{dE_S}{dt} &= \beta_S S_S(I_C + I_S) - \epsilon_S E_S \\
\frac{dI_S}{dt} &= \epsilon_S E_S - \gamma_S I_S \\
\frac{dR_S}{dt} &= \gamma_S I_S - \alpha_S R_S \\
\frac{dS_C}{dt} &= -\beta_C S_C I_C + \alpha_C R_C \\
\frac{dE_C}{dt} &= \beta_C S_C I_C - \epsilon_C E_C \\
\frac{dI_C}{dt} &= \epsilon_C E_C - \gamma_C I_C \\
\frac{dR_C}{dt} &= \gamma_C I_C - \alpha_C R_C
\end{aligned} \tag{9}$$

where, S_S are the susceptible class nodes of the switches population, E_S are the exposed class nodes of the switches

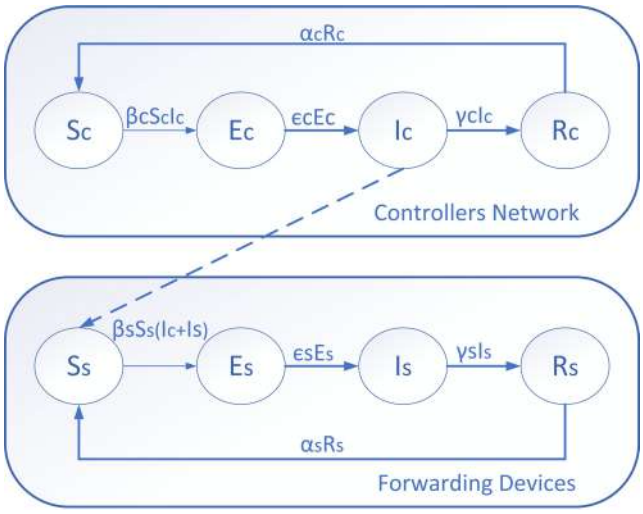


FIGURE 5. Service provider model state diagram.

population, I_S are the infectious class nodes of the switches population, R_S are the recovered class nodes of the switches population. S_C are the susceptible class nodes of the controllers' population, E_C are the exposed class nodes of the controllers' population, I_C are the infectious class nodes of the controllers' population, R_C are the recovered class nodes of the controllers' population. Furthermore, we define the compartments as asset of ω_{SP} as follows:

$$\omega_{SP} = \{S_S, E_S, I_S, R_S, S_C, E_C, I_C, R_C\} \tag{10}$$

β_S and β_C are transition rates of the nodes from susceptible class to exposed class. ϵ_S and ϵ_C are the transition rates of nodes from exposed class to infectious class, γ_S and γ_C are the recovery rates, α_S and α_C are the transition rates of nodes from recovered class to susceptible class due loss of immunity. The total population of the two infection vectors is given by:

$$\begin{aligned}
S_S + E_S + I_S + R_S &= 1 \\
S_C + E_C + I_C + R_C &= 1
\end{aligned} \tag{11}$$

where both population sizes are independent from each other, however the number of infected forwarding devices is impacted by the amount of infected controllers.

The next step is to determine the basic reproduction number R_o to analyse the dynamics of the system. As we did with the enterprise model, we used the next generation matrix (NGM) approach [41], [42] in order to calculate R_o when the system is at disease free equilibrium (DFE). The SP model resultant matrices $\boldsymbol{F}$ and $\boldsymbol{V}^{-1}$ are:

$$\boldsymbol{F} = \begin{pmatrix} 0 & \beta_S S_S & 0 & \beta_S S_S \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \beta_C S_C \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{12}$$

TABLE 2. SP epidemic model notations.

Parameter	Notation
Susceptible Switches class nodes	S_S
Exposed Switches class nodes	E_S
Infected Switches class nodes	I_S
Recovered Switches class nodes	R_S
Susceptible Controllers class nodes	S_C
Exposed Controllers class nodes	E_C
Infected Controllers class nodes	I_C
Recovered Controllers class nodes	R_C
S to E transition rates	β_S, β_C
E to I transition rates	ϵ_S, ϵ_C
I to R transition rates	γ_S, γ_C
R to S transition rates	α_S, α_C
Service Provider system	ω_{SP}
Basic reproduction number	R_o
Transmission matrix	$\boldsymbol{F}$
Transition matrix	$\boldsymbol{V^{-1}}$

and,

$$\boldsymbol{V^{-1}} = \begin{pmatrix} 1/\epsilon_S & 0 & 0 & 0 \\ 1/\gamma_S & 1/\gamma_S & 0 & 0 \\ 0 & 0 & 1/\epsilon_C & 0 \\ 0 & 0 & 1/\gamma_C & 1/\gamma_C \end{pmatrix} \tag{13}$$

then:

$$\boldsymbol{FV^{-1}} = \begin{pmatrix} \beta_S S_S/\gamma_S & \beta_S S_S/\gamma_S & \beta_S S_S/\gamma_C & \beta_S S_S/\gamma_C \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \beta_C S_C/\gamma_C & \beta_C S_C/\gamma_C \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{14}$$

From the next generation matrix (NGM) for compartmental epidemic models we know that the reproduction number R_o is the dominant eigenvalue of the matrix $\boldsymbol{FV^{-1}}$ [42], but for the SP model we found that we have two eigenvalues as follows:

$$\lambda(\boldsymbol{FV^{-1}}) = \begin{pmatrix} 0 \\ 0 \\ \beta_C S_C/\gamma_C \\ \beta_S S_S/\gamma_S \end{pmatrix} \tag{15}$$

According to [42], to determine which of the values is the dominant eigenvalue we have to build an auxiliary matrix $\boldsymbol{E}$ that singles out the rows and columns relevant to the reduced set of states. Where $\boldsymbol{E}$ has the same number of rows as $\boldsymbol{F}$. Then we place one column of $\boldsymbol{E}$ for each non-zero row of $\boldsymbol{F}$ or for each state at infection. The columns of $\boldsymbol{E}$ have a one in the row that corresponds to the non-zero row of $\boldsymbol{F}$, and zeros elsewhere. In other words, we create a matrix $\boldsymbol{E}$ whose columns consist of unit vectors relating to non-zero rows of $\boldsymbol{F}$ only. Then the next generation matrix is computed as $\boldsymbol{E'FV^{-1}E}$. The $\boldsymbol{E}$ auxiliary matrix for our model is:

$$\boldsymbol{E} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \tag{16}$$

Computing $\boldsymbol{E'FV^{-1}E}$ we get:

$$\boldsymbol{E'FV^{-1}E} = \begin{pmatrix} \beta_S S_S/\gamma_S & \beta_S S_S/\gamma_C \\ 0 & \beta_C S_C/\gamma_C \end{pmatrix} \tag{17}$$

The dominant eigenvalue for a 2×2 matrix can be obtained by computing the spectral radius of the matrix. Hence, R_o can be obtained from the trace and the determinant of the matrix as follows [42]:

$$\begin{aligned} R_o &= \rho(\boldsymbol{NGM}) \\ &= \frac{1}{2}\left(Tr(\boldsymbol{NGM}) + \sqrt{Tr(\boldsymbol{NGM})^2 - 4|\boldsymbol{NGM}|}\right) \end{aligned} \tag{18}$$

then,

$$R_o = \frac{\beta_C S_C}{\gamma_C} \tag{19}$$

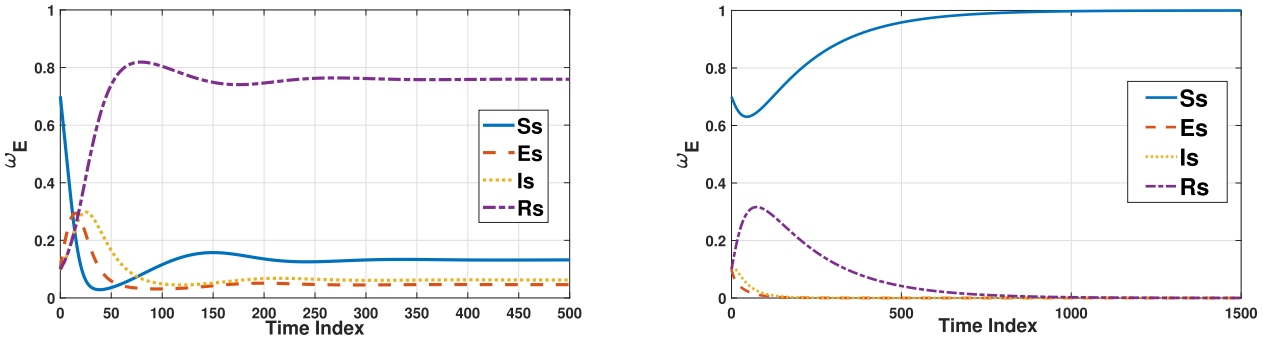
V. MODEL SIMULATIONS

Simulations are carried out using Matlab software, the first step is to define the function that will allow us to solve the ordinary differential equation (ODE) system. Within the mentioned function, we set the number of ODEs' according to the model under analysis. Then the period of time in which the system will become stable needs to be set. Afterwards the initial condition parameters are defined. Finally we call the ode45 function in Matlab in order to solve the system and get the results of its behaviour. The main purpose of the model simulations is to evaluate the system stability and the bot infection behaviour under different scenarios. Since there is no similar model for SDN networks, we used the transition rates utilised in human epidemics that share similar infection vectors compared to our proposed models. The transition rates affect the model dynamics in the way how the individuals get exposed, infected, recovered and become susceptible again.

A. ENTERPRISE MODEL SIMULATIONS

The transition parameters used for the simulations are taken from the Covid-19 model proposed in [6], which correspond to β=0.506, ϵ=0.0903, γ=0.0668 and α=0.0055. We established the initial conditions to be $\{S_S, E_S, I_S, R_S\}$ = {0.70, 0.10, 0.10, 0.10} (Table 3). To prove the stability of the system we perform the simulations when $R_o > 1$ as shown in figure 6.a. Where the system is in endemic equilibrium, meaning that the different devices are going to move among different states in time according to the transition parameters. A graphical representation of such behaviour is shown in figure 7. Where the blue circles represent the susceptible devices within the network, the orange crosses represent the exposed devices, the red stars represent the infected devices and the green squares represent the recovered devices. Figure 7 also shows the condition of the system when it reaches the steady-state, which will be later validated using the final value theorem (FVT).

We also proved the system stability when $R_o < 1$ as shown in figure 6.b where we can see that the amount of nodes within the state S_S are the ones that experience continuous growth in time, eventually allowing to the system to become disease free. Then we tested the system for different spreading rate values (β), which allowed us to identify that the higher this value the more infectious the system becomes



(a) Positive Reproduction Number Analysis.

(b) Negative Reproduction Number Analysis.

FIGURE 6. Reproduction number stability analysis - Enterprise Scenario - Susceptible (S), Exposed (E), Infected (I) and Recovered (R).

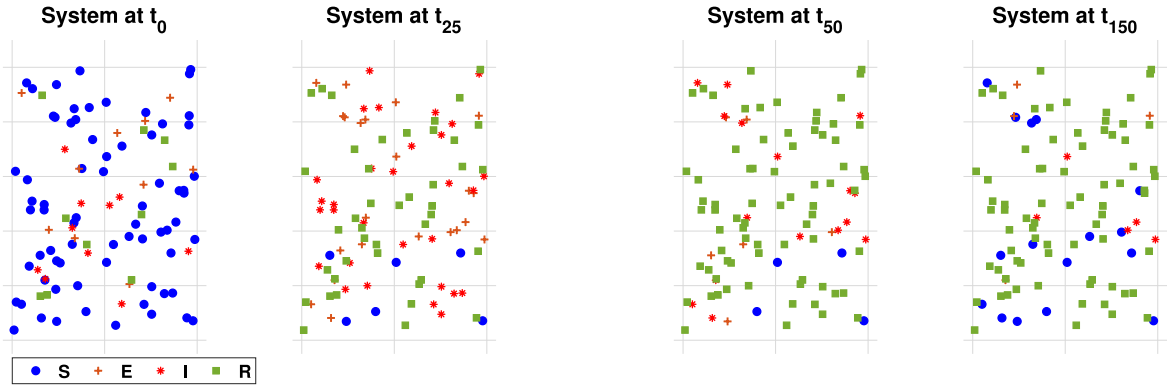


FIGURE 7. Enterprise system evolution in time. t_0 = initial condition - t_{150} = steady condition.

TABLE 3. Enterprise epidemic simulation values.

Parameter	Value
S_S	0.70
E_S	0.10
I_S	0.10
R_S	0.10
$\beta\ (R_o > 1)$	0.5060
$\beta\ (R_o < 1)$	0.0500
ϵ	0.0903
γ	0.0668
α	0.0055

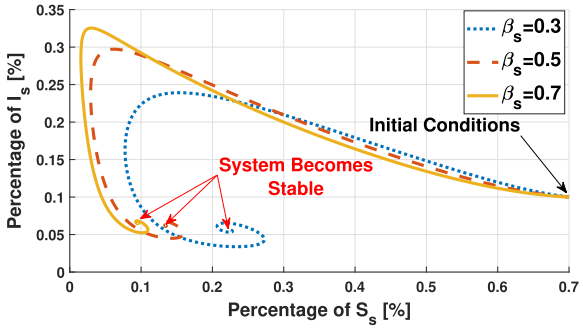


FIGURE 8. Susceptible compartment behaviour versus infectious compartment behaviour in enterprise model.

as shown in figure 8. Where the infectious class nodes (I_S) versus the susceptible class nodes (S_S) behaviour over the time is presented. The system behaviour is clearly determined by the transition rates, thus it is crucial to have as much control as possible over them. Well defined security policies will help to reduce the amount of vulnerable devices that can be infected. However, attackers can take advantage of zero-day vulnerabilities to infect devices. For such cases a fast detection of anomaly behaviour is required to identify which devices could be infected and act accordingly to help to stop the spread of the malware.

B. SERVICE PROVIDER MODEL SIMULATIONS

The transition parameters used for the simulations are taken from the Zika model proposed in [10], which correspond to β_S=0.9688, ϵ_S=0.1174, γ_S=0.1137 and α_S=0.0710 for the switches and β_C=0.2610 ($R_o > 1$), β_C=0.1000 ($R_o < 1$), ϵ_C=0.1174, γ_C=0.1137 and α_C=0.071 for the controllers. We established the initial conditions to be $\{S_S, E_S, I_S, R_S\}$ = {0.55, 0.15, 0.15, 0.15} and $\{S_C, E_C, I_C, R_C\}$ = {0.55, 0.15, 0.15, 0.15} (Table 4). To prove the stability of the system we perform the simulations when $R_o > 1$ as shown in figure 11.a. Also, we proved the system stability when $R_o < 1$ as shown in figure 11.b where we can see that the amount of nodes within the states S_S and S_C are the ones that experience continuous growth in time, eventually allowing to the system to become disease free. Then we tested the system for different spreading rate values β_C, which allowed us to identify that the higher this value the more infectious

TABLE 4. SP epidemic simulation values.

Parameter	Value
S_S, S_C	0.55
E_S, E_C	0.15
I_S, I_C	0.15
R_S, R_C	0.15
β_S	0.9688
ϵ_S, ϵ_C	0.1174
γ_S, γ_C	0.1137
α_S, α_C	0.0710
β_C ($R_o > 1$)	0.2610
β_C ($R_o < 1$)	0.1000

the system becomes. Not only in regards to the controllers, but also the forwarding devices are affected by such changes. When we increase the value of β_C, the amount of infected controllers increases exponentially as shown in figure 9.

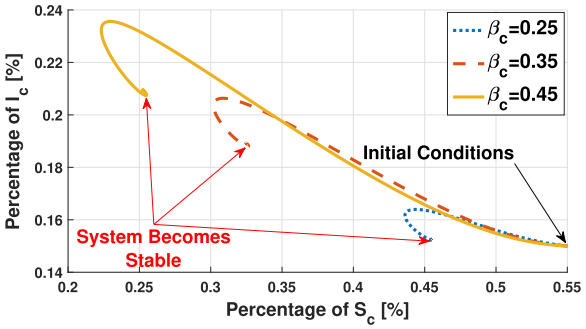


FIGURE 9. Susceptible compartment behaviour versus Infectious compartment behaviour of controllers in SP model.

Meanwhile, the number of infected switches has a linear increase due to the controller infection rate as shown in figure 10.

We found that when the reproduction number R_o increases in both scenarios, the botnet malware is able to rapidly spread among the SDN devices. The proposed models allow to identify that maintaining and ensuring low infection rates and a high recovery rates would stop the spread of botnet malware within SDN networks. Thus, the main goal is to keep R_o as low as possible, and try to have it lower than 1 to avoid the infection spread at all. Such achievement could be obtained by following well defined security methodologies, policies and processes. Such as patching and hardening the operating system running in the devices; running vulnerabilities assessments in well defined periods of times; doing periodical checks of the systems and identify possible infections; and safeguarding the communication channels that are being used by the SDN devices.

C. THEORETICAL MODEL VALIDATION

In order to validate the proposed models we applied the final value theorem (FVT) used in control systems to the resultant ordinary differential equations (ODEs) of the Enterprise Epidemic Model. The FVT allows to calculate the asymptotic value of a signal (steady-state value) [46]. The FVT is used

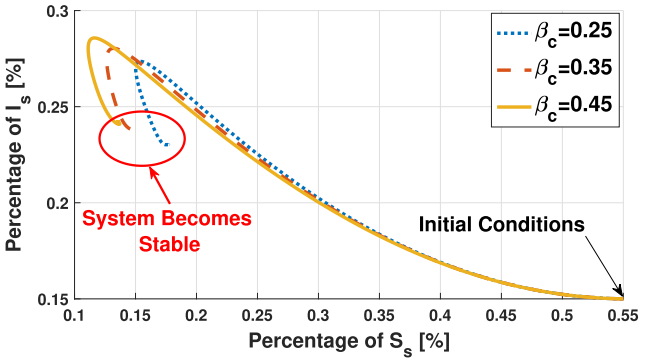


FIGURE 10. Susceptible compartment behaviour versus infectious compartment behaviour of switches in SP model.

to determine this value when the time signal function is not available, but the function in the s domain is known or can be calculated. For our specific scenario we can get the Laplace transform of the enterprise model system of ODEs represented in eq.(2) to set the system into the s domain. Then, we computationally solve the system of equations using MATLAB, in order to find the values of $S_S(s)$, $E_S(s)$, $I_S(s)$ and $R_S(s)$, where:

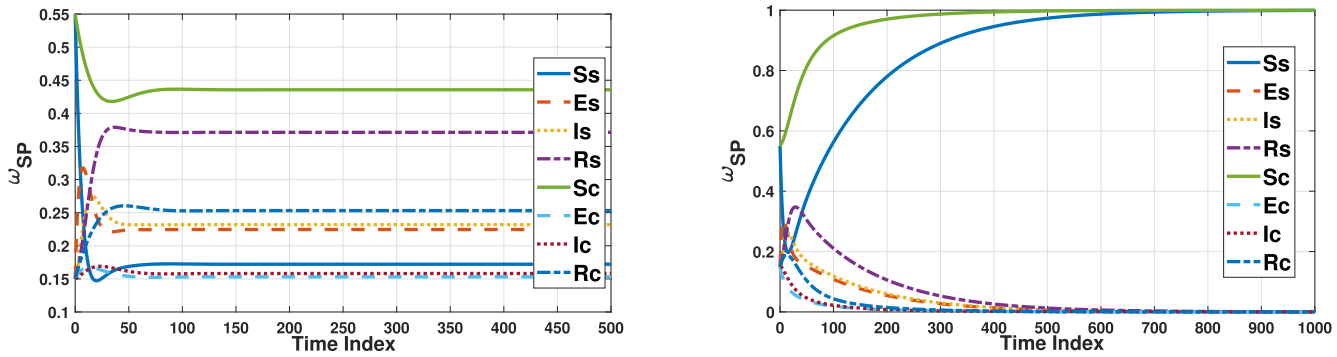
$$\begin{aligned} S_S(s) &= \mathcal{L}\{S_S(t)\} \\ E_S(s) &= \mathcal{L}\{E_S(t)\} \\ I_S(s) &= \mathcal{L}\{I_S(t)\} \\ R_S(s) &= \mathcal{L}\{R_S(t)\} \end{aligned} \tag{20}$$

Finally, we apply the FVT represented in (21) to the previous equations to calculate the steady-state values.

$$\lim_{t\to\infty} \omega_E(t) = \lim_{s\to 0} s\Omega_E(s) = \omega_{E\infty} \tag{21}$$

where $\Omega_E(s) = \mathcal{L}\{\omega_E(t)\}$ and the steady-state value of the system is defined as $\omega_{E\infty} = \{S_{S\infty}, E_{S\infty}, I_{S\infty}, R_{S\infty}\}$.

According to our simulations, the enterprise model has two different possibilities for its steady-states values, the first one when $R_o > 1$ and the second one when $R_o < 1$ as shown in figure 6. The steady-state values estimated in the simulations when $R_o > 1$ are the following for each compartment: $S_S = 0.1321$, $E_S = 0.0462$, $I_S = 0.0624$ and $R_S = 0.7593$. Meanwhile, the steady-state values when $R_o < 1$ are $S_S = 1$ and $E_S = S_S = R_S = 0$. The calculated values obtained using the FVT must match the ones we found in the simulations. After solving the system of equations in the s domain, we obtained 2 functions for each state. We set the same initial conditions used in the simulations in order to assign values to the transition rates in the equations. Finally, we solve 21 for each node and function in the s domain. The solution for the first functions of each node provide the following results: $S_S = 0.1120$, $E_S = 0.0533$, $I_S = 0.0720$ and $R_S = 0.7627$, which correspond to the system when $R_o > 1$. As we can see the values have a difference of ± 0.0100 compared to the simulated values as consequence of computational errors during the estimations. However, the solution for the second functions of each node were the



(a) Positive Reproduction Number Analysis.

(b) Negative Reproduction Number Analysis.

FIGURE 11. Reproduction number stability analysis - Service Provider Scenario - Susceptible (S), Exposed (E), Infected (I) and Recovered (R).

following: $S_S = 1$ and $E_S = S_S = R_S = 0$, which is equal to the results simulated when $R_o < 1$. Then, it is possible to say that the model satisfies the FVT, thus the model has been theoretically validated. The service provider model followed the same design considerations as the enterprise model. Then, it is possible to conclude that is a valid model as the enterprise model.

VI. CONCLUSION

The COVID-19 pandemic triggered a huge shift in everyone's ways of work and lifestyle, while exponentially increasing the growth of DDoS attacks [2]. The attacks targeted critical infrastructure during the pandemic, such as e-commerce, healthcare and educational services using high-throughput attacks generated from botnet armies. Such attacks were designed to quickly overwhelm and take down victims with short-burst attacks. Therefore, understanding the infection behaviour of botnets becomes relevant for the prevention and mitigation of DDoS attacks.

We present two models regarding the botnet infection dynamics in SDN following the same fashion as in human diseases. The proposed models consider more comprehensive factors when compared to existing models, like the possibility of having an infection vector between the control and data plane as we propose in the SP scenario. Thus, we propose two epidemic models to represent botnet propagation among SDN devices for two different scenarios. The first proposed model analyses the dynamics for SDN enterprise networks using a SEIRS model. The second one is designed for the infection process in SDN service provider networks, and it is a SEIRS-SEIRS model. We compare our models with the approaches used for Zika and COVID-19 diseases because they share equivalent infection vectors. In specific, the enterprise model shares similarities with the COVID-19 models proposed so far [6]. While the service provider (SP) model is comparable to models in which zoonoses is present, such as the Zika virus [10], where infection amid different species is possible. Both scenarios are represented using the compartmental modelling approach, in such a way that the models can be applied to any other kind of networks as long as they have similar infection vectors. Ordinary differential equations (ODEs) have been used to analyse and simulate the proposed epidemics dynamics. For such purpose, the reproduction number R_o is obtained using the next generation matrix (NGM) approach in both cases. Next, the stability of the systems was proved and the infection behaviour was studied under different environments. Finally, we presented the theoretical model validation using the final value theorem (FVT) by finding the steady-state values of the systems. The steady-state values are relevant to our models since they provide a better understanding of the epidemic process. Such understanding is fundamental in the development of prevention and mitigation techniques for SDN. The proposed models provide a wider insight about the bot recruitment cycle, which is essential when studying DDoS attacks.

REFERENCES

[1] NETSCOUT. (2020). *NETSCOUT Threat Intelligence Report Issue 4: Findings From 2H 2019*. [Online]. Available: https://www.netscout.com/sites/default/files/2020-02/SECR_001_EN-2001_Web.pdf

[2] NETSCOUT. (2020). *NETSCOUT Threat Intelligence Report Issue 5: Findings From 1H 2020*. [Online]. Available: https://www.netscout.com/threatreport

[3] NETSCOUT. (2019). *NETSCOUT Arbor's 14th Annual Worldwide Infrastructure Security Report (WISR)*. [Online]. Available: https://www.netscout.com/sites/default/files/2019-03/SECR_005_EN-1901%E2%80%93WISR.pdf

[4] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, and D. Kumar, "Understanding the mirai botnet," in *Proc. 26th USENIX Secur. Symp.*, 2017, pp. 1093–1110.

[5] H. W. Hethcote, "The mathematics of infectious diseases," *SIAM Rev.*, vol. 42, no. 4, pp. 599–653, 2000.

[6] J. M. Carcione, J. E. Santos, C. Bagaini, and J. Ba, "A simulation of a COVID-19 epidemic based on a deterministic SEIR model," *Frontiers Public Health*, vol. 8, p. 230, May 2020.

[7] C. M. Batistela, D. P. F. Correa, Á. M. Bueno, and J. R. C. Piqueira, "SIRSi compartmental model for COVID-19 pandemic with immunity loss," *Chaos, Solitons Fractals*, vol. 142, Jan. 2021, Art. no. 110388.

[8] Q. Deng, "Dynamics and development of the COVID-19 epidemic in the united states: A compartmental model enhanced with deep learning techniques," *J. Med. Internet Res.*, vol. 22, no. 8, Aug. 2020, Art. no. e21173.

[9] S. Mwalili, M. Kimathi, V. Ojiambo, D. Gathungu, and R. Mbogo, "SEIR model for COVID-19 dynamics incorporating the environment and social distancing," *BMC Res. Notes*, vol. 13, no. 1, pp. 1–5, Dec. 2020.

[10] M. Rahman, K. Bekele-Maxwell, L. L. Cates, H. T. Banks, and N. K. Vaidya, "Modeling Zika virus transmission dynamics: Parameter estimates, disease characteristics, and prevention," *Sci. Rep.*, vol. 9, no. 1, pp. 1–13, Dec. 2019.
[11] E. Bonyah, M. A. Khan, K. O. Okosun, and S. Islam, "A theoretical model for Zika virus transmission," *PLoS ONE*, vol. 12, no. 10, Oct. 2017, Art. no. e0185540.
[12] F. B. Agusto, S. Bewick, and W. F. Fagan, "Mathematical model of Zika virus with vertical transmission," *Infectious Disease Model.*, vol. 2, no. 2, pp. 244–267, May 2017.
[13] M. V. Ozanne, G. D. Brown, A. J. Toepp, B. M. Scorza, J. J. Oleson, M. E. Wilson, and C. A. Petersen, "Bayesian compartmental models and associated reproductive numbers for an infection with multiple transmission modes," *Biometrics*, vol. 76, no. 3, pp. 711–721, Sep. 2020.
[14] H. Wan and H. Zhu, "The backward bifurcation in compartmental models for West Nile virus," *Math. Biosci.*, vol. 227, no. 1, pp. 20–28, Sep. 2010.
[15] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy*, May 1991, pp. 343–359.
[16] J. O. Kephart and S. R. White, "Measuring and modeling computer virus prevalence," in *Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy*, May 1993, pp. 2–15.
[17] A. Mahboubi, S. Camtepe, and H. Morarji, "A study on formal methods to generalize heterogeneous mobile malware propagation and their impacts," *IEEE Access*, vol. 5, pp. 27740–27756, 2017.
[18] V. Taynitskiy, E. Gubar, and Q. Zhu, "Optimal impulse control of bi-virus SIR epidemics with application to heterogeneous Internet of Things," in *Proc. Constructive Nonsmooth Anal. Rel. Topics (CNSA)*, May 2017, pp. 1–4.
[19] S. Shen, H. Zhou, S. Feng, J. Liu, H. Zhang, and Q. Cao, "An epidemiology-based model for disclosing dynamics of malware propagation in heterogeneous and mobile WSNs," *IEEE Access*, vol. 8, pp. 43876–43887, 2020.
[20] P. K. Srivastava, S. P. Pandey, N. Gupta, S. P. Singh, and R. P. Ojha, "Modeling and analysis of antimalware effect on wireless sensor network," in *Proc. IEEE 4th Int. Conf. Comput. Commun. Syst. (ICCCS)*, Feb. 2019, pp. 639–643.
[21] A. Dabarov, M. Sharipov, A. Dadlani, M. S. Kumar, W. Saad, and C. S. Hong, "Heterogeneous projection of disruptive malware prevalence in mobile social networks," *IEEE Commun. Lett.*, vol. 24, no. 8, pp. 1673–1677, Aug. 2020.
[22] Giri, S. Jyothi, and C. S. Vorugunti, "Epidemic model based evaluation of malware propagation in Twitter," in *Proc. 9th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2017, pp. 407–408.
[23] A. Zhaikhan, M. A. Kishk, H. ElSawy, and M.-S. Alouini, "Safeguarding the IoT from malware epidemics: A percolation theory approach," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 6039–6052, Apr. 2021.
[24] Q. Fu, Y. Yao, C. Sheng, and W. Yang, "Interplay between malware epidemics and honeynet potency in industrial control system network," *IEEE Access*, vol. 8, pp. 81582–81593, 2020.
[25] D. Kreutz, F. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.
[26] J. F. Balarezo, S. Wang, K. G. Chavez, A. Al-Hourani, J. Fu, and K. Sithamparanathan, "Low-rate TCP DDoS attack model in the south-bound channel of software defined networks," in *Proc. 14th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2020, pp. 1–10.
[27] P. J. Delves and I. M. Roitt, "The immune system," *New England J. Med.*, vol. 343, no. 1, pp. 37–49, 2000.
[28] I. You and K. Yim, "Malware obfuscation techniques: A brief survey," in *Proc. Int. Conf. Broadband, Wireless Comput., Commun. Appl.*, Nov. 2010, pp. 297–300.
[29] O. Yurekten and M. Demirci, "SDN-based cyber defense: A survey," *Future Gener. Comput. Syst.*, vol. 115, pp. 126–149, Feb. 2021.
[30] N. T. Bailey, *The Mathematical Theory of Infectious Diseases and its Applications*. High Wycombe, U.K.: Charles Griffin, 1975.
[31] A. Dadlani, M. S. Kumar, K. Kim, and K. Sohraby, "Stability and immunization analysis of a malware spread model over scale-free networks," *IEEE Commun. Lett.*, vol. 18, no. 11, pp. 1907–1910, Nov. 2014.
[32] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Optimal control of epidemic information dissemination over networks," *IEEE Trans. Cybern.*, vol. 44, no. 12, pp. 2316–2328, Dec. 2014.
[33] S. Hosseini, M. A. Azgomi, and A. T. Rahmani, "On the global dynamics of an SEIRS epidemic model of malware propagation," in *Proc. 7'th Int. Symp. Telecommun. (IST)*, Sep. 2014, pp. 646–651.
[34] I. Androulidakis, S. Huerta, V. Vlachos, and I. Santos, "Epidemic model for malware targeting telephony networks," in *Proc. 23rd Int. Conf. Telecommun. (ICT)*, May 2016, pp. 1–5.
[35] S. Shen, H. Zhou, S. Feng, J. Liu, and Q. Cao, "SNIRD: Disclosing rules of malware spread in heterogeneous wireless sensor networks," *IEEE Access*, vol. 7, pp. 92881–92892, 2019.
[36] S. R. Biswal and S. K. Swain, "Model for study of malware propagation dynamics in wireless sensor network," in *Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI)*, Apr. 2019, pp. 647–653.
[37] G. Meng, M. Patrick, Y. Xue, Y. Liu, and J. Zhang, "Securing Android app markets via modeling and predicting malware spread between markets," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1944–1959, Jul. 2019.
[38] Y. Chen, Y. Mao, S. Leng, Y. Wei, and Y. Chiang, "Malware propagation analysis in message-recallable online social networks," in *Proc. IEEE 17th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2017, pp. 1366–1371.
[39] Z. Wang, H. Hu, and C. Zhang, "On achieving SDN controller diversity for improved network security using coloring algorithm," in *Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC)*, Dec. 2017, pp. 1270–1275.
[40] L. Liu, R. K. L. Ko, G. Ren, and X. Xu, "Malware propagation and prevention model for time-varying community networks within software defined networks," *Secur. Commun. Netw.*, vol. 2017, pp. 1–8, Jan. 2017.
[41] O. Diekmann, J. A. P. Heesterbeek, and J. A. J. Metz, "On the definition and the computation of the basic reproduction ratio R_0 in models for infectious diseases in heterogeneous populations," *J. Math. Biol.*, vol. 28, no. 4, pp. 365–382, Jun. 1990.
[42] O. Diekmann, J. A. P. Heesterbeek, and M. G. Roberts, "The construction of next-generation matrices for compartmental epidemic models," *J. Roy. Soc. Interface*, vol. 7, no. 47, pp. 873–885, Jun. 2010.
[43] P. van den Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," *Math. Biosci.*, vol. 180, no. 12, pp. 29–48, Nov./Dec. 2002.
[44] M. G. Roberts and J. A. P. Heesterbeek, "Characterizing the next-generation matrix and basic reproduction number in ecological epidemiology," *J. Math. Biol.*, vol. 66, nos. 4–5, pp. 1045–1064, Mar. 2013.
[45] S. K. Biswas, U. Ghosh, and S. Sarkar, "Mathematical model of Zika virus dynamics with vector control and sensitivity analysis," *Infectious Disease Model.*, vol. 5, pp. 23–41, Jan. 2020.
[46] J. Chen, K. H. Lundberg, D. E. Davison, and D. S. Bernstein, "The final value theorem revisited-infinite limits and irrational functions," *IEEE Control Syst. Mag.*, vol. 27, no. 3, pp. 97–99, Jun. 2007.

JUAN FERNANDO BALAREZO (Member, IEEE) received the Engineering degree in electronic and telecommunication engineering from the Army Polytechnic School, Ecuador, in 2013, the master's degree in networks and security from Monash University, Australia, in 2016, and the ethical hacker certification from the EC Council, in 2018. He is currently pursuing the Ph.D. degree in electrical and electronic engineering. His research interests include the security of software-defined networks, denial of service attacks (DDoS), and attack modeling. He received the Postgraduate Dux Award for his master's degree.

SONG WANG received the B.E. degree in communication engineering from Shanghai University, China, in 2007, and the master's degree in telecommunication engineering from RMIT University, Australia, in 2016, where he is currently pursuing the Ph.D. degree in electrical and electronic engineering. His research interests include security of software-defined networks and the Internet of Things.

KARINA GOMEZ CHAVEZ received the Engineering degree in electronic and telecommunication engineering from the National Polytechnic School, Ecuador, in 2006, the master's degree in wireless systems and related technologies from the Polytechnic University of Turin, Italy, in 2006, and the Ph.D. degree in telecommunications from the University of Trento, Italy, in 2013. In 2007, she joined the Communication and Location Technologies Area, FIAT Research Centre. In 2008, she joined the Future Networks Area, Create-Net, working on several national, European, and industrial projects. In July 2015, she was a Lecturer with the School of Engineering, RMIT University, where her role is to coordinate several networking courses and supervise several master's and Ph.D. students. She is currently a Project Manager with Milano Teleport. She has several patents and published her research in important journals and conferences. Her current research interests include energy efficiency networks, 4G/5G mobile networks architecture and network protocols, the Internet of Things (IoT) technologies, software-defined networking (SDN), network functions virtualization (NFV), network security, multi-layer resources management and orchestration, and emergency communications.

AKRAM AL-HOURANI (Senior Member, IEEE) received the B.Eng., M.B.A., and C.P.Eng. degrees, and the Ph.D. degree from RMIT University, Melbourne, Australia, in 2016. He is currently a Senior Lecturer and the Program Manager for the Master of Engineering (telecommunication and networks) with the School of Engineering, RMIT University. He has published more than 55 journal articles and conference proceedings, including three book chapters. In 2020, he received the IEEE Sensors Council Paper Award for his contribution to hand-gesture recognition using neural networks. He has extensive industry/government engagement as the Chief Investigator in multiple research projects related to the Internet of Things (IoT), smart cities, and satellite/wireless communications. As the Lead Chief Investigator, he oversaw the design and deployment of the largest open IoT network in Australia in collaboration with five local governments "Northern Melbourne Smart Cities Network"; this project has won the 2020 "IoT Awards," the official awards program of IoT Alliance Australia. Prior to his academic career, between 2006–2013, he extensively worked in the ICT industry sector, as a Research and Development Engineer, a Radio Network Planning Engineer, and then as an ICT Program Manager for several projects spanning over different technologies, including mobile networks deployment, satellite networks, and railway ICT systems. His current research interests include UAV communication systems, automotive and mmWave radars, energy efficiency in wireless networks, and the Internet of Things over satellite. He is also serving as an Associate Editor for *Frontiers in Space Technologies* and *Frontiers in Communications and Networks*, and a Guest Editor for *Remote Sensing* (MDPI) Special Issue on Satellite communication.

SITHAMPARANATHAN KANDEEPAN (Senior Member, IEEE) received the Ph.D. degree from the University of Technology Sydney. He has previously worked at the NICTA Research Laboratory, Canberra, and the CREATE-NET Research Center, Italy. He has authored over 140 peer-reviewed journals and conference papers, including a book on cognitive radio techniques, with Dr. A. Giorgetti. His current research interests include the Internet of Things (IoT), SDN, security, and wireless/mobile/satellite communications systems and networks. He was a recipient of the RMIT Research Excellence Award, in 2019; the IEEE Communications Society Certificate of Appreciation, in 2015, for ten years' contribution to the field; and the IEEE Exemplary Reviewer Award, in 2011. He was the chair of several IEEE Committees and Workshops. He is currently an Editor of the Special Issue on Future Evolution of Public Safety Communications in the 5G Era in the *ETT* journal (Wiley).